WOODHEAD PUBLISHING
IN MECHANICAL ENGINEERING

Aircraft system safety

Military and civil aeronautical applications

Duane Kritzinger

CRC

WP

Aircraft system safety

Related titles:

Introduction to aerospace materials
(ISBN-13: 978-1-85573-946-8; ISBN-10: 1-85573-946-1)
An extensive introduction to the materials used in modern aircraft, helicopters and spacecraft, this book is intended for undergraduate students studying aerospace and aeronautical engineering. The contents have been based on curriculum subjects delivered at universities in the United States, Europe and Australasia. The book will be a valuable resource for postgraduate students and practising aerospace engineers.

Engineering catastrophes – Causes and effects of major accidents, 3rd edition
(ISBN-13: 978-1-84569-016-8; ISBN-10: 1-84569-016-8)
This new edition of a well received and popular book contains a general update of historical data, more material concerning road and rail accidents and, most importantly, a new chapter on the human factor. The author provides a broad survey of the accidents to which engineering structures and vehicles may be subject. Historical records are analysed to determine how loss and fatality rates vary with time and these results are displayed in numerous graphs and tables. Notable catastrophes such as the sinking of the *Titanic* and the *Estonia* ferry disaster are described. Natural disasters are considered generally, with more detail in this edition on the role that humans play in disasters.

Details of these and other Woodhead Publishing books and journals can be obtained by:

- visiting our website at www.woodheadpublishing.com
- contacting Customer Services (e-mail: sales@woodhead-publishing.com; fax: +44 (0) 1223 893694; tel.: +44 (0) 1223 891358 ext. 30; address: Woodhead Publishing Limited, Abington Hall, Abington, Cambridge CB1 6AH, England)

If you would like to receive information on forthcoming titles, please send your address details to: Francis Dodds (address, tel. and fax as above; email: francisd@woodhead-publishing.com). Please confirm which subject areas you are interested in.

Aircraft system safety

Military and civil aeronautical applications

Duane Kritzinger

CRC Press
Boca Raton Boston New York Washington, DC

WOODHEAD PUBLISHING LIMITED
Cambridge, England

Published by Woodhead Publishing Limited, Abington Hall, Abington
Cambridge CB1 6AH, England
www.woodheadpublishing.com

Published in North America by CRC Press LLC, 6000 Broken Sound Parkway, NW,
Suite 300, Boca Raton, FL 33487, USA

First published 2006, Woodhead Publishing Limited and CRC Press LLC

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. Reasonable efforts have been made to publish reliable data and information, but the author and the publishers cannot assume responsibility for the validity of all materials. Neither the author nor the publishers, nor anyone else associated with this publication, shall be liable for any loss, damage or liability directly or indirectly caused or alleged to be caused by this book.

Trademark notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data
A catalog record for this book is available from the Library of Congress.

Woodhead Publishing Limited ISBN-13: 978-1-84569-136-3 (book)
Woodhead Publishing Limited ISBN-10: 1-84569-136-9 (book)
Woodhead Publishing Limited ISBN-13: 978-1-84569-150-9 (e-book)
Woodhead Publishing Limited ISBN-10: 1-84569-150-4 (e-book)
CRC Press ISBN-10: 0-8493-9012-5
CRC Press order number: WP9012

The publishers' policy is to use permanent paper from mills that operate a sustainable forestry policy, and which has been manufactured from pulp which is processed using acid-free and elementary chlorine-free practices. Furthermore, the publishers ensure that the text paper and cover board used have met acceptable environmental accreditation standards.

Typeset in India by Replika Press Pvt Ltd.
Printed by T J International Limited, Padstow, Cornwall, England.

Contents

Preface *ix*

Acknowledgements *xi*

Introduction *xiii*

1 Safety within the legal framework 1

1.1 Introduction 1
1.2 Criminal liability 1
1.3 Civil liability 2
1.4 Sentencing trends 4
1.5 Organisational responses 6
1.6 Implications on the engineer 13
1.7 Discussion 15
1.8 Further reading 16

2 The safety concept 17

2.1 Understanding safety 17
2.2 The importance of safety 18
2.3 Safety segments 19
2.4 Ensuring safety 20

3 Standards and regulations 23

3.1 Introduction 23
3.2 Airworthiness 24
3.3 Source of regulations 26
3.4 Civil regulatory authorities 28
3.5 Military regulatory authorities 34
3.6 Health and safety regulations 38
3.7 The impact on organisations 40
3.8 The impact on safety management systems 41
3.9 Discussion 41

4 Risk-based approach 43

4.1 Introduction 43
4.2 Defining risk 44
4.3 Assessing risk 45
4.4 As low as reasonably practicable (ALARP) 46
4.5 Managing the risk 49
4.6 Summarising the risk-based approach 52
4.7 Discussion 55
4.8 Further reading 56

5 Goal-based approach 57

5.1 Introduction 57
5.2 Probability targets vs. failure severity levels 57
5.3 Discussion 60
5.4 Combining the risk- and goal-based criteria 66

6 Hazards 69

6.1 Understanding hazards and their causes 69
6.2 Identifying hazards 74
6.3 Equipment failures and faults 76
6.4 Hazards of a normal functioning system 80
6.5 Systemic failures 85
6.6 Safety assessment tools and techniques 91
6.7 Discussion 92

7 The fail-safe dimension 94

7.1 Introduction 94
7.2 Defences against failures 94
7.3 Fail-safe principles 96
7.4 Applying fail-safe principles 99
7.5 Summary 102

8 The system safety assessment 104

8.1 History 104
8.2 Aims and objectives of a system safety assessment 105
8.3 The system and its relationship to safety 107
8.4 Planning the safety assessment 110
8.5 Safety during the development process 112
8.6 Modelling the safety assessment process 115
8.7 Conducting a safety assessment 120
8.8 Generating the system safety assessment report 123
8.9 Discussion 127

9 The safety case 129

9.1 History 129
9.2 Developing the requirement 133
9.3 Core components 136
9.4 The safety case report 141
9.5 Discussion 146

10 Numerical probabilistic approach 148

10.1 Introduction 148
10.2 The fundamental concepts 149
10.3 Applied quantitative assessment 155
10.4 Assessment process 160
10.5 Specific issues of concern 162
10.6 Determining failure rates of basic events 171
10.7 Discussion 180
10.8 Further reading 181

11 Minimum equipment lists 182

11.1 Introduction 182
11.2 The concept of minimum equipment lists 182
11.3 Generic approach 184
11.4 Process 185
11.5 Equipment included in an MMEL/MEL 191
11.6 Discussion 192

12 The safety management system 193

12.1 Introduction 193
12.2 What is a safety management system? 194
12.3 Safety culture 195
12.4 Developing a safety management system 197
12.5 Discussion 202
12.6 Further reading 203

13 Concluding observations 204

13.1 Aviation trends 204
13.2 Safety assessments/safety cases 205
13.3 New technologies 207
13.4 Safety engineering competence 209
13.5 Safety culture 209
13.6 Impact on projects 210
13.7 Final remarks 211

Appendix A: Safety assessment tools and techniques 213

Appendix B: Safety criteria 292

Appendix C: GSN safety argument 313

Abbreviations and acronyms 319

Definitions 324

References and further reading 335

Index 339

Preface

As a young mechanical engineer, in the South African Air Force, I was soon expected to conduct safety assessments on proposed modifications to aircraft. Initially, these assessments were based around the blind application of a limited set of techniques (specifically the FMEA). The task was seldom enjoyable or productive.

A few years later I moved on to evaluating modifications proposed by third parties (e.g. contractors) where it was easy to criticise and demand more from their safety assessments. Again I found that efficiency was not the order of the day and that the final results were considered little more than dust-gathering tombs of data, which soon became outdated as they did not keep pace with the system's configuration.

After thirteen adventurous years in the Air Force, I joined the private sector. I had now come full circle, whereupon I was once again faced with the other side of the coin. Now my safety assessments were to be scrutinised by military authorities (i.e. those in my old role), as well as the civil authorities (e.g. CAA, FAA, etc.).

It was time for me to find a better, more consistent way of assessing safety, and reporting on such an assessment. The fundamental concerns I had included:

- stakeholder expectations (e.g. what is expected from a safety case or an FMEA) – especially when combining military and civil approaches (e.g. a civil design organisation modifying a military aircraft, or vice versa)
- terminology and definitions (e.g. distinguishing between a hazard and a failure)
- safety criteria (i.e. objective targets which can be given to a responsible party to achieve or monitor)
- auditability (i.e. recording the safety argument, evidence and decisions)
- practical use (i.e. the safety assessment/case should not only be used to evaluate risks, but should be useful throughout the product lifecycle – from evaluating a design, to assisting in fault diagnoses during operational use)
- system integration (i.e. efficiently conducting and integrating sub-system safety assessments into a system safety assessment/case)
- presentation (i.e. how to argue the integrity of the systems (and the assessment) though the compilation of previously disparate documents).

Starting from the principle that there is no one correct way of doing a safety assessment, I nevertheless endeavoured to compile my own 'user-guide' (from which I could 'cut-and-paste' definitions, approaches, templates, etc.), that would assist me to deliver consistently high-quality safety assessments efficiently.

As a Principal Safety and Certification Engineer, I was also expected to assist/train/educate fellow engineers to conduct safety assessments on a variety of modifications. I found this user-guide particularly useful in this regard, and the lessons learned (from our struggles) I plough[1] back into this 'user-guide' so as to make the whole process more efficient and effective the next time round. It was during one of these learning cycles that a young engineer remarked 'I wish we had this information at university when they tried to teach us this' when the idea was instilled to compile a textbook that could be used for just such a purpose.

The objective of this book is to address the bulleted points above. It does not provide templates of how to apply specific tools or techniques (this may be presented in the next book, who knows). Safety has always been of paramount concern to the aerospace industry and it has been a leading sector in the take-up of new and increasingly sophisticated methods for assessing acceptable levels of safety. The methods described in this book are those considered appropriate for the development of large transport aircraft systems,[2] but any industrial sector producing complex and potentially hazardous systems would need something similar.

A wealth of ideas, concepts, tools and approaches from various and diverse sources and industries have been drawn on in this book in an attempt to bring concisely the theory of safety together in a useful reference guide. Although this subject area is very dynamic and constantly evolving, there are some basic elements which form the foundation for its understanding. It is hoped that those who are concerned with safety assessments (i.e. students, designers, safety assessors and their managers, customers, etc.) will be assisted in appreciating the context, value and limitations of the concepts introduced and, if nothing else, will lead people to ask the right questions.

[1] Note the use of the present tense – I am still learning and will probably continue to do so for as long as I am involved with safety assessments.

[2] The proven safety record of commercial transport aircraft under JAR/FAR Part 25 is the standard by which the safety of other transportation systems is often measured.

Acknowledgements

This book would never have existed without the experience I received from my time of employment at the South African Air Force and Marshall Aerospace of Cambridge. I will be forever grateful for the breadth of exposure I received from working on a variety of aircraft platforms (i.e. fixed- and rotor-wing, military and civil aircraft, transport and fast jets, manned and unmanned); international certification authorities (military and civil); a variety of programmes (i.e. structural and avionic); as well as the interesting and knowledgeable individuals I have met along the way.

I cannot begin to thank adequately those who helped in the preparation of this book. A special thank you to my friends and colleagues who kindly volunteered to review and provide valuable new insights for the theories I was trying to convey: Bernie Guignard (Ch. 1), Doug Henderson (Ch. 10), Grayhame Fish (Ch. 1), Ian Roberts (Fig. 8.8), Iya Solodilova (Fig. 8.8 and Appendix A), Jim Watts (Chs 8 and 9), Stephen Goldsmith (Chs 1 to 12), Richard Ehlers (Chs 3 and 6) and Vic Owen (Chs 2, 4 and 6). I am also grateful for the illustration assistance provided by Adam Cundick (front cover photo), Dave Ash (Fig. 8.8) and Simon Parker (Fig. 5.2).

I have learned a lot from seminars, conferences, journals, papers and the books of others. All those whom I have cited in the text have their relevant works listed in the references at the end. I am especially indebted to Ted Lloyd and Walter Tye for their ground-breaking book *Systematic Safety* first published in 1982, and which remains an invaluable point of reference for anyone attempting to assess the safety of an aircraft system. I am grateful for the constructive criticism and tactful suggestions made by Woodhead Publishing's independent reviewers, as well as my airworthiness consultant friends Brian Perry (civil) and Jan Schutte (military) who provided invaluable comments, corrections, suggestions and improvements. It is my sincere hope that they will all approve of the final result.

I acknowledge with thanks the permission I have been given to reproduce the following copyright material: Fig. 13.1 from Boeing; Fig. 13.2 from Doug Arbuckle (NASA); Fig. 6.1 from Lockheed Martin; Fig. 8.1 from Barry de Beer (South African Department of Defence); and to Captain Robert Eijkelkamp (from the Royal Netherlands Airforce) for the front cover photo (taken by Fotovlucht Soesterberg).

I would also like to thank the following personnel at Woodhead Publishing Limited for the quality of support, advice, feedback and assistance during transformation of my manuscript into this publication: Sheril Leich (Commissioning Editor), Emma Pearce (Project Editor) and Stuart Macfarlane (Production Services).

Above all it was my best friend, sternest critic, biggest fan and loving wife Nicole who encouraged me to persevere, who has been a careful reader of the manuscript and a contributor to its final form and content.

Introduction

All individuals want to be free from harm, whatever the cause. But perfect safety is rare because almost every activity has its dangers. Accidents can, and do, happen. Sooner or later the unexpected interactions will occur, and every type of accident has this in common:

- Nobody perceived the conspiracy of events that would lead to disaster
- They were all preventable – which means that blame will be allocated.

Management's legal liabilities are likely to increase in the future. In the UK a new draft bill proposes the introduction of the new offence of corporate killing. This hinges on past cases where charges of manslaughter have been unsuccessful, as it was impossible to lay the blame on any specific individual, and there was no precedent for 'convicting' a company. However, according to Hadden-Cave (1999), the new bill will introduce corporate killing, reckless killing and gross carelessness. Once this is introduced, it could be adopted throughout the Commonwealth, which often shadows English Law. Other parts of the world are facing similar changes and have already progressed management's liability to new frontiers.

Fulfilling these legal and ethical obligations requires that safety risks be identified, quantified and managed accordingly. The crucial question will be whether there was a failure of management (for all stakeholders) to provide for safety. In terms of criminal liability, all companies will have to look very carefully at their safety management systems.

Legislation generally requires the production of a written justification that a new system is acceptably safe before it is allowed to enter service. Traditionally this has been addressed by presenting a large collection of test results, safety analyses, outputs and other data to a third party (such as a regulatory body). The hope is often that the weight (quite literally) of such evidence will be accepted as an overwhelming demonstration that the system has been adequately proven. But as systems become more complex and software intensive, assessment of the completeness and consistency of such information becomes more difficult. What is needed is a far more rigorous approach to safety, which provides logical arguments with supporting evidence and has clearly defined objectives, strategies, assumptions and justifications.

We often hear that safety is paramount – or that it has the highest priority. Safety is an emotive and subjective topic and many people want all risks eliminated at all costs. This is seldom possible. What is needed is a practical and consistent approach to target potential causes of harm and identify where the most benefit could be derived. A balanced view must be taken in which safety does not dominate and prevent effective business but in which safety is not ignored, as it so often has been in the past.

Safety must be built in, not added on. The emphasis should be on hazard identification and analysis, rather than on the reliability of design standards. It involves a planned, disciplined, systematically organised, and pro-active process. The emphasis should be placed on considering safety as a design parameter and thereby integrating an acceptable level of safety into the system in the first place. This requires a disciplined application of the tools and methods involved in order to ensure a cost-effective achievement of the desired goal. Yet historically, the degree of rigour applied to these processes has often been less than the consequences of error might suggest to be appropriate.

Complex[1] new technologies, more often than not, have a significant effect on safety. Aviation's history provides evidence that, whatever the benefits of technological advances, the safety graph dips – or at least wavers – while industry learns how to use the new technology. There is a clear indication that the sheer complexity of modern systems create problems for notions of management control (Smith, 1999). Weaknesses in the management of complex technological systems permit predictable and unintentional errors and cause catastrophic loss (Keely, 2000). Given the sheer complexity of modern systems, management faces problems of emergence – where elements of a system interact to create properties that had previously been unforeseen. When it comes to system safety, the 'total is often more than the sum of the parts'. By breaking complex systems down into their component parts (reductionism) to generate solutions, we compound the risk of further failure by neglecting the impact of such interventions on the emergent properties of the system.

Designs likely to mature within the next decade will involve even more critical use of complex systems, many of which will apply:

- digital techniques to achieve the complex functions envisaged
- system integration (including inter-reactions and inter-dependabilities) (Collins and Perry, 2003)
- redundancy and reconfiguration capabilities (Collins and Perry, 2003).

Demonstrating the accomplishment of safety requirements is likely to be a formidable task. The problem is that many system engineers do not have the appropriate training in the required safety approaches, tools and techniques and their managers do not know when and how they may be applied.

A revised relationship between management and safety is the most important avenue to explore. It is this relationship between complexity and control that lies at the heart of the problem of safety management and which is of both pragmatic and academic importance. We need some way of measuring safety and an ability to ensure that we arrive at the necessary safety parameters. It is implicit, therefore, that all reasonably foreseeable hazards have to be identified systematically (throughout

[1] The term 'complex' refers to systems whose safety cannot be shown solely by test and whose logic is difficult to comprehend without the aid of analytical tools.

the product life-cycle, not only during development) and the risk assessed before a judgement can be made upon their acceptability.

In order to do this we have to understand the issues that influence safety and the means by which they are identified and managed. Only then can we judge the acceptability of any threats associated with the initial and continued use of a particular product. This book will attempt to address many of these issues.

In Chapter 1, we consider the legal issues associated with system safety. The purpose of this chapter is to reinforce the liabilities assumed in the generation of safety related documentation. In Chapter 2 we attempt to put the term 'safety' into perspective, and the basic approaches used to achieve it. The next three chapters will then explore three of these approaches; the use of Regulatory Standards is explored in Chapter 3; Chapter 4 considers the risk-based approach, which is widely adopted in the military industry as well as by Health & Safety specialists; Chapter 5 introduces the civil aeronautical approach to safety assessments, which (for the want of a better term) we shall call the 'goal-based' approach (in contrast to the risk-based approach in Chapter 4) as it provides clear goals (i.e. failure probability targets) for system designers to achieve.

In Chapter 6 we consider the issues surrounding the application of the term 'hazard' and how the causes of hazards can be identified. Appendix A supports this chapter as it summarises a list of potential tools and techniques that can be used for cause and consequence assessments. Chapter 7 provides an introduction into the fail-safe concept, which is needed to ensure the high levels of functional integrity needed from essential systems.

The next two chapters consider the generic approach to two frequently asked for deliverables. Chapter 8 considers the system safety assessment (SSA), which is usually required for the certification of a new/modified system. In the civil arena, the SSA is often based on the goal-based approach. In contrast, the safety case in considered in Chapter 9. The safety case is the document that manages (via the risk-based approach) the major hazards that an operator/maintainer of a system/facility faces, as well as the means employed to control those hazards.

Probability assessment (either qualitative or quantitative) is an essential part of any safety validation (whether risk- or goal-based). Chapter 10 provides some guidance in this regard and should be read with an understanding of Chapter 7. In Chapter 11 we continue the probability estimation theme of Chapter 10 by applying it to the minimum equipment list, which allows operation of a system despite deficiencies and equipment failures. Chapter 12 explores how, via the safety management system, organisations manage safety as an integral part of their business management activities.

Appendix A supports Chapter 6 by summarising the advantages and limitations of some of the models used for causal or consequence analyses. Appendix B supports Chapters 4, 5, 8 and 9 by summarising useful safety criteria that can be used in safety assessments. Appendix C provides a brief introduction to goal structured notation, which is useful for defining safety arguments as referenced in Chapters 8 and 9.

1
Safety within the legal framework

Men are only clever at shifting blame from their own shoulders to those of others

Titus Livius (59BC–AD12)

1.1 Introduction

Most industrial activities are regulated, and this includes military and civil aviation safety management. Ethical considerations and an increasingly litigious society regarding product liability have become driving factors in changing the way we conduct the initial safety certification (which leads to the release of a system) and manage the continuing safety of the system (including operations and maintenance).

Laws are a system of rules, which are intended to reflect social values, and are enforced through the courts (e.g. it is unacceptable to steal, kill, etc.). Laws can be considered as a compilation of rights, duties and obligations – the violation of which could give rise to legal liability.

In the aftermath of an accident, there is an increasing issue of corporate liability of the CEO and the board of the blamed (e.g. the design authority, maintainer, operator, etc.) – with both fiscal and penal punishments for failure. In today's world, litigation is very expensive and the duty of care of the board exposes them, through their accountabilities, to the possibility of corporate liability – or even to charges of corporate manslaughter.

The content of this chapter is based on English law and is intended to draw engineering management's attention to the legal aspects affecting system safety – it is not meant to be, and should not be regarded as, a complete or accurate statement of the current law. Legislation in this area is developing throughout the world, and is likely to continue to do so for some time. Under English law, legal liability is enforced in two ways: criminal liability and civil liability.

1.2 Criminal liability[1]

This is the law of offences (i.e. crimes) against the state and those under its protection. Prosecution is usually started by the state and it aims to punish and to act as a deterrent through fines, imprisonment, orders and disqualification from holding office. Guilt is determined through the application of the 'beyond all reasonable doubt' principle.

[1] See also *Introduction to System Safety Engineering and Management,* University of York.

One example of the impact of criminal law affecting the work of engineers is from the legislation by government through the agency of the Health and Safety Executive. The Health and Safety at Work Act[2] (HSWA) of 1974 imposes duties on persons who design, manufacture, import or supply articles for use at work to ensure (so far as reasonably practicable) that they are 'safe'; to test them; provide proper information; carry out research with a view to eliminating risks, etc.

The HSWA established the Health and Safety Commission (HSC) and the Health and Safety Executive (HSE). Whilst the HSC defines policy, the HSE is responsible for the day to day monitoring and enforcing of the HSWA. The HSE[3] has delegated powers to serve Improvement Notices (requires remedial action) and Prohibition Notices (stops a process). Failure to comply can lead to prosecution. The HSWA affects product safety as well as workplace safety and is based on the 'as low as reasonably practicable' (ALARP[4]) principle, where 'practicable' refers to what is possible to do, and 'reasonable' requires a balance of costs, time, and trouble against the risk.

> Reported in *Aerospace International* (RaeS, Nov 2005): 'Henry Perrier, a former head of the Concorde division at Aerospatiale, has been placed under criminal investigation in connection with the crash of the (Concorde) airliner in July 2000. He may face a manslaughter trial for flaws in the aircraft which could have contributed to the disaster'.

1.3 Civil liability[5]

Criminal law does little for the victims of a crime. Civil law regulates the relationship between individuals and thus provides the mechanism whereby the wrongdoers have to compensate the victims. Guilt is determined through the application of the 'balance of probability' principle.

Civil Law comprises Contract Law, Tort (civil wrong), the Law of Property, Succession and Family Law, etc. Action is started by a person (which, in law includes a corporate body such as a company) and it has the aim to compensate (and to deter).

Civil liability for a defective system can arise under the laws of contract, misrepresentation, tort, other common law doctrines and under current UK legislation. Liability can fall on the manufacturer, supplier, distributor or certifier of products (Falla, 1997). In practice, such a supplier or manufacturer is a company and is

[2] The principal health and safety legislation in Great Britain is the Health and Safety at Work etc. Act 1974 (HSWA). This sets out in general terms the health and safety duties of employers, employees, and manufacturers, suppliers, and designers of articles for use at work. The HSWA applies to all workplaces (including the MoD and the self-employed). It provides protection for workers and general public.

[3] The HSE has subsidiary organisations (e.g. Nuclear Installations Inspectorate (NII), Her Majesty's Railway Inspectorate (HMRI)).

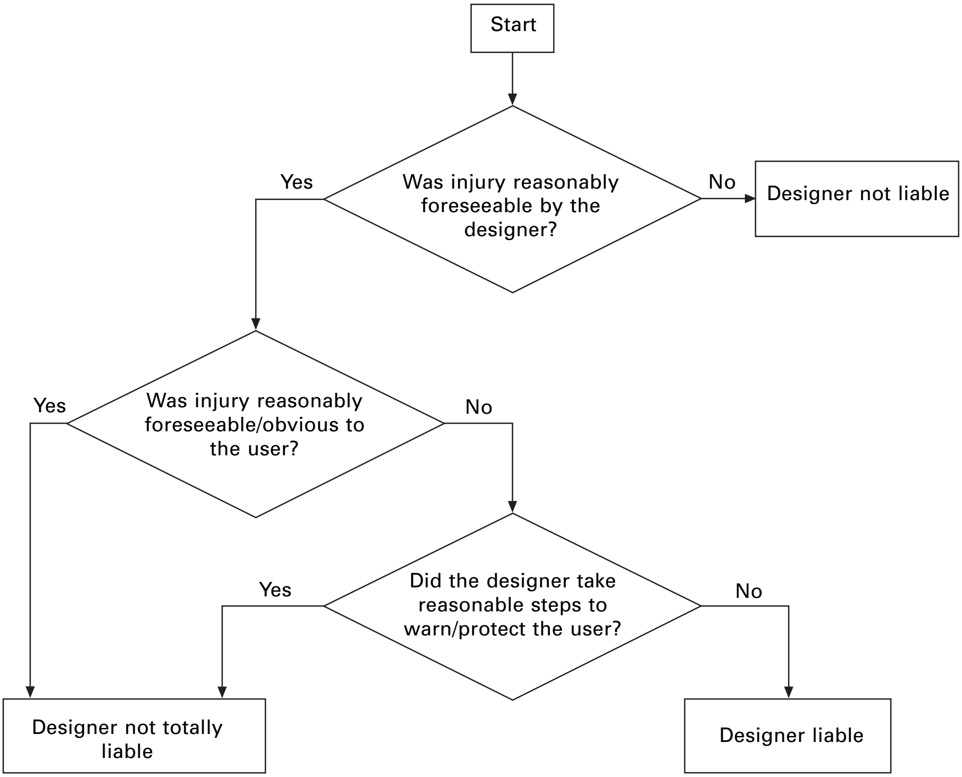
[4] See also Chapter 4.

[5] See also *Introduction to System Safety Engineering and Management,* University of York.

regarded as a legal entity who can sue or can be sued in its own right. Suppliers of components can also be liable. In cases where the component is used in products which are exposed to the general public the extent of such liability can be enormous.

Under Civil Law (Tort), individuals can claim compensation if they can show that a duty of care was owed, this duty has been breached, and that a loss has been suffered. An example of this process is illustrated in Fig. 1.1. Plaintiffs have to prove that they were owed a duty of care, that there was a breach of that duty, and that the loss or damage was a direct result of that negligence. The claimant does not have to prove negligence[6] on the part of the supplier. All professional work is done under contracts containing either an express or implied term that professional persons will use reasonable skill and care in the performance of the work.

Under the Consumer Protection Act of 1987 (see section 1.4.1), a supplier is liable if there is a causal link between a defect and an injury (this is referred to as the 'Liability of Tort'). A product is defective if it does not provide the safety that people are generally entitled to expect, taking into account all circumstances (all circumstances


Start
Was injury reasonably foreseeable by the designer?
Yes
No
Designer not liable
Was injury reasonably foreseeable/obvious to the user?
Yes
No
Did the designer take reasonable steps to warn/protect the user?
Yes
No
Designer not totally liable
Designer liable

1.1 Duty of care vs. liability.

[6] Negligence is the failure to exercise the degree of care that is required by law in the particular circumstances. Negligence can occur by an act or omission.

include 'the manner in which and the purpose for which the product has been marketed'). Products are defined very loosely, and without a doubt includes all aviation products – from substances, materials, components, through to systems and platforms. Furthermore, a product consists not only of the product itself, but also of the literature and warnings (i.e. instructions for, or warning of, doing or refraining from doing anything with the product) which accompany it.

1.4 Sentencing trends

1.4.1 Consumer Protection Act

The Consumer Protection Act, 1987, was enacted in the UK to fulfil obligations to implement a European Directive designed to protect consumers across member states. It introduces so-called 'strict liability' (as opposed to 'fault liability' in contract and tort) for defective products supplied in the course of a business. Where damage is caused by a defect in a product then the producer is liable to compensate the injured party whether or not he is at 'fault' (Falla, 1997).

Falla (1997) also highlights the fact that the removal of the fault criteria means that the Consumer Protection Act imposes the highest 'standard of care' on a producer. If a producer is not liable under the Act it is unlikely he will be found liable in negligence. Only damage of a specific type may form the basis of an action under the Consumer Protection Act. The damage may be death, personal injury or damage to property. However, only property which is of a type ordinarily intended for private use[7] may be the subject of a claim and property damage must exceed £275.[8]

A plaintiff who brings an action under the Consumer Protection Act must show that, as a result of the defect in the product, it was reasonably foreseeable that an injury of the type suffered would occur. This is unlikely to be difficult in the context of a safety-critical system: if it is not safe, it is reasonably foreseeable that persons will be injured and property damaged as a result.

1.4.2 Legal charges

The legal consequence of product failures that subsequently cause harm and/or loss might include criminal actions (e.g., manslaughter, Health & Safety at Work charges, corporate manslaughter, corporate manslaughter by gross neglect) or civil actions (e.g., on the contract, trespass (person), trespass (property), negligence, strict liability actions).

[7] Therefore, if a chemical plant were to explode because of a faulty computer control system the damage to any surrounding office buildings or to the chemical plant itself could not be the subject of a claim under the Act. Office buildings are not ordinarily intended for private use. However, if the homes or possessions of nearby individuals were also damaged, liability to pay compensation would arise for the damage to those houses and possessions under the Consumer Protection Act.

[8] Or such other figure as substituted by legislation from time to time.

1.4.3 Fines

Fines under HSWA (sections 2–6) can be up to £20,000, with the average fine in 1997–1998 being £6,223.

> A judgment in the Court of Appeal (*Regina* vs. *F Howe & Sons*, Nov. 1998): 'a fine must be large enough to bring home to those who manage a company, and their shareholders, the need for a safe environment for workers and the public. While a fine should not generally be so large as to imperil the earnings of employees or create a risk of bankruptcy, there may be cases where an offence is so serious that the defendant ought not to be in business.'

Fines have been increasing under the civil law (HSWA), e.g., £5.1 million in March 2001 for a boy made quadriplegic (civil). Fines have also been increasing under the criminal law (HSWA), e.g., £1.2 million fine on Balfour Beatty in Feb 1999 due to collapse of train tunnels in Heathrow Express Rail Link.

1.4.4 Prosecutions

At the extreme, accidental loss of life could result in individuals and companies being prosecuted for manslaughter under the criminal law. Any company is represented by senior members (e.g. the main board) who could be subject to imprisonment or fines.

> Kite and OLL (1996): Death of school children in canoeing accident in Lyme Bay. Kite was one of only two directors, and was jailed as the 'controlling mind'.

Manslaughter is an unusual crime where the prosecutor does not have to establish intent, but has to show reckless disregard of accepted practices, gross negligence (or 'such disregard for life'), or conscious wrong doing before it is a criminal act. However, determining the extent of individual responsibility on the 'controlling mind' has led to many unsuccessful prosecutions. Hence the Law Commission report in 1996, which recommended[9] laws on:

- Corporate killing, applicable to companies: this is intended to make a company accountable in criminal law where conduct falls far below that which can be reasonably expected in the circumstances. The proposed maximum penalty here is for an unlimited fine and a remedial order that is designed to prevent the original cause of the accident. In addition, directors might well be liable to disqualification.

[9] The UK Home Secretary has made it clear that he intends to reform the law to make it easier to identify and convict those responsible for corporate killing. It is generally accepted that a company and/or a corporation must operate responsibly but the current debate on corporate killing really starts with the current involuntary manslaughter law, which has proved to be ineffective when applied to corporate killing.

- Reckless killing and killing by gross carelessness: this is applicable to individuals, including company directors, where:
  - reckless killing typically involves an individual knowing that there is a risk that their product or conduct will cause a fatality or a serious injury and that it is not reasonable to take that risk. In this instance the maximum penalty is quoted as life imprisonment.
  - A person is guilty of gross carelessness when the risk that the product/conduct could cause death or serious injury is obvious to a reasonable person in his position. The individual concerned should have been capable of appreciating the risk and that their conduct fell far below what could reasonably be expected of them in the circumstances. Or they intended their action to cause an injury, or they unreasonably took a risk that it might cause an injury. Killing by gross carelessness could lead to a maximum penalty of ten years in prison.

The Law Commission's suggested text states:

4 (1) A corporation is guilty of corporate killing if:
(a) a management failure by the corporation is the cause or one of the causes of a person's death; and
(b) that failure constitutes conduct falling far below what can reasonably be expected of the corporation in the circumstances.
(2) For the purposes of subsection (1) above:
(a) there is a management failing by a corporation if the way in which its activities are managed or organised fails to ensure the health and safety of persons employed in or affected by those activities.
(b) Such a failure may be regarded as a cause of a person's death notwithstanding that the immediate cause is the act or omission of an individual

1.5 Organisational responses

1.5.1 Legal liability for dangerous or defective systems

Manufacturers, suppliers, importers and designers of articles (which includes equipment for use at work) must (refer HSWA Section 6) in so far as they are matters within their control:

- ensure that articles for use at work are designed and constructed to be safe at all relevant times, i.e., when they are being set, used, cleaned or maintained by persons at work
- arrange for testing and examination to ensure compliance with the above
- provide persons supplied by them with adequate information about:
  - the uses for which such articles are designed or tested
  - any conditions necessary to ensure that the articles will be safe at all relevant times and when being dismantled or disposed of
- update the information referred to above as necessary, upon discovering that anything gives rise to a serious risk to health and safety.

An issue which should exercise the mind of any supplier of a critical system is the question of exposure in law should the system fail.

Directors

A director of a company will operate under some form of service contract which will include, either explicitly or implicitly, a term that the director will take reasonable care in the exercise of his or her duties. A director has authority to exercise the powers which the company has given him. If in the exercise of such powers he breaches his duty of care either through negligence or by a deliberate act or omission, the director may be held liable for the breach, the consequences of which could vary from the death of an unconnected individual to financial loss by the company's creditors. The degree of fault required to impose liability on a director varies according to the consequence of the breach. This will depend upon whether he is liable under civil or criminal law.[10] Breach of this contract will have the effect that the company could in theory sue the director, but the damages available to the company will be limited by the director's resources. In addition, the company may have difficulty showing that the company's loss is a consequence of the director's breach of contract.

Employees

Negligent employees and independent contractors may also be held liable in contract and in tort, but again the damages available will be limited by the individual's resources. The distinction between an employee and a contractor does not depend solely on whether the contract declares a worker to be an independent contractor. Each case will depend on its own facts but account will be taken of the ownership of equipment, the chance of profit and the risk of loss on the worker's part.

1.5.2 Organisational response to the criminal law

The standard 'as far as reasonably practicable' is that used in the HSWA case law. The standard has acquired the meaning that the risk of adverse effect (e.g. death or injury) must be balanced against the cost, time and physical difficulty of taking measures to

[10] There have been recent moves for directors to be made personally liable in criminal cases, e.g., manslaughter. Although there have only been a few reported cases, there is a definite trend towards making directors more accountable. The one hundred delegates (refer to www.health and safety.co.uk (10 January 2004)) to the recent British Safety Council conference (2004) heard its Director General David Ballard warn that 'Time is running out for those who, through blatant disregard of the law, allow employees to be killed or injured and yet are punished with fines in the low thousands'. Ballard continued 'Every senior executive and health and safety director should be extremely concerned about the new offences. This may even deter some from taking jobs that carry heavy responsibilities. Executives working under the threat of possible imprisonment for safety lapses will simply have to be more alert and better trained to appreciate risks. The public's desire for retribution is a strong consideration for any change to the law but, in the end, the purpose of any legislation has to be to improve health and safety performance.'

reduce the risk. If the quantified risk is insignificant compared with the measures needed to mitigate the risk, then no action needs to be taken to satisfy the law. However, increased risk will require robust justification to support a choice of no action.

All organisations must publish Health and Safety Policy, covering:

- risk assessment, identification and minimisation
- procedures and facilities for safe handling, storage and transportation
- product integrity regime
- surveillance (information, instructions, supervision)
- emergency procedures.

Corporate response must include:

- a safety management system (SMS)
- safety management plans and procedures/processes (including those to deal with product integrity).

Milan Linate Airport (Oct. 2001), 118 casualties:
A high-speed collision in severe fog between a Scandinavian Airlines Boeing MD-87 and a private Cessna Citation CJ2 occurred because the CJ2 was on the wrong taxiway and then crossed the active runway without permission. Four people were judged guilty (subject to appeal) of negligence and manslaughter and ordered to pay court costs, to pay compensation to the victims' families and disqualified for life from public service. Prison sentences: the Tower Controller and the Airport Manager each received 8 years, an official at Italy's National Agency for Civil Aviation (ENAC) received 6.5 years, as did the managing director of Italy's air traffic services. One of the issues criticised in the accident report was the lack of a safety management system: there were systematic faults in the sense that the [management] system had either not noticed them, or it had tolerated them.

Source: *Flight International* (27 Apr.–3 May 2004)

The Act also requires:

- a director in charge with explicit responsibilities for training, inspection (prevention) and investigation
- an explicit chain of authority and identification of responsibilities (often normal management chain and separate line to responsible manager)
- regular auditing.

1.5.3 Organisational response to the civil law

Project teams, contractors, consultants, software houses, advisers, independent auditors, test houses, manual producers, operators, maintainers, regulators, etc., all make for one big happy family until it goes wrong and there is a big hole in the ground (e.g. after the Concorde crash in France, the defendants included BAe systems, Air France, Continental, Middle River, GE, Goodyear, EADS, etc.). Then the lawyers reach for their law reports and legal liability will surely arise. Each party will then try to devolve their liability to the producers, operators, maintainers, contractors, consultants, advisers, integrated project teams (IPTs), independent advisers, regulators, etc.

The crucial question will be whether there was a failure of management to provide for safety. In terms of criminal liability, all companies have to look very carefully at their management systems.[11] Management need to take the following actions to discharge a duty of care and to reduce the chance of product liability:

- Establish an effective safety management system/process. Nominate key roles/ responsibilities. Define approval signatories – especially for safety reports. Establish independent verification/audit to reduce chance of undetected error. Establish a workforce-wide commitment to product integrity. Learn from previous mistakes.
- Initiate a documentary audit trail (identify, log and track all hazards). Airworthiness and safety must be foremost in the minds of the entire organisation. Furthermore, as many legal cases turn on documentation, it is essential that risk assessment activities and choices are documented and that records are kept.[12]
- Spread the risks, either via contract terms, or via insurance (see section 1.5.4).
- Insurance can give limited protection against some civil claims; specific advice should be sought from brokers specialising in this field.

1.5.4 Organisational responses to the Consumer Protection Act

Section 10 of Part II of the Consumer Protection Act 1987 makes it a criminal offence to supply any consumer goods[13] which do not comply with the ‘general safety requirement’ of it being reasonably safe with due regard to all circumstances. Organisations will have to ensure, so far as reasonably practicable, that the hardware and software are designed and constructed for safe operation of the system (*Safety-*

[11] It seems likely that a chief executive will be able to reduce the chance of a corporate killing prosecution through employing a competent health and safety director who is directly responsible to a board. But a company will need to introduce a watertight health and safety plan which will cover worker participation and reports of all near misses which will have to be reviewed at Board level. Busy Directors will be forced into expanding their energies into risk identification and elimination and, it is a fact, that many organisations will have to provide additional resources towards providing a safer workplace. In fact, the forthcoming legislation could well create the ethic of putting safety ahead of any cost considerations. And there is no guarantee that a jail sentence will not be imposed on the most safety-conscious executive in a safety-conscious organisation arising from circumstances where the risk was not obvious or appreciated by anybody from shop floor upwards in an organisation.

[12] In a recent court case in England, the judge stated that any form of retrievable information, no matter how that information may be stored, is a document. Letters, internal memos, drawings, films, videos, e-mails, note books, personal dairies, log books, reports, etc., are all food for litigation. Document management is thus essential. According to Williams (2003), the elements of an effective document management system are: their preparation; their storage; ease of retrieval; destruction management; training

[13] ‘Consumer goods’ are defined for the purposes of Section 10, as ‘any goods which are ordinarily intended for private use or consumption’, but exclude a number of products, such as motor vehicles and aircraft, food, water, gas, drugs and (of course) tobacco.

related systems, Guidance for Engineers, Aug 2002, page 14). This includes undertaking all necessary research, testing and examination. It may not be necessary to repeat tests, examinations, certification carried out by other parties in the supply chain, provided that it can be demonstrated that the system is appropriate for the purpose for which it is supplied. All information necessary for the safe operation of the system must be provided.

The practical scope for a manufacturer or supplier to exclude or restrict their liability under the Consumer Protection Act is very limited. According to Falla (1997), the only practical step which a manufacturer or supplier can take is to 'pass the buck' by seeking an indemnity through contract from the person who supplied them. The person who is likely to end up with the liability is, therefore, the person at the beginning of the supply chain.[14]

A producer may be able to rely on the following defences:

- that the defect did not exist when the producer supplied the product
- that the state of scientific and technical knowledge at the time was such that a producer of the same type of product could not be expected to have discovered the defect[15]
- that the component was supplied in accordance with instructions from the producer and the component would not contain a defect had the overall product been designed properly with the component in mind. This defence protects the component manufacturer against a claim arising from a defect in that component which they would otherwise be liable for.[16]

[14] Whether an indemnity from the persons at the beginning of the chain is of any financial value is, of course, something that must always be borne in mind.

[15] This is the so called 'development risk defence' (Falla, 1997). The test is applied at the time when the product was under the producer's control. The wording of UK legislation seems to point to the defence being based upon what a reasonable producer would do. However, a producer should not rely upon this being the case, as the wording of the underlying Directive provides that the defence will apply only if the scientific and technical knowledge was not such as would allow the defect to have been discovered at all. In practice therefore a prudent producer needs to take all the steps possible in order to be sure that they have a defence. The legislation places the burden of proof on the defendant and so it is for the producer to prove that it is impossible to discover the defect.

Manufacturers and suppliers of hardware and software must take notice of (and comply with) those standards which do exist in the industry. Similarly, manufacturers should ensure that adequate verification and validation procedures in the production of hardware and software are followed. They should also take note of any other procedures and draft standards generally followed by cautious manufacturers. Such actions would be seen as evidence in support of this defence, although would not necessarily absolve the defendant from liability.

[16] This defence has the following limitations (Falla, 1997): (i) it is available only to the manufacturer of a *component*; (ii) the component manufacturer must receive instructions from the producer of a product which incorporates his component; (iii) the component manufacturer must have actually complied with those instructions; and (iv) the component manufacturer must be able to show that the defect is wholly attributable to his compliance with those instructions.

Falla (1997) advises that, from a practical point of view, it is unlikely that this third defence will operate in many circumstances. In most situations, manufacturers of complete products will not give instructions which are so detailed as to enable a component manufacturer to take advantage of the defence, particularly since the defence only arises in the defect is wholly attributable to compliance with instructions.

Note that Section 10 of the Act does not apply to goods intended for export or to second-hand goods (refer *Safety-related systems, Guidance for Engineers*, Aug. 2002, page 15). Nor does it apply to retailers if they had no reasonable grounds for believing that the goods failed to comply with the general safety requirement. Defendants who can demonstrate that they follow 'good practice' will usually have a defence to an action founded on the case of negligence (*Safety-related systems, Guidance for Engineers*, Aug. 2002, page 18). This is because the test for negligence is based on a test of 'reasonableness' and following 'good practice' will usually be synonymous with taking reasonable care. However good practice may not be a sufficient defence for complex, integrated safety critical systems. Instead, a 'best practice' argument may be required and a well prepared safety case, safety assessment and/or safety argument would be essential.

1.5.5 Contracts

An agreement between parties forms the basis of a claim in contract. Contractual relationships frequently exist despite the lack of a written document or prior to signing, provided that there is an agreed common intention to form legal relations (Falla, 1997). For a contract to exist there must be:

- an agreement between parties which is formed from an offer given by one and accepted by another
- a consideration which supports the agreement, e.g., money payable or a promise in return for the promise to perform the contract
- an intention to create legal relations (this is presumed in most agreements).

Under legislation which regulates the 'sale of goods' and 'supply of services' and which invariably applies to the supply of hardware and software, there are terms implied in the supply contract. Most important of the provisions are under sections 13 and 14 of the Sale of Goods Act 1979 as amended by the Sale of Goods (Amendments) Act 1994 and the equivalent sections 8 and 9 of the Supply of Goods and Services Act 1982:

- Section 13 states that the goods supplied must correspond with their description. For example, if a computer system has a description that it will 'perform X number of functions per second' or that the software complies with specified standards, the supplier will be in breach of this implied term if the system or software is not as described.
- Section 14 states that the goods must be of satisfactory quality[17] and that they are reasonably fit for the buyer's purpose. The latter part of this implied term applies where the buyer expressly or by implication makes known to the supplier any

[17] The Sale of Goods (Amendments) Act 1994 introduced a new subsection to section 14, i.e., subsection (2D). This provides that the quality of goods includes both state and condition, and includes a non-exhaustive list of factors for taking into account when assessing whether goods meet the requirements of satisfactory quality. Primarily buyers will now find it easier to complain if there are a number of minor defects.

particular purpose for which the goods are being bought (whether or not that purpose is one for which the goods are commonly supplied). In many circumstances, such as in the supply of safety-critical systems, the purpose arises by implication. In circumstances where it would be unreasonable for the buyer to rely on the skill and judgement of the seller, or he did not in fact rely on the seller's skill, then this term is not implied. In the safety-related field it is also likely that a particular purpose will be expressly stated.

Certain clauses (so-called 'exclusion clauses') are commonly relied on to exclude or restrict the liability of a party arising through the failure to perform a contract. The Unfair Contract Terms Act 1977 limits this ability to exclude or restrict liability in certain contracts. In particular, it is never possible to exclude or restrict liability in negligence, or in relation to failure to take reasonable care in the performance of a contract, for personal injury or death by reference to any contract term.[18] A contract sets the parameters of liability, and the rules of privity (i.e. only a party to the contract is able to sue) limit the persons who can claim for loss or damage under a contract. Where, however, a duty of care can be established between a person who has manufactured or supplied a product and the person injured then this injured party may be able to sue in tort for the negligence of the manufacturer or supplier (Falla, 1997).

Falla advises that, in order to have a good cause of action in negligence, a plaintiff must establish that:

- the defendant (manufacturer or supplier) owed the plaintiff a duty of care
- there has been a breach of this duty which caused the injury or damage
- the kind of damage sustained was reasonably foreseeable as a consequence of that breach.

For a duty of care to exist it must be reasonably foreseeable that in the absence of reasonable care in the preparation of a product the consumer (or the innocent bystander) may suffer injury to his (or her) life or property. This duty will occur when the product is intended to reach the ultimate consumer in the state in which it left the manufacturer. In practice, it is not usually difficult to find one or more persons who owe a duty of care in the circumstances of the supply of a safety-critical system.

Case law on negligence in product manufacture and supply has established a number of areas where a lack of reasonable care would constitute a breach of duty (Falla, 1997):

- the design and construction of the product should be done with the care appropriate to the likely dangers in its use
- the component parts should be inspected or otherwise examined to ensure that if properly used in the end product, the end product can be safely used by the consumer

[18] On 1 July 1995 the Unfair Terms in Consumer Contracts Regulations came into force. They only apply to consumer contracts and not to business contracts. Unlike the Unfair Contract Terms Act 1977 the regulations apply to all unfair contract terms and not just unfair exception clauses.

- the container used for the product must be suitable
- the product must be labelled to take account of its dangers
- proper instructions must be given for the safe use of the product.

The manufacturer may raise a number of defences, which could include (Falla, 1997):

- that the manufacturer took all reasonable care whilst making the product to ensure that the defect was not present
- that the product was not initially dangerous but became so because of the action of some intervening person
- that the manufacturer made it clear that the products should not be used before being tested.

Products where computer software is a component present a further level of difficulty. It is not clear, for instance, what the software supplier needs to do to take 'reasonable' care in the design of the system.[19] In practice, an injured party may face significant hurdles establishing a lack of reasonable care. Furthermore, the injured party must also prove that the damage which occurred was a reasonably foreseeable consequence of the breach.

1.6 Implications on the engineer[20]

The *Code of Professional Practice on Engineers and Risk Issues* (hereafter referred to as the Code) became effective on 1 March 1993 and applies to all registrants of the Engineering Council. A member of the engineering profession knowingly and voluntarily undertakes a responsibility to others, and in doing so shoulders certain personal, social and professional responsibilities. Because of their involvement and understanding, engineers have a central role in the control of risk. Their professional duty rightly includes the exercise of competence[21] and integrity.

It is evident that engineers can be held legally accountable for their actions, or for a failure to act. Consequently, all engineers need to acquire an understanding of the law and its relevance to risk issues. Although absolute safety can never be guaranteed, this fundamental limitation is under no circumstances an excuse to avoid professional responsibility. The Code sets out duties of a professional engineer working with safety related systems. These general duties are often supplemented by law (e.g. Health and Safety at Work Act), industry specific regulations (e.g. JAR25.1309) and local codes of practice applicable to a particular task. These all have the following requirements in common:

- to take all reasonable care
- to do all that is reasonably practicable to ensure safety
- to show due diligence to prevent danger.

[19] Note the disclaimer notice contained in many licences issued by software suppliers.

[20] See Engineering Council, *Guidelines on risk issues.* See also (http://www.iee.org/policy/areas/scs/hazpub.cfm

[21] For more on competence, see paragraph 4 of *Safety-related systems, Guidance for Engineers*, Aug. 2002, The Hazards Forum, 1 Great George St, London, SW1P 3AA, ISBN 0 9525103 0 8.

The above three points are usually summarised in some sort of safety case, safety assessment, safety justification or safety argument, which has the following main purposes:

- firstly, and most obviously, to justify to others the confidence which designers and intended purchasers and users have in the safety of the system
- secondly, to provide evidence that, even though an event may occur which was not foreseen or considered when the system was designed, all reasonably determinable safety related concerns were considered and dealt with appropriately in the design and certification of the system. This may provide an important legal defence.

An in-depth assessment from first principles and a cost-benefit analysis are not needed for every job. The extent of consideration should match the nature of the hazard and the extent and uncertainty of the risk and the measures necessary to avert it. In many cases it will be sufficient to identify and comply with the appropriate regulations. However, with hindsight (e.g. after an event) others may challenge actions/ decisions, and an engineer may have to establish the facts in the face of a hostile situation. Ultimately, a decision may have to be defended on judgement and so, particularly where decisions or recommendations are finely balanced, the consideration should be documented and, if possible, corroborated.

Individual engineers[22] need to be aware of their limitations and not undertake tasks for which they are not competent (*Safety-related systems, Guidance for Engineers*, Aug. 2002, page 2). However, there is the possibility that:

- some engineers however well-intentioned, ethically minded, and otherwise competent, might not appreciate their limitations for particular tasks which are, without them being aware of it, differ in some respects from those for which they have proved themselves competent in the past
- some engineers are instructed to perform tasks for which they know or suspect they are not competent enough.

For these circumstances, it is management's responsibility to continually ensure that all practitioners have qualifications, experience and qualities appropriate to their duties and that they are provided with the required resources and authority to perform their duties. Furthermore, sufficient diversity of input/participation will also ensure the intended integrity of the task.

Engineers should be aware of the potential for conflicts of interest, and for differences of opinion between themselves and their employing organisation. In such circumstances, they are advised (*Safety-related systems, Guidance for Engineers*, Aug. 2002, page 25) to maintain written records, kept in a safe place, of any disagreement and the course of action that was taken.

[22] Regarding professional/chartered engineers it is worth noting the following: in many countries (but not yet in the UK) certain positions of engineering authority can be occupied only by registered professional/chartered engineers. Just as medical doctors can be struck off the medical register, so these engineers face being struck off the engineering register if found guilty of professional misconduct or neglect. Loss of professional/chartered registration thus has a severe impact on future career prospects.

Words of wisdom

- ‘Do not believe, prove it for yourself’
- ‘Do not ignore the feelings in your bones’
- ‘Stand by the technical truth, however great the political or commercial pressures’
- ‘*Non fici facio – vera prae ceteres* (don’t give a fig – truth above all)’

David, P.D. (1920–2003),
(Chief Test Pilot for UK CAA for 33 years until his retirement in 1982)

1.7 Discussion

The Engineering Council advises that engineers should, within the constraints of their work responsibility, seek to identify possible hazards and ways to reduce risk. They should not take the attitude that risk management is someone else’s business; rather, they should take the initiative. There is no substitute for professional practice in this regard. A systematic and documented approach will be more cost-effective, auditable and more likely to come to the right conclusions. As a minimum, key risk decisions together with their reasoning should be recorded. It should not be an unreasonable burden. If it is unnecessarily bureaucratic, the system must be modified to be more flexible and so that it can cost-effectively contribute to product quality.

To maintain professional integrity, as well as to avoid legal repercussions, specialist input must be obtained where necessary – even if it has to be bought in. Engineers should not exceed, nor ask others to exceed, their level of competence where the result may put people at risk. Similarly, it is important to validate the competence of contractors and sub-contractors. Professional judgement is by far the most important tool in risk management. Judgement is particularly important in the initial assessment of risks and deciding on their tolerability. Formal safety assessments methods should be used as aids to judgement, not as substitutes for it.

Effective training is essential to success in almost every area of engineering, and risk management is no exception. The key to quality and efficiency is professionalism, which is a combination of expertise and attitude:

- training and experience provide the expertise, while
- company culture and experience shape the attitudes.

In the event of an accident people want someone to blame. We feel unsafe and the only way to feel safe again is to blame somebody. We want one name or entity to blame, who unlike the rest of us, caused us to feel unsafe. The truth is that it never is one name. But still we feel much safer if there is someone to blame. And if the finger is pointed at us, our only defence will be accurate and measurable records of our company’s safety policy and its achievements.

If companies involved in fatal accidents face the risk not only of paying compensation, but also having their employees prosecuted, then accurate and measurable records of a company’s safety policy and its achievements become important evidence. Remember that actions and decisions may be challenged by others with the benefit of hindsight. And hindsight is well known to be an ‘exact science’. Our decisions may have to be defended on the basis of judgement of the issue under concern, and, wherever possible, our decision making process must be documented and validated. How would your records face up to third party scrutiny? How would you be able to demonstrate that you have taken reasonable care as a professional engineer/manager should you be faced with a court appearance?

> The ultimate measure of a man is not where he stands in moments of comfort, but where he stands at times of challenge and controversy.
>
> Martin Luther King Jr (1929–1968)

1.8 Further reading

Chapter 2 in Falla, M. *Advances in Safety Critical Systems, Results and Achievements from the DTI/EPSRC R&D Programme in Safety Critical Systems,* June 1997.
http://www.comp.lancs.ac.uk/computing/resources/scs/#APPENDICES

Safety-related systems, Guidance for Engineers, Aug 2002, The Hazards Forum, Institute of Electrical Engineers, 1 Great George St, London, SW1P 3AA, ISBN 0 9525103 0 8.
http://www.iee.org/policy/areas/scs/hazpub.cfm

Engineers and Risk Issues, Engineering Council's Code of Professional Practice, 1992, Engineering Council, UK.
http://www.iee.org/policy/areas/scs/hazpub.cfm

2
The safety concept

To understand what we think, we need to hear what we are saying

An old saying

2.1 Understanding safety

We often hear pundits pontificate the catch-phrase 'safety at all costs!' But what do we understand by the term 'safety'? Safety can be defined as 'freedom from unacceptable risk of harm' (ISO/IEC Guide 2: 1986 Definition 2.5). But how do we determine an acceptable risk of harm?

From an industry point of view, the acceptability of safety is very difficult to discuss with customers, users, and, even worse, society in general (Murphy, 1991). The perception of safety risk is often influenced by any combination of the following factors:

- **Ignorance.** People may unintentionally accept risk because they are ignorant of the risks, e.g., consider the manner in which tobacco companies marketed the benefits of smoking during the mid-20th century. This trust is largely based upon pragmatics (Johnson, 2003). No individual is able to personally check that their food and drink is free from contamination; that their train is adequately maintained and protected by appropriate signalling equipment; that their domestic appliances continue to conform to the growing array of international safety regulations. On the flip side we may, sometimes irrationally, fear that which we know little about, e.g., consider arachnophobia in countries such as the UK where indigenous spiders are harmless.
- **Familiarity.** People are more comfortable and accepting of risk when they are personally familiar with the operation. For example, is a traveller more fearful of a car accident or a plane crash? Which has the greater risk?
- **Media attention.** We fear problems that we are aware of and that we think are important and credible. Media coverage of issues increases our awareness of a problem and our belief in its credibility.
- **Cost and inconvenience.** A fear of flying transformed the early nineteenth-century world in which it took several weeks rather than a few hours to cross the Atlantic. Another good example is the preference for forward-facing public transport, when it has been proven that rearward facing seats could significantly decrease injuries and increase survival rates.
- **Frequency.** Our belief in the frequency of an accident influences our risk acceptance. If we do not believe that the accident will happen, we are more likely to accept the risk.

- **Control.** Risks from sources outside their direct control are usually perceived to be more significant than they really are (e.g. nuclear power generation vs. conventional means). We accept more risk when we are personally in control, because we trust ourselves. For example, are you more afraid when you drive a car too fast or when you are the passenger in a speeding car?
- **Consequence.** We are not likely to accept risk for facilities that can have accidents with severe consequences. For example, an accident at a nuclear power plant could affect a large population. Therefore, we build very few such plants and we stringently regulate their safety. The risk related to coal-fired plants may be higher, but such plants are not as stringently regulated by the government.
- **Suddenness of consequence.** The sooner we feel the impact of an event, the less likely we are to accept the risk. Would you risk your life to save your car from a carjacker? Would you risk your life by smoking cigarettes for 40 years?
- **Personal versus societal.** We accept risk that affects only ourselves. We apply a higher standard to protect society.
- **Benefit.** Tolerance of risk can be related to perceived benefit; those who derive most benefit often tolerate greater risk than those who derive little or no benefit from the system. As the benefit we receive from an operation increases, we are more accepting of the risk. For example, driving a car is more risky than travelling by plane. Because of personal benefit, people are usually more accepting of driving than flying.
- **Dread.** We have a strong fear or dread of risks whose severity we believe we cannot control. These risks are often thought to be catastrophic, fatal, hard to prevent, inequitable, threatening to future generations, and involuntary. An example is the risk of cancer. People are fearful of anything that may cause cancer because of the nature of the disease, its treatment, and, in some cases, the low probability of recovery.

The above leads to the delusory concepts of ‘safe’ and ‘unsafe’ which, of course, have no real meaning and very little acknowledgement of a measured response to achieve an acceptable level of safety (Murphy, 1991). All systems have a probability of failing to a dangerous state, even though the probability may be extremely small. Miller (2003, p. 105) advises that we should think realistically of safety in relative terms, and he recalls the old vaudevillian exchange in which a man asks, ‘How’s your wife’, to which the comic responds, ‘Compared to what?’

2.2 The importance of safety

Safety is certainly important, but important relative to what?

The problem is that safety is non-deterministic; that is, it cannot be measured directly. Consider the following two definitions of safety:

- Safety is a perceived quality that determines to what extent the management, engineering and operation of a system is free of danger to life, property and the environment (Kuo, 1990).
- Safety is the state in which risk is lower than the boundary risk. The boundary risk

> is the upper limit of acceptable risk. It is specific for a technical purpose or state (SAE ARP4754 p 80).

The common dictionary definition of safety is 'freedom from harm', i.e., freedom from those conditions that can cause death, injury, occupational illness or damage to or loss of property, or damage to the environment. But does such an absolute application exist in the real world where we accept, live with, or otherwise integrate hazards into our everyday lives? It is probably safe to proclaim that there is no such thing as a safe system.

Industry is required to develop products which are sufficiently safe. An unsafe product (actual or perceived) will result in retribution in law and/or the market place. Hence it is essential for management to ensure that effective procedures and practices are in place to ensure that a product is 'safe enough'. Such procedures must ensure the law is satisfied and must also protect against the fallibility of the human (i.e. producer or consumer) involvement.

But how do we then measure safety? Safety is an attribute of a product/system considered in the context of activities for meeting a specific goal. Safety is concerned with physical artefacts and in common with any other it has cost implications (Bradshaw, 1998). An artefact is unsafe if it can cause a hazard which may lead to unacceptable harm (i.e. an accident causing injury, loss of life, material damage or environmental damage). But what is 'unacceptable harm'?

Murphy (1991) reminds us that the safety of any system is always a compromise between:

- the risk of potential accidents and their severity
- the required performance and response time
- design limitations (e.g. imposed by size or weight limits)
- The costs of maintaining redundant systems throughout the product lifecycle
- historical society perception of risk in the specific sector.

Consider the following typical safety goals:

An aircraft developer's/integrator's goal may be

'to be competitive in meeting client's specifications with solutions that are cost-effective at an acceptable level of safety'.

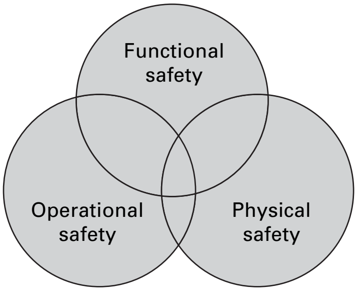
An air force goal may be

'to implement the defence capability by meeting operational requirements with solutions that are both human-resource efficient and cost effective at an acceptable level of safety'.

Both these goals require solutions that can be feasible only if we juggle the five trade-offs above, so there is no such thing as absolute safety. At best it can only be an acceptable level that we are willing to accept or try to achieve.

2.3 Safety segments

For purposes of clarity, we can loosely distinguish between three overlapping segments of safety as shown in Fig. 2.1.



2.1 Three safety segments.

- **Functional safety.** This is part of the overall safety that depends on the system or equipment under consideration operating correctly in response to its inputs. It considers functional hazards caused by loss of intended function, malfunction, response time/accuracy, etc. Systems may be 'safe' in one application, but 'unsafe' in another (e.g. consider loss of altitude display during a clear day, versus the same failure under instrument meteorological conditions (IMCs). Functional safety is strongly connected to system performance and its reliability.
- **Operational safety.** There are safety concerns which are directly related to the type of operations undertaken (e.g. combat missions; deciding to fly with inoperative systems; changing maintenance practices, etc.).
- **Physical safety.** This is usually directly recognisable by examination of the system and operating environment and is strongly connected to the physical characteristics of the components in the system. Physical safety is usually governed by prescriptive health and safety legislation.

2.4 Ensuring safety

There are various methods that can be used (in isolation or in any combination) to achieve satisfactory levels of safety. These methods can loosely be grouped as follows:

- **Informal guidelines.** Safety is achieved by good practice in the form of informal guidelines prepared by persons/parties with an interest in user welfare. Informal guidelines are usually found in products/processes which are non-commercial but where accidents have led to attention. Leisure activities provide numerous applications of this approach (e.g. not flying a kite during a storm, or not using electrical appliances in the bath).
- **Formalised rules.** Some accidents start raising concern and have the potential to affect corporate liability. Organisations thus draft rules, based on past experience, to help users in some specific activity. Examples can be found in company procedures and rules of classification societies.
- **Objective regulations.** Safety is achieved by stipulating the top-level objectives which a system needs to accomplish, whilst leading the methodology (i.e. system architecture and process) up to the applicant. These regulations are often based on past experience (i.e. lessons learned). It is a straightforward and familiar concept.

Compliance with safety standards and requirements can form part of a robust safety argument and facilitate the safety assessment process. Examples can be found in the regulatory activities of the FAA and JAA (see Chapter 3).

- **Prescriptive regulations.** Sometimes strict compliance is desired on a national level, which is then enforced by legal backing. In this case, one party devises formalised regulations/codes on an activity, function, product, process, etc., which are to be obeyed by other parties. These regulations provide a useful point of reference to the inexperienced (e.g. are considered an important mechanism for defining the safety management and design approaches required and to achieve, and to be seen to be achieving, a 'safe' product).

  Examples can be found in many military environments, such as the Military Standards and Defence Standards (see Chapter 3). This approach has similar advantages to the 'objective regulations', and is furthermore favoured by many insurance providers. However, its key weaknesses are that:
  – it often devolves responsibility from the design authority
  – cost implications are not always fully considered
  – it can inhibit innovative thinking because it does not always cater for new technology
  – is often difficult to keep up to date.
- **Established equivalence.** Sometimes established regulations (especially if not objective-based) are too inflexible to deal with new technologies or alternative applications. The alternative solution is thus for the user to demonstrate to the authority that the new product/approach has equivalence to existing approved solutions. A typical example can be found in the certification of unmanned aerial vehicles (UAVs) based on establishing an equivalent level of safety as manned air vehicles.
- **Subjective approach.** Decision-makers consider the range of possible actions and select those that they believe are appropriate for the industry and society. This is a flexible approach that automatically takes account of economical and practical constraints. Unfortunately it has the potential to be inconsistent and open to abuse.
- **Technology-based approach.** The best available technology is selected, regardless of the risk reduction it achieves, and sometimes regardless of cost. It is easy to justify, and so is often used under heavy political pressure. Unfortunately, technology alone cannot solve problems created by technology. New technology may be unproven, not cost-effective, and may introduce new hazards never encountered before.
- **Risk-based approach.** The risk-based approach (see Chapter 4) is used to prioritise risk in such a way that attention is drawn to the most serious situations. Hazards are identified and assessed for the significance of their consequences before focusing on the more important ones.
- **Goal-based approach.** This approach treats safety from basic principles. It manages safety by identifying failures, assessing their severity and allocating appropriate safety levels that need to be systematically accomplished (see Chapter 5). It is often used in completely new situations or modified existing situations.

All these methods have their uses and are applied separately or in conjunction to suit any particular situation. Although the regulatory approaches are dominant, goal-setting and risk-based approaches are becoming more prominent. Chapter 3 will discuss the regulatory approach in more detail, whilst Chapters 4 and 5 will compare the risk-based and goal-setting approaches.

3
Standards and regulations

The nice thing about standards is that you have so many to choose from; further, if you do not like any of them, you can just wait for next year's model.

Andrew Tanenbaum

3.1 Introduction

A regulatory approach is the most common method employed to enforce a required safety standard or, in the case of many military regulations, to enforce a process. Most industrial activities are regulated, and this includes military and civil aviation safety management. Within the context of safety, this chapter explores some of the most widely used regulations used in the western aviation industry and how these influence our approach to safety.

To regulate means to control by rule. From a national perspective, regulation is centred around control of the market place, and the regulators intervene to ensure that certain social objectives are not sacrificed in the pursuit of profit (Johnson, 2003). These objectives include:

- the preservation of consumer rights
- the protection of the environment
- the protection of competition in the face of monopolistic practices
- improvements in safety.

Example

The Federal Railroad Administration's mission statement contains environmental and economic objectives as well as a concern for safety.

'The Federal Railroad Administration promotes safe, environmentally sound, successful railroad transportation to meet current and future needs of all customers. We encourage policies and investment in infrastructure and technology to enable rail to realise its full potential.'

http://www.dot.gov/affairs/1999/fra1899.htm, as reported by Johnston (2003)

Example

A similar spectrum of objectives is revealed in the Federal Aviation Administration's strategic plan for 2000–2001:

'The first of their three objectives relates to safety; they will by 2007, reduce U.S. aviation fatal accident rates by 80 percent from 1996 levels.
The second relates to security; to prevent security incidents in the aviation system.
The final aim is to improve system efficiency; to provide an aerospace transportation system that meets the needs of users and is efficient in the application of FAA and aerospace resources.'

Dembski (1998), as reported by Johnsion (2003)

3.2 Airworthiness

3.2.1 Design standards and airworthiness

The term 'airworthiness' goes by a variety of definitions. However, for the purposes of this chapter, airworthiness will be viewed from the perspective of compliance to one key element of the Certification basis: the Design Standard. Design Standards are aimed at setting out rules and standards that are considered necessary to produce a safe product/system. It tells those involved in the design of a product/system what to strive for, what to do, and what not to do. The driver behind the formulation of Design Standards has always been to maintain an adequate level of safety by learning from historical experience of the participating stakeholders (e.g. authorities, designers, test facilities, accident investigation boards, etc.)

Lloyd and Tye (1995) recall that the airworthiness requirements (e.g. BCAR and FAR) of the mid-20th century 'were devised to suit the circumstances. Separate sets of requirements were stated for each type of system and they dealt with the engineering detail intended to secure sufficient reliability'. Where a system was such that its failure could result in serious hazard, the degree of redundancy (i.e. multiplication of the primary systems or provision of emergency systems) was stipulated. The traditional line of thought was that safety could be ensured by compliance to these predefined Design Standards.

Unfortunately, accidents continued to happen, and it soon became apparent that it was a fallacy to assume that meeting these standards makes the system safe. The reason for this is due to the following limitations inherent in their application:

- Design Standards often do not apply to an entire system and fail to consider the entire life-cycle.
- Design Standards are often reactive, i.e., they are often formulated after the occurrence of an undesired event (the so-called tombstone imperative).
- Design Standards encourage compliance with minimum standards and provide little incentive to consider safety further. In general, they are consensus documents which represent the minimum considered acceptable for systems of a particular type, and often they do not specify the hazard(s) which they are intended to prevent.

These points are further emphasised by Chuck Miller (former head of the Bureau of Aviation Safety) who is known to have said:

> One of the shortcomings of … regulations … is that you can't cover everything. Another is that they tend to classify components, and that's not the nature of

> accidents. Accidents combine these problems with different pieces, or combine the characteristics of these different pieces into an accident. It's called System Safety, and a System Safety approach makes sure that all the pieces fit together and that the interactions between them are adequately covered in some form of hazard analysis.

Standards have other practical limitations as well:

- Many prescriptive standards (see Section 3.3) do not keep up with technology advances (it can be difficult to apply to novel technology) and quickly become inappropriate (i.e., it can limit innovative solutions). As such, standards do not produce an optimal balance between investment and overall safety benefit.
- Standards (especially if too prescriptive) can inhibit innovation, especially when the standards are too explicit in the means of achieving the required functionality (i.e., forces the choice of technology to solve a certain problem).
- Standards are often expressed in a form and format which are not readily usable by industry in generating specifications, acceptance criteria, or compliance matrices.

So why have Design standards? The reason for the existence of Design Standards is that it is important that past experience is used to the benefit of industry and society. From a safety perspective the use of Design Standards provides a framework within which a programme or project can be contracted to, or for a system to operate within. Furthermore, proving compliance to any accepted Design Standard should rightfully form part of any complete safety argument. However, for Design Standards to be useful they need to be constantly updated – especially the prescriptive standards. Dunn (1988) suggests that there are at least three things that make this necessary:

- experience, quite often in the form of feedback from incident and accidents (e.g. new inspection techniques)
- the development of new technology (e.g. fly-by-wire, fly-by-light)
- demand from the market (in terms of safety requirements, societal expectations, etc.).

3.2.2 System safety and airworthiness

System safety is often viewed in the aeronautical industry to be synonymous with the term airworthiness. However:

- airworthiness is concerned with the approved configuration of the aircraft (as at the time of certification) and is primarily focused on the ability of the aircraft to continue safe flight and landing
- system safety is but one element of the entire certification basis and, depending on the system level (see Fig. 8.1) and the regulatory authority (refer to Sections 3.4 to 3.6), may include safety of the aircraft and its on-board systems; safe application of ground-based systems which interface to it either directly or indirectly; all occupational health and safety threats to anyone involved with the aircraft and/or its assemblies.

Table 3.1 briefly compares these two concepts.

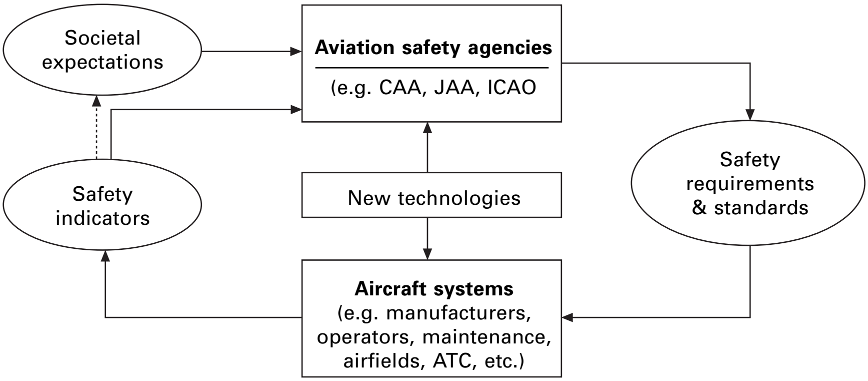
Table 3.1 System safety and airworthiness certification

Airworthiness certification	System safety
The systematic process, during the design of an aircraft or airborne system, of demonstrating conformance to a set of specific and predetermined airworthiness regulations (e.g. FAR25) for a specific type and category of aircraft (as determined by the relevant airworthiness authority).	The systematic process involving: • the justification of functional integrity (see Chapters 4 and 8), and • the identification and resolution of any hazards that can be expected during the system's life-cycle (see Chapters 3 and 9).
Airworthiness regulations driven (e.g. FAR25, FAR23). Strives to show compliance to minimum standards.	Analytically driven. Strives towards the design and operational deployment of a generically safe product, irrespective of any prescribed airworthiness regulations. However, is often required by the Regulations (e.g. FAR1309 and HSWA).
Process is satisfied as soon as it is objectively proven that the laid down regulations and requirements for that specific aircraft type and category have been satisfied. The process is typically concluded with the Authority issuing a Type Certificate	Functional integrity is justified upon certification. However, the resolution of hazards is never satisfied. The Safety Case (refer Ch. 9) continually monitors the design and operational safety risks through a continuous process of hazard identification, and trend monitoring throughout the system's life-cycle.
Terminated upon issuing, by the authority, of the Type Certificate (or, in the case of modification, a Supplemental Type Certificate) for that specific aircraft or airborne system. Reactivated on performing a major modification/repair, or if non-compliance to the conditions in the TC/STC are suspected. Note that airworthiness is considered compromised if the aircraft configuration differs from that specified in the approved TC/STC.	Depending on contractual arrangements the System Level 1-4 (see Fig. 8.1) analysis usually stops upon the issue of the final Safety Assessment. The Safety Case (System Level 5/6, see Fig. 8.1) remains active during the whole of the product lifecycle and calls for continuous and careful engineering management, usually via some sort of safety management system.[1]

[1] With reference to Fig. 8.1, it can be noted that some Regulatory requirements can be matched against the System Hierarchy. For instance, it can be argued that JAR OPS 1 is pitched at System Level 7; JAR/FAR/CS25 is pitched at System Level 4; AC25.11 is pitched at System Level 3.

3.3 Source of regulations

Regulation is affected by many means, including an increasingly vociferous society, politicians, economic factors, international relations and, without doubt, the law (Williams, 2003). A simple high-level model of aviation safety regulation is depicted in Fig. 3.1. This model shows the interaction between the industry and the regulatory



3.1 Safety regulation model (adapted from Perry (1988) page 17).

authorities and recognises the 'input' from the public in the form of 'societal expectations'.

Regulating involves using Regulations/Orders/Directives, Design Standards, as well as Advisory/Guidance material. All of these often fall under the blanket term 'regulations'. They are meant to be easily understood, are often legally enforced, and apply to a variety of products and installations. However, the resulting regulations/standards vary in the rigour of their application and/or enforcement. We can broadly make the following distinctions:

- Prescriptive regulations[1] usually prescribe that certain process/product features must be present, or that the process is performed in a certain way. These 'strict' standards may involve additional development costs, for given levels of safety, through requiring unnecessary additions to, or changes to, an organisation's products and/or processes. So, they may not deliver the safest solution for a given cost (Falla, 1997) or result in any safety improvement.
- Objective regulations[2] are also usually prescriptive, but about relatively abstract features of the process/product. These standards are intended to ensure that a product/process has certain essential properties. A standard might, for instance, specify that a certain safety objective be met (or that audit trail must be provided) without specifying how it is to be done. These standards are intended to avoid over-constraining industry and allow different solutions and also the evolution of solutions. These 'loose' standards should in theory allow the most cost-effective compliance, through minimising unnecessary prescription and allowing maximum flexibility in ways to comply with those aspects which are prescribed. However, both the implementation of these standards and the assessment of compliance to them require greater judgement, and often greater experience of the responsible individuals, to determine what is an appropriate interpretation in a given situation. It is also possible to misinterpret the intentions of the requirements and to implement them in a less than satisfactory way.

[1] Prescriptive requirements are commonly led by the auxiliary verb 'shall' or 'will'.

[2] Objective requirements are also commonly led by the auxiliary verb 'should'.

- Guidance/advisory material[3] comes in the form of industry best practice. It usually supplements the prescriptive and objective standards and is intended to provide guidance on how those requirements can be accomplished. It provides a means of compliance but, most importantly, not the only means of compliance.

In practice, most standards contain some elements of each of these styles, for instance:

- IEC 1508 contains different parts, one with the mandatory high-level standards and the other with guidance on specific ways in which the high-level standards might be satisfied
- the JAR/FAR/CS differentiates between regulations (i.e. the prescriptive bit) and advisory material that provides a recommended means of meeting the regulation.

Each endeavour undertaken to design, certificate, support, maintain and operate aircraft fall under the standards and regulations of a regulatory authority. In order to assist entry into market and to reduce costs, it is vital that those involved with these endeavours have an understanding of the various 'bodies' involved in the market. Sections 3.4 to 3.6 will briefly summarise the key authorities in the western hemisphere.

3.4 Civil regulatory authorities

3.4.1 Background

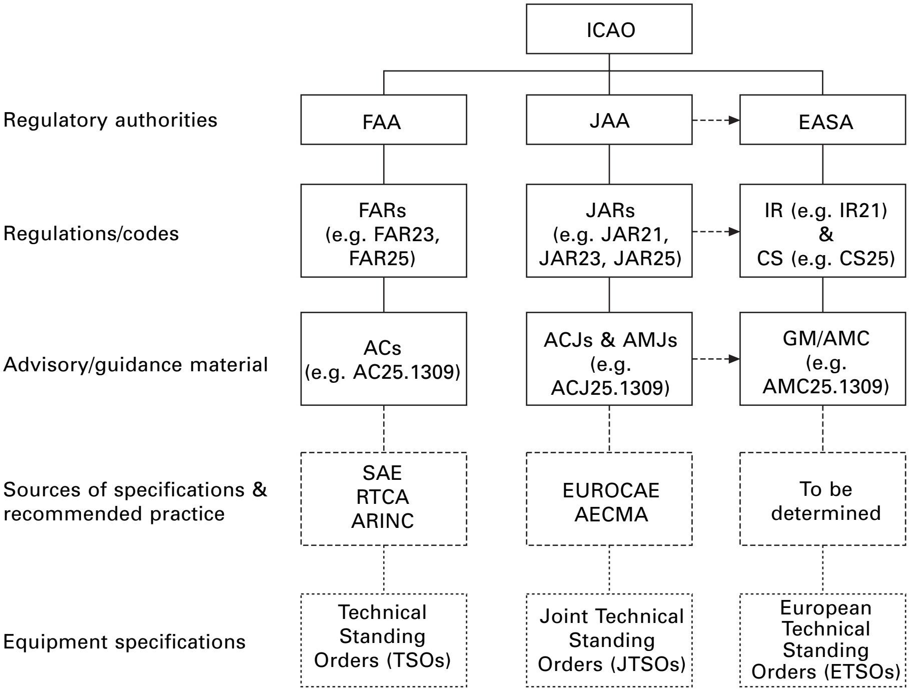
Most nations have their own civil aviation regulatory body (e.g. the UK CAA, French DGAC, Australian CASA). These exist generally in five main categories:

1. Those that are totally independent and rigidly apply their own national airworthiness requirements, e.g., the USA applying Federal Aviation Regulations (FARs) via the Federal Aviation Administration (FAA).
2. Those subject to multinational government agreements where a standardised set of requirements has been established and certification by one participant national authority is accepted by all other participant nations (e.g. JAA and EASA).
3. Those nations that have competent authorities but who, for the purposes of efficiency, chose to adopt (selectively, or wholeheartedly) the regulations of another larger authority such as the FAA/JAA/EASA.
4. Those subject to international government bi-lateral agreements where, by arrangement, one authority can deputise for another.
5. Those, usually small nations, who accept certification by a larger nation.

Most civil aviation authorities co-operate at some level, and are subject to international agreement. They apply similar standards to airworthiness and safety. Their interpretations may vary and 'Special Conditions' may apply, but the foundations are generally based on the requirements of the International Civil Aviation Organisation (ICAO). Figure 3.2 diagrammatically illustrates the relationships between the key aviation regulations in the USA and Europe.

Both the preparation of new regulations and the development of changes to existing

[3] Guidance/advisory material is commonly led by the auxiliary verb 'should'.


ICAO
Regulatory authorities
FAA
JAA
EASA
Regulations/codes
FARs (e.g. FAR23, FAR25)
JARs (e.g. JAR21, JAR23, JAR25)
IR (e.g. IR21) & CS (e.g. CS25)
Advisory/guidance material
ACs (e.g. AC25.1309)
ACJs & AMJs (e.g. ACJ25.1309)
GM/AMC (e.g. AMC25.1309)
Sources of specifications & recommended practice
SAE RTCA ARINC
EUROCAE AECMA
To be determined
Equipment specifications
Technical Standing Orders (TSOs)
Joint Technical Standing Orders (JTSOs)
European Technical Standing Orders (ETSOs)

3.2 Civil aviation safety regulation hierarchy (adapted from Perry (1988) page 17).

regulations are carried out by the civil aviation authorities through a process that involves detailed consultation with the interested parties in the aviation industry, via specialist working groups. Such additions and changes are then published for wider comment as Notices of Proposed Amendments (NPA) in Europe, and Notices of Proposed Rulemaking (NPRM) in the United States of America.

3.4.2 International Civil Aviation Organisation (ICAO)

International civil aviation is governed by the Convention on International Civil Aviation (commonly known as the Chicago Convention). Under this Convention, the International Civil Aviation Organisation (ICAO), a specialised agency of the United Nations, sets the minimum Standards and Recommended Practices for international civil aviation. These standards are contained in 18 Annexes to the Convention. Of particular interest, in the context of system safety, are:

- Annex 6 covering operation of aircraft
- Annex 8 covering airworthiness of aircraft, which is supported by the *ICAO Airworthiness Manual* (within the context of system safety, note especially Volume II, *Design Certification and Continued Airworthiness*)
- Annex 10, which contains five volumes covering aeronautical telecommunications.

The responsibility for implementing Annexes 1 and 18 rests with the State of Registry (i.e. the State in which the aircraft is registered). The responsibility for implementing Annex 6 rests with the State of Operator (i.e. the State in which the airline is based). Often the State of Operator and the State of Registry will be the same, as airlines tend to operate aircraft registered in the State in which they are based.

ICAO has six strategic objectives:

- safety
- security
- environmental protection
- efficiency
- continuity
- rule of law.

The strategic objectives are action oriented and present a range of activities which include development, implementation and technical support.

All countries[4] who export aircraft or operate international flights are required to conform to standards, regarding design and operation, which satisfy the ICAO guidelines (Perry, 1998). Every country is entitled to develop its own requirements to satisfy the ICAO objectives. However, most countries use and/or accept, either directly or with their own modifications and/or additions, either the European Joint Aviation Authority (JAA) or the United States Federal Aviation Administration (FAA) Requirements/ Regulations, Joint Aviation Requirements (JAR) and Federal Aviation Regulations (FAR) respectively. Some countries, such as Canada, publish their own airworthiness codes that are similar, but may not be identical, to the corresponding JARs/FARs.

Among its many other activities, ICAO also (Perry, 1998):

- monitors accident investigations worldwide and provides guidance on continued airworthiness
- monitors compliance with internationally agreed Safety and Recommended Practices (SARP), in particular through its Safety Oversight Programme
- issues a wide variety of technical, economic and legal publications as well as films, video tapes, slides, diskettes and posters. These are designed to assist government authorities, manufacturers and operators in the civil aviation community to ensure safe, orderly and efficient air transport systems worldwide.

While the average designer will not normally be directly involved with these activities (since these are usually handled at national level), ICAO does set the requirements, applicability and implementation dates for major international standards that affect worldwide operation and safety.[5] Thus, from a future products point of view, awareness of these activities is desirable. For more information on ICAO, see:

- http://www.icao.int/
- http://www.ariane-info.com/ ICAO%20Annexes%20to%20the%20Conventions%20SARPS.htm

[4] For a list of contracting states, see http://www.icao.int/cgi/goto_m.pl?/cgi/statesDB4.pl?en

[5] Current examples of these include Future Air Navigation System (FANS); Ground Proximity Warning System (GPWS) and Instrument Landing System/Microwave Landing System/Global Positioning System (ILS/MLS/GPS).

3.4.3 Federal Aviation Administration (FAA)

In the USA, the Federal Aviation Act of 1958 created the agency (under the name Federal Aviation Agency) and adopted the present name in 1967 when it became a part of the Department of Transportation. The major roles of the FAA include[6]:

- regulating civil aviation to promote safety by:
  - issuing and enforcing regulations and minimum standards covering manufacturing, operating, and maintaining aircraft
  - certifying airmen and airports that serve air carriers
- encouraging and developing civil aeronautics, including new aviation technology
- developing and operating a system of air traffic control and navigation for both civil and military aircraft by:
  - developing a safe and efficient use of navigable airspace
  - operating a network of airport towers, air route traffic control centres, and flight service stations
  - developing air traffic rules, assigning the use of airspace, and controlling air traffic
  - building/installing/maintaining/operating/auditing visual and electronic aids to air navigation
  - sustaining other systems to support air navigation and air traffic control, including voice and data communications equipment, radar facilities, computer systems, and visual display equipment at flight service stations
- researching and developing the National Airspace System and civil aeronautics
- developing and carrying out programmes to control aircraft noise and other environmental effects of civil aviation
- regulating US commercial space transportation
- promoting aviation safety and encouraging civil aviation abroad by:
  - exchanging aeronautical information with foreign authorities
  - certifying foreign repair shops, airmen, and mechanics
  - providing technical aid and training
  - negotiating bilateral airworthiness agreements with other countries
  - taking part in international conferences
- regulating and encouraging the US commercial space transportation industry. The FAA license commercial space launch facilities and private launches of space payloads on expendable launch vehicles
- conducting research on, and developing, the systems and procedures needed for a safe and efficient system of air navigation and air traffic control. Helping to develop better aircraft, engines, and equipment and testing or evaluating aviation systems, devices, materials, and procedures; also conducting aeromedical research
- registering aircraft and recording documents reflecting title or interest in aircraft and their parts. Administering an aviation insurance program, developing specifications for aeronautical charts, and publishing information on airways, airport services, and other technical subjects in aeronautics.

[6] Refer http://www.faa.gov/about/mission/activities/ (dd 15-08-2005)

Of particular interest, in the context of system safety, are FAR25.1309 (for large aeroplanes) and FAR23.1309 (for normal, utility, aerobatic and commuter category aeroplanes). Both of these require some form of System Safety Assessment as the means of proving compliance. For more information on the FAA, see http://www.faa.gov/

3.4.4 Joint Aviation Authorities (JAA)

Industry continually has a paramount need for common international requirements relating to safety regulation. This is so that aircraft can be built and maintained to agreed and known standards, thus avoiding different national requirements for certification and enabling the relatively easy transfer of aircraft and their equipment.

According to Ashford (1994) 'A lack of harmonised safety regulations in all fields increases costs, works against a "level playing field" commercially, causes complications and delays in certification and approvals and can affect operating costs.' In the European aviation industry this led to the goal of a single certification (so removing national variants), thus the formation of the Joint Aviation Authority (JAA) whose activities started in 1970,[7] with inputs from the Federal Aviation Authority.[8]

The JAA Membership is based on the 'JAA Arrangements' document originally signed by the then current member states in Cyprus in 1990. The Joint Aviation Authority (JAA) is an associated body of the European Civil Aviation Conference (ECAC) representing the civil aviation regulatory authorities of a number of European States who have agreed to co-operate in developing and implementing common safety regulatory standards and procedures. This co-operation is intended to provide high and consistent standards of safety and a 'level playing-field' (i.e. a uniform standard of requirements) for competition in Europe.[9] The JAA's key objectives[10] are as follows:

- **Aviation safety.** To ensure, through co-operation amongst member states, that JAA members achieve a high, consistent level of aviation safety.
- **Transition from JAA to EASA.** To ensure the highest level of contribution to the European Union for establishing a European aviation safety agency that would absorb all functions and activities of the JAA in as short a period as possible and would ensure the full participation of the JAA in non-EU member states.
- **Business effectiveness.** To achieve a cost effective safety system in order to contribute to an efficient civil aviation industry.

[7] The JAA's work started in 1970 (when it was known as the Joint Airworthiness Authority). Originally its objectives were only to produce common certification codes for large aeroplanes and for engines. This was in order to meet the needs of European industry and particularly for products manufactured by international consortia (e.g. Airbus).

[8] In general the JARs use the same numbering system as the FARs and are written in the same format. While a lot of effort is being made to 'harmonise' these codes, there are differences and these are identified in the JARs (but not in the FARs), by underlined text.

[9] From the start, much emphasis was always placed on harmonising the JAA regulations with those of the US.

[10] See http://www.jaa.nl/introduction/introduction.html

- **Consolidation of common standards.** To contribute, through the uniform application of common standards and through regular review of existing regulatory situations, to fair and equal competition within member states.
- **World-wide aviation safety improvement.** To co-operate with other regional organisations or national authorities of states who are playing an important role in civil aviation, in order to reach at least the JAA safety-level and to foster the worldwide implementation of harmonised safety standards and requirements through the conclusion of international arrangements.

As is evident from the second objective, the JAA became a 'gentlemen's club' with JAR compliance voluntary. Legal standing for the JARs was provided by the National Approval Authorities (NAA) in each member country (e.g. the UK CAA, or the French DGAC). Unfortunately, despite the 4th objective above, this often led to the NAA's adding their own supplemented requirements. The only way to give JARs the backing of law was for the European Community to legislate to adopt a common set of requirements. This process led to the formation of EASA, which will eventually totally replace the JAA. For more information on the JAA, see http://www.jaa.nl/

3.4.5 European aviation safety agency

The European Parliament and the Council of the European Union (EU) established the European Aviation Safety Agency (EASA) via Basic Regulation (EC) No 1592/2002 of 15 July 2002.[11] With the adoption of the Basic Regulation (EC) a new regulatory framework (on common rules) was created in the field of European civil aviation. EASA became an agency of the European Union which has been given specific regulatory and executive tasks in the field of aviation safety. EASA thus became responsible for the airworthiness and environmental certification of products, parts and appliances for the majority of the civil aircraft registered in the member states of the European Union (EU). According to this Regulation, from 28 September 2003, EU Member States' national regulations have been replaced by EU Regulations, and certification tasks have been transferred from National Authorities to EASA.

The EASA rules for continuing airworthiness will be implemented at staged intervals over the next five years. Where EASA rules are not yet in place the national requirements of member states still apply.

[11] The Basic Regulation was twice amended by 'enabling legislation':

- Regulation (EC) 1643/2003 of 22 July 2003 amending Regulation (EC) No 1592/2002: this amendment brings the Basic Regulation into line with Regulation 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (which sets out the financial procedures applying to all EU institutions and agencies) and Regulation 1049/2001 of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (which sets out the public's right of access to documents created by, or held by all EU institutions and agencies).
- Regulation (EC) 1701/2003 of 24 September 2003 adapting Article 6 of Regulation (EC) No 1592/2002: Article 6 of the Basic Regulation refers to Annex 16 to the Chicago Convention. This annex has itself been amended since the adoption of the Basic Regulation in July 2002 and therefore a corresponding change is necessary to the reference in the Basic Regulation.

Example: The UK CAA

CAA Specifications and Airworthiness Notices contain:

- operational requirements
- maintenance requirements
- design requirements.

Due to the staged nature of the transition to EASA, the maintenance and operational aspects of the CAA Specifications and Airworthiness Notices will continue to be applicable to all aircraft with UK certificates of airworthiness (including both new and used aircraft at C of A issue) when compliance with ANO Articles 8 and 9 and paragraphs 630 and 890 of JAR-OPS 1 and 3 is required. This applicability will remain until UK requirements are superseded by EASA requirements.

Aircraft that are outside the scope of the EASA Regulation will continue to be regulated under UK national procedures.

[http://www.caa.co.uk/srg/easa/default.asp, 6/7/05]

The agency's mission is twofold:

- to provide technical expertise to the EU by assisting in the drafting of aviation safety rules and providing technical input to relevant international agreements
- carry out certain executive tasks related to aviation safety, such as the certification of aeronautical products and organisations involved in their design, production and maintenance. These certification activities help to ensure compliance with airworthiness and environmental protection standards.

  The Basic Regulation is supported by a set of Implementation Regulations:

- **IR Certification:** Commission Regulation (EC) No. 1702/2003 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations.
- **IR Maintenance:** Commission Regulation (EC) No. 2042/2003 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks.

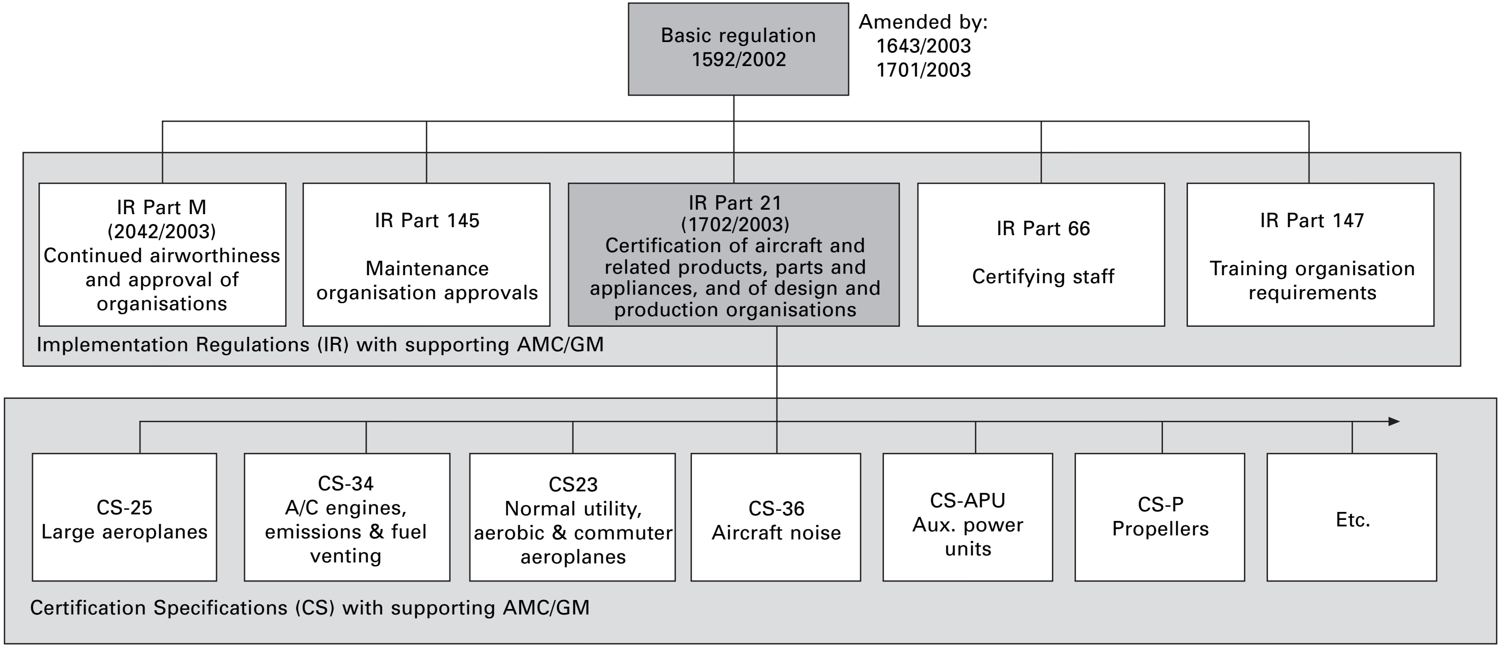
The regulatory hierarchy of EASA Design Standards is illustrated in Fig. 3.3.[12] Of particular interest, in the context of system safety, are CS25.1309 and CS23. Both of these require a system safety assessment as the means of proving compliance. For more information on the EASA, see http://www.easa.eu.int/home/regul_en.html

3.5 Military regulatory authorities

3.5.1 General

Unlike the civilian aircraft industry, the military industry is both the operator and

[12] See http://www.easa.eu.int/home/regul_en.html


Basic regulation
1592/2002
Amended by:
1643/2003
1701/2003
IR Part M
(2042/2003)
Continued airworthiness and approval of organisations
IR Part 145
Maintenance organisation approvals
IR Part 21
(1702/2003)
Certification of aircraft and related products, parts and appliances, and of design and production organisations
IR Part 66
Certifying staff
IR Part 147
Training organisation requirements
Implementation Regulations (IR) with supporting AMC/GM
CS-25
Large aeroplanes
CS-34
A/C engines, emissions & fuel venting
CS23
Normal utility, aerobic & commuter aeroplanes
CS-36
Aircraft noise
CS-APU
Aux. power units
CS-P
Propellers
Etc.
Certification Specifications (CS) with supporting AMC/GM

3.3 EASA regulatory hierachy.

regulator of their aircraft – albeit in a separate department. Military aircraft operate under state prerogative and are thus usually the responsibility of the appropriate Ministry/Department of Defence. From a system safety point of view, this combined regulator/operator function presents at least two unusual challenges compared to the civil aviation industry:

- The System Safety Assessment (SSA, see Chapter 8) conducted during System Certification is available to the operator – and is expected to form a key part of the operator's Safety Case (see Chapter 9). In the civil arena, the SSA is generally deliverable only to the certification authority and is usually not released into the public domain.
- Being both the operator and the regulator, the Safety Case (see Chapter 9) is not only concerned with Safety Certification and Continued Airworthiness, but also with Occupational Health and Safety (see Section 3.6).

The remainder of this section will explore some of the approaches taken by different military authorities.

3.5.2 US military

In the early 1990s, the US military acquisition process was subject to more that 1,700 different prescriptive Military Standards/Specifications. In 1994 the (then) US Secretary of Defence, William J. Perry, issued a directive:[13] Instead of using Military Specification and Standards the policy was changed to procure against 'performance specification' (or objective regulation, see Section 3.1 above) as the new norm (i.e. what the product is to do, not how it should be made). The idea was to cut costs, and increase innovation by the use of commercial equipment and standards. The use of Military Standards is authorised only as a last resort.

MIL-STD (Military-Standard) or MIL-SPEC (Military-Specifications) is an abbreviation used to describe an item that can meet standards determined by the United States Department of Defense. A MIL-STD can also be documentation which lists and explains a compilation of prerequisites and standards that an item must meet for DoD acceptance. For example, a MIL-STD can be expressed as MIL-STD-X, in which the 'X' is a set of numbers or numbers and letters which designate a specific standard.

Of particular interest, in the context of system safety, is MIL-STD-882[14] and MIL-

[13] See http://www.sae.org/standardsdev/military/milperry.htm and http://www.defenselink.mil/releases/1994/b111094_bt645-94.html

[14] MIL-STD-882D (System Safety Program Requirements) provides requirements for developing and implementing a system safety programme to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing risks. It applies to every activity of the system life cycle, e.g., research, technology development, design, test and evaluation, production, construction, checkout/calibration, operation, maintenance and support, modification and disposal. Twenty-two tasks are defined in the areas of programme management and control and design and evaluation. Typical tasks are system safety programme plan, preliminary hazard analysis, and software hazard analysis. An appendix is provided to give some rationale and methods for satisfying the requirements previously detailed.

STD-810.[15] It is interesting to note that many projects still contract against the requirements of MIL-STD-882, which (at issue D) is still procedurally very prescriptive. For more information on US Military standards, see: http://dodssp.daps.dla.mil/ and http://www.defenselink.mil

3.5.3 UK Ministry of Defence

Policy and requirements for the management of safety and environment in relation to the equipment and services the MoD procure, support and operate can be found in a series of Joint Service Publications (JSP) published by the MoD Functional Safety Boards:

- The Safety Health Environment and Fire Board (SHEFB) publish the following top-level policy statements of the Secretary of State:
  - JSP 375 *MOD Health and Safety Handbook*
  - JSP 418, *Safety, Health and Environmental Protection in the Ministry of Defence*.

A key element of the policy is that the MoD complies with the requirements of the Health and Safety at Work, etc., Act (1974) and other relevant legislation (see Section 3.6 below). The main purpose of the Health and Safety at Work, etc., Act is to ensure that employers provide a safe working environment for their employees. In the case of the MoD, the latter includes both civilian and service personnel.

- The Defence Aviation Safety Board (DASB) publish[16] the following regulations:
  - JSP 550, *Military Aviation Policy, Regulations and Directives*
  - JSP 551, *Military Flight Safety Regulations*
  - JSP 552, *Military Air Traffic Service Regulations*
  - JSP 553, *Military Airworthiness Regulation*. This document describes the Safety Management System for the management and regulation of military aircraft airworthiness; it contains mandatory requirements, advice and guidance. It is intended for all staff concerned with the airworthiness and safety of all UK military aircraft, their equipment, and air-launched weapons; it addresses policy, the acquisition process, the preparation of Military Aircraft Release, the Aircraft Document Set, the Release to Service and the management of change in-service.
  - JSP 554, *Military Aviation Aerodrome Criteria and Standards*
  - JSP 556, *Military Test Flying Regulations*
  - JSP 558, *Military Aviation Diplomatic Approvals and Clearances.*

[15] MIL-STD-810E (Environmental Test Methods and Engineering Guidelines) standardises the design and conduct of tests for assessing the ability of military equipment to withstand environmental stresses which it will encounter during its life cycle, and to ensure that plans and test results are adequately documented. This document provides guidelines for conducting environmental engineering tasks and provides test methods for determining the effects of natural and induced environments on equipment used in military applications. Included in the numerous types of tests detailed are purpose, environmental effects, guidelines for determining test procedures and test conditions, references, apparatus, preparation for test, procedures, information to be recorded.

[16] http://www.ams.mod.uk/ams/content/docs/jsp553.htm

- The Ship Safety Board (SSB) publishes JSP 430, *Ship Safety Handbook*
- The Land Systems Safety Board (LSSB) publishes JSP 454
- *Land Systems Safety Assurance Procedures*
- The Defence Ordnance Safety Board (DOSB) publishes JSP 520, *Ordinance, Munitions & Explosives Safety Management System*
- Defence Nuclear Safety Board (DNSB) publishes
- JSP 518, *Regulation of Naval Nuclear Propulsion Programme* and
- JSP 538, *Regulation of the Naval Nuclear Weapons Programme.*

To comply with the Secretary of State's policy, the MoD needs to ensure that the management and technical standards that are adopted are consistent with best civil and international standards. To achieve maximum harmonisation it is therefore MoD policy to utilise international standards where appropriate and an agreed (refer, *inter alia*, JSP 520 para 0109) hierarchy is as follows:[17]

- European Union civil standards
- International civil standards
- UK civil standards
- Standardized NATO Agreements (STANAGs)
- UK Defence Standards.

In the context of system safety, the following Defence Standards are of particular interest:

- DEF-STAN 00-56 (Safety Management Requirements for Defence Systems), which revolves around safety management requirements that the MoD apply to all their platforms (e.g. tanks, aircraft, ships, etc.). Not dissimilar to the MIL-STD-882 approach, the UK MOD also contracts to DEF-STAN 00-56, which requires a 'Safety Case' (it refers to a contractor assisting the MoD with managing through-life safety) and which defines safety in terms of reducing the risks of 'Harm to human life (including MoD employees and the general public); material loss; and environmental damage'.
- DEF-STAN 00-55 (Requirement for Safety Related Software in Defence Equipment), which again applies to all MoD platforms. This standard is often discarded in favour of the more internationally recognised RTCA-DO-178B.

For more information of Defence Standards, see: http://www.dstan.mod.uk/ and http://www.ams.mod.uk/

3.6 Health and safety regulations

The topic of safety revolves around ensuring that equipment provided will not endanger the health and safety of the user or the general public. All operators and facilities are subject to the health and safety statutory and common law duties which management owes their employees and the general public.

During any acquisition project, an essential condition of compliance with these duties is compliance on the part of designers and manufacturers with health and

[17] http://www.ams.mod.uk/ams/content/docs/dosgweb/sms/jsp520/cov.pdf

safety specifications and procedures intended to ensure the safety of the product. Monitoring and enforcement of this compliance does not fall within the remit of any aviation safety authorities (who are primarily interested in technical airworthiness), but falls into the lap of the relevant Health and Safety Regulator in each particular country.[18]

Health and Safety legislation has a direct effect on the responsibility, authority, accountability and liability towards the safety management approach of any operator. It explicitly requires the operator to assess and manage the risk (which includes technical airworthiness risk) during the lifetime of the product/facility. This proactive approach is the backbone of current harmonised European Safety, Health and Environmental Standards and Regulations; the term 'reasonably practicable' enshrined in this act is interpreted as a balance between risk and cost.

The principal health and safety legislation in the UK is the Health and Safety at Work, etc., Act 1974 (HSWA). This sets out in general terms the health and safety duties of employers, employees, and manufacturers, suppliers and designers of articles for use at work. Health and safety regulations under the HSWA are generally supported by guidance and sometimes by an approved code of practice (ACOP). Safety standards have a similar effect in law to an ACOP. Failure to comply with a safety standard may be taken as evidence of a breach in the HSWA (JSP 553 Ch 1 page 3), which is a statutory offence and could also lead to common law liability.

Section 6 of the HSWA places particular duties on designers, manufacturers, importers and suppliers of equipment. The MoD acquisition community can assume several of these roles and are therefore fully subject to a number of associated duties. One of these is: 'To ensure, as far as reasonably practicable that the article is so designed and constructed so as to be safe, and without risks to health'.

Depending on the type of project or equipment it may be necessary to consider whether additional legislation applies, for example:

- The Merchant Shipping Act 1995
- The Civil Aviation Act 1982 (which refers to the applicable aviation safety regulator)
- The Road Traffic Act 1991
- The Explosives Act 1875
- The Supply of Machinery (Safety) Regulations 1992.

The Management of Health and Safety at Work Regulations 1992 sets out management responsibilities to demonstrate that all risks associated with work activities (which includes the maintenance and operation of aircraft) are reduced to a level that is as low as reasonably possible (T853, Block 3 Part 5 pp. 4–8). The emphasis in post-1992 legislation is on developing the 'safety case' approach, which demonstrates that an organisation has implemented a risk management system, and that the goal of 'all risks are reduced to a level that is ALARP' (as low as reasonably practicable) is

[18] It is emphasised that all the material in the JARs and the FARs relate to aircraft safety only. The other aspects of personnel safety (i.e. risk of injury/death other than during the flight phase); commercial performance; and related requirements at airframe, system and equipment levels are covered by the commercial specifications from the operators and the airframe constructors, who will also require that the appropriate safety requirements are satisfied.

achieved. So, since 1992 a Risk Assessment Approach (see Chapter 9) has become the cornerstone of all UK health and safety legislation and Standards. For more information of the UK HSWA, see http://www.hse.gov.uk

3.7 The impact on organisations

For many organisations, certification as a contractual obligation has been largely limited to a requirement to meet certain recognised Standards. This often leads to the following recurring issues:

- The manner in which compliance to a Standard is demonstrated. Proving compliance (e.g. by analyses or tests) down to paragraph level is costly and time consuming.

  Criticism is often levelled at the authorities regarding the cost of safety certification. While this, in some cases, is justified, the constructors do not always make life as easy in this respect as they could. The concepts of 'Certification by Design' and 'Design for Certification' should be borne in mind since they offer a way not only towards optimising the certification process but also improving the system design and hence reducing costs.
- For international programmes, to design and build equipment to different certification requirements means either to build to the 'envelope' of the requirements or build to different standards. A lack of harmonised safety regulations/requirements increases costs (contract sunk costs as well as other product lifecycle costs), works against a 'level playing field' commercially and causes complications and delays in certification.

  As industry has to operate outside the boundaries of any one authority's jurisdiction, it has a fundamental need for the harmonisation of requirements over as wide a sphere of influence as possible. This has been the fundamental driver in the establishment of the JAA and EASA. However, industry has to be the facilitator or catalyst for any harmonisation activity. It has to be an active participant, i.e., an intervener, not just an acceptor (Senker, 1990), in this process to ensure that the engineering difficulties and the cost associated with achieving an adequate level of safety can be accurately assessed.
- For the aircraft industry to benefit from emerging technologies, affordability and effectiveness of these innovations depends on clarifying and simplifying certification processes:
  - It is argued that the William J. Perry approach (refer Section 3.5.2) requires more initial effort to define the performance but less in evaluating the responses and allows the industry to offer solutions based on their strengths. Hence the realisation that suppliers should be given a performance requirement, i.e., what the product is to do, not how it should be made.
  - The aerospace industry shows a decreasing reliance on defence-unique requirements and a greater reliance on the commercial market. The emphasis of the integration of commercial and military development ensures that the strengths of industry are used where possible. Where an application is not purely military there should be no need for a unique military specification.

Aircraft systems will become increasingly complex in the years to come and hence increasingly difficult to monitor and govern. However, at the same time there will be increasing convergence of technology, economics, environment, safety, regulatory regimes, etc. This combination of complexity and convergence means an increasing global need for information co-operation with a real need for world-wide information sharing and co-operation.

3.8 The impact on safety management systems

Jenkins (1999, p. 10) warns that the impact of a regulatory style on the form of Safety Management System (SMS) cannot be underestimated. When the SMS process is enforced by rules, instructions, externally imposed physical and operational standards, etc., there is little room for innovation or discretion. There is an ever-present danger of creating separate formal policies to respond to each regulator or to each new hazard.

At a strategic level, the safety aspirations and principles (policies) are common to all processes and hazards, whilst at the detailed or activity level the implementation is specific and tailored to the process and hazard. If a manager has a good grasp of what the fundamental principles are, then it is no longer necessary to develop too many different processes for delivering that principle in order to achieve good safety performance.

3.9 Discussion

Standards and Regulations provide the basis of a consistent approach to a project, but must:

- be underpinned by a sound and extensive knowledge base (i.e. using data to drive decisions)
- the regulations must be separated from information that is advisory
- be based on cost-benefit analysis (Senker, 1990)
- consult industry at the earliest stages of rulemaking (Senker, 1990).

Because authorities are moving from high levels of direct intervention towards industry accountability, industry must be empowered by:

- requiring organisations to have self-correcting internal systems
- becoming interveners (instead of acceptors) in the formulation of policy and standards.

Nationally and internationally, industry and authorities (civil and military) need to collaborate with a prime objective of minimising certification costs, engender a safety culture and achieve safety goals. This will require (Senker, 1990):

- a convergence of definitions and terminology (common understanding)
- clear goals and a consistent approach
- have regard to public expectations for increasing levels of safety.

Markey (1994) warns that we should learn from mistakes, but must always be mindful of resorting to reactive legislation only when it is unavoidable, and after careful consideration of the cost and risk factors involved. So, although engineering codes, standards and regulations are necessary for design, and in many countries their use is required by law, they are insufficient for hazard identification and need to be supplemented by other techniques. Rather than placing reliance on the regulatory system alone, this will require the adoption of disciplined and systematic safety assessment and safety management methodologies to guide us through the safe application of complex technologies of the future.

4
Risk-based approach

Be wary of the man who urges an action in which he himself incurs no risk.

Joaquin Setanti

4.1 Introduction

Risk management is a concept applied as part of a decision-making process, and can also be explained[1] as follows:

A process …

Risk-based decision making involves a series of basic steps. It can add value to almost any situation, especially when the possibility exists for serious (or catastrophic outcomes). The steps can be used at different levels of detail and with varying degrees of formality, depending on the situation.

… that organizes information about the possibility for one or more unwanted outcomes …

This information about the possibility for one or more unwanted outcomes separates risk-based decision making from more traditional decision making. These unwanted outcomes can be project, market, mission and/or safety related.

… into a broad, orderly structure …

Most decisions require information not only about risk, but also about other things as well. This additional information can include such things as cost, schedule requirements and public perception. In risk-based decision making, all of the identifiable factors that affect a decision must be considered. The factors may have different levels of importance in the final decision.

… that helps decision makers …

The only purpose of risk-based decision making is to provide enough information to help someone make a more informed decision. The information must therefore be compiled and presented in a consistent (e.g. the safety criteria applied) and user-friendly fashion (e.g. a Hazard Log) to ensure that 'apples are not compared with pears'.

… make more informed management choices …

The objective of risk-based decision making is to help people make better, more logical choices without complicating their work or taking away their authority.

[1] Tailored from http://www.uscg.mil/hq/g-m/risk/e-guidelines/html/vol2/01/v2-01-01.htm#1 during 2002 (author unknown, no longer available).

The business world usually distinguishes between:

- project risk (e.g. failure to meet specification/schedule)
- marketing risk (e.g. inappropriate product, not being the dominant design)
- business risk (e.g. financial risk of insufficient cash flow, or legal risk of being sued)
- insurance risk (e.g. risk of theft, damage to property or unexpected medical bills).

Conventionally, risk deals with uncertainty in project appraisal, project management and financial performance. However, when it comes to safety, we also have to add safety risk as another factor. Although it can be argued to fall under project risks, it has a different slant to it. A product may meet the specification, be on time and within cost, but that does not mean to say that it is safe. Note that safety is also closely connected with the other sorts of risk (e.g. an accident can affect insurance and business risk) and the prudent manager thus needs to ensure that safety is given due attention.

4.2 Defining risk

When it comes to safety, many interpretations exist when we use the term 'risk'. For instance:

- risk is the chance of achieving a certain, usually negative, outcome; or
- risk means the same as hazard; or
- risk is the consequence of failure; or
- risk is the same as danger; or
- risk is about taking chances.

The concept of risk starts from the premise that perfect safety (i.e. complete freedom from harm) is not achievable for all but the simplest systems (David, 2002). Risk is the measure which allows different safety concerns to be compared according to how serious they are. But how do we make decisions regarding risk?

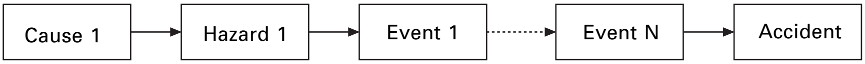
For the purposes of establishing objective evaluation criteria, an appropriate definition of 'risk' is taken from ISO/IEC Guide 51 (1999): 'Risk is the combination of the probability of occurrence of harm and the severity of that harm'. This implies that risk can be expressed as the combined effect of the probability of occurrence of an undesirable event, and the severity of the consequence of that event. This can be expressed mathematically as follows:

$$R = S \times P$$

where R = risk, S = severity of the consequence, P = probability of occurrence of the consequence. Please note that risk is estimated on the *probability of occurrence of the consequence*. The consequence is the undesired event and is usually some sort of accident.

In any accident there is rarely only one single cause. Generally there are a number of causes (e.g. failures) and events (i.e. pilot error) which combine like links in a chain to create an accident. This concept is illustrated in Fig. 4.1.

So, to estimate risk we are thus not only interested in the probability of a specific



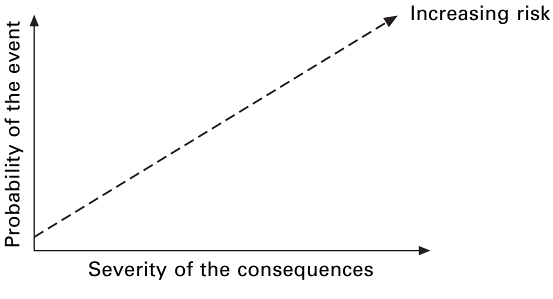
4.1 Simple accident sequence model.

hazard and or failure, but also in all the factors that lead to the undesired event.[2] Risk therefore relates to accidents (i.e. the event causing the harm) rather than hazards (i.e. the situation with the potential to cause harm) or failures of any individual piece of equipment.[3] Accidents happen when the characteristics of different factors (such as component failures, procedural shortcomings, and environmental effects) combine in an unexpected fashion. Manipulating any of the causes/hazards/events in the accident sequence can influence the risk. This includes the series of human failures (e.g. pilot error when exposed to increased stress) which may contribute to the accident.

4.3 Assessing risk

We have already stated that risk is a combination of accident likelihood (probability) and severity of the consequence. The risk increases with either severity or the probability of the accident as illustrated in Fig. 4.2. Different regulatory authorities use a variety of classification criteria in order to evaluate the acceptability of risk. Some of these are discussed in more detail in Appendix B, but the remainder of this paragraph will use the UK MoD criteria to illustrate the basic approach adopted by most.

- The UK MoD evaluates risk though the application of tables such as that illustrated in Table 4.1.



4.2 Increasing risk.

[2] An ARINC advert sums this up nicely: ‘The passenger in seat 16F depends on pilot awareness, which depends on the tower. Which depends on the satellite, which depends on the data link, which depends on the ground station, which depends on ARINC’

[3] This is often misunderstood and risks are then evaluated incorrectly for identified failures or hazards instead of their harmful outcomes.

Table 4.1 Example[1] of risk categorisation[2]

	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	C	D	D	D

Class A: these risks are deemed as being intolerable and shall be removed by the use of safety features.

Class B: these risks are considered as being undesirable, and shall only be accepted when risk reduction is impracticable.

Class C: these risks are deemed as being tolerable with the endorsement of the Project Safety Review Committee. May need to show that risk is ALARP (see Section 4.4).

Class D: these risks are accepted as being tolerable with the endorsement of normal project reviews. No further action needed.

[1] Table 4.1 presents general principles and is not specific to the aircraft industry (DEF STAN 00-56 Part 1 Para 7.3.2.b). Sometimes it may be that different safety criteria are applied to individual risk groups (e.g. safety of passengers vs. safety of armament personnel).

[2] Source: DEF STAN 00-56 Part 1 page 26 Table 5.

Table 4.2 Accident severity categories[1]

Negligible	Marginal	Critical	Catastrophic
At most a single minor injury or minor occupational illness.	A single severe injury or occupational illness; and/or multiple minor injuries or minor occupational illnesses.	A single death; and/or multiple severe injuries or severe occupational illnesses.	Multiple deaths

[1] Refer DEF STAN 00-56 Part 1 Section 7.3.2.

In order to understand the terminology used in Table 4.1, we need to define accident severity and the accident probability terms.

- Accident severity can be categorised in accordance with the impact on personnel as defined in Table 4.2.
- *Accident* probability can be categorised during risk estimation in accordance with the definitions in Table 4.3.

4.4 As low as reasonably practicable (ALARP)

The Health and Safety at Work Act (HSWA) affects product safety as well as workplace safety and has its basis in law (see Chapter 1). It requires us to determine if the risk is ALARP (as low as reasonably practicable), where:

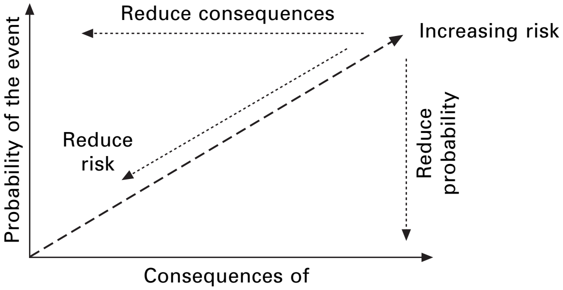
- 'practicable' means what is possible to do, such as considering options to reduce the frequency of occurrence and/or the consequence of the event (see Fig. 4.3),

Table 4.3 Accident probability categories[1]

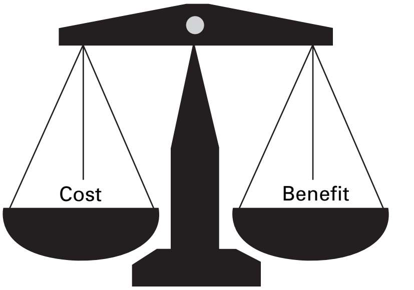
Accident probability (qualitative probability)	Occurrence (during operational life considering all instances of the system)	Quantitative probability per operating hour[2]
Frequent	Likely to be continually experienced	$< 1 \times 10^{-2}$
Probable	Likely to occur often	$< 1 \times 10^{-4}$
Occasional	Likely to occur several times	$< 1 \times 10^{-6}$
Remote	Likely to occur some time	$< 1 \times 10^{-8}$
Improbable	Unlikely, but may exceptionally occur	$< 1 \times 10^{-10}$
Incredible	Extremely unlikely that the event will occur at all, given the assumptions recorded about the domain of the system	$< 1 \times 10^{-12}$

[1] Refer DEF STAN 00-56 Part 1 Section 7.3.2.

[2] Note that the term ‘operating hour’ does not necessarily correlate with ‘flight hours’. Within the risk-based approach, operating hours could include the hours during maintenance (e.g. for hazards presented to ground crew). Or, from another perspective, a fleet of 10 aircraft flying in formation for 2 operating hours will accumulate 20 flying hours.



4.3 Reduction of frequency/severity.



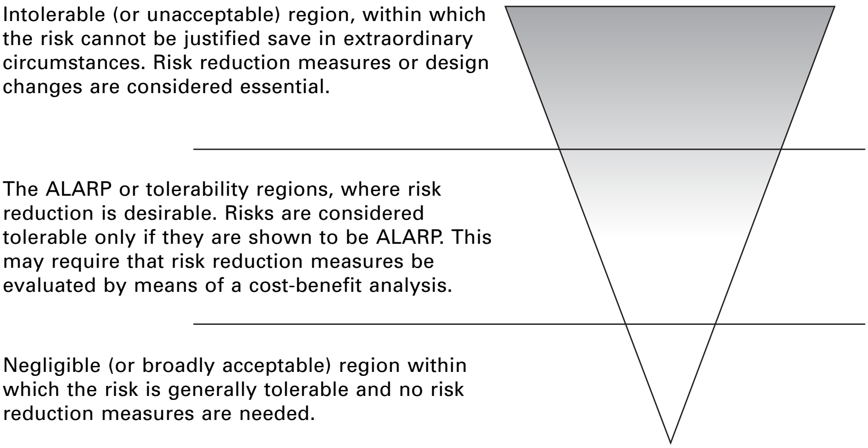
4.4 Cost-benefit scale.

- 'reasonable' means to balance costs, time, trouble against the risk (see Fig. 4.4). 'As low as reasonably practicable' means that risk in a particular activity/product can be balanced against the time, cost and difficulty of taking measures to avoid the risk. The greater the risk to safety, the more likely it is that it is reasonable to go to substantial effort to reduce it.[4]

The UK HSE divides risk into three tiers as illustrated in Fig. 4.5. ALARP is based on the legal standard of 'as far as reasonably practicable'. This standard has acquired its meaning in case law (i.e., the decisions made by judges in court) and has come to mean that the degree of risk of injury or adverse effect must be balanced against the cost in terms of money, time, and physical difficulty, of taking measures to reduce the risk. If the quantified risk of injury is insignificant compared with measures needed to mitigate the risk, then no action need be taken to satisfy the law. However, the greater the risk, the more likely it is to be reasonably practicable to go to substantial expense to do something about it.

In the main, changes to the safety of modern aircraft are made only when a cost-benefit analysis has been done in which the cost of the new safety feature is balanced against a notional figure for the monetary value of a life. If the cost of the measure exceeds the 'value' of the lives saved, then it will not be implemented.[5]

The regulation of safety in the United Kingdom is based upon the principle that risks must be reduced to a level that is 'as low as reasonably practicable' (ALARP).


Intolerable (or unacceptable) region, within which the risk cannot be justified save in extraordinary circumstances. Risk reduction measures or design changes are considered essential.
The ALARP or tolerability regions, where risk reduction is desirable. Risks are considered tolerable only if they are shown to be ALARP. This may require that risk reduction measures be evaluated by means of a cost-benefit analysis.
Negligible (or broadly acceptable) region within which the risk is generally tolerable and no risk reduction measures are needed.

4.5 ALARP triangle (the triangle illustrates the concept of diminishing proportions).

[4] The application of ALARP requires that benefit in reduction must be balanced against financial expenditure. Risk is tolerable when there is demonstrable gross disproportion between the cost of further risk reduction and the resulting risk reduction benefit. There is therefore a requirement to use a consistent 'value of life' throughout risk reduction in order to demonstrate compliance with the ALARP principle. This value is generally set by the regulator. Do not, however, use cost benefit to decide not to do something; rather use it as a trade-off study to prioritise most effective solution.

[5] For more on this topic, see *The Tombstone Imperative – The Truth about Air Safety* by A. Weir (2000).

It is a philosophy applied to the reduction and acceptability of risk. There is little guidance from the courts as to what this means. The key case is *Edwards* vs. *The National Coal Board*, where the Court of Appeal considered whether or not it was reasonably practicable to make the roof and sides of a road in a mine secure. The Court of Appeal held that

> … in every case, it is the risk that has to be weighed against the measures necessary to eliminate the risk. The greater the risk, no doubt, the less will be the weight to be given to the factor of cost

and

> … reasonably practicable is a narrower term than physically possible and seems to me to imply that a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them.

Precedent in which ALARP was found not to comply
Stark vs. *Post Office* (March 2000)

The Provision and Use of Work Equipment Regulations (PUWER) regulation 6(1) states: ‘Every employer shall ensure that work equipment is maintained in efficient working order and in good repair’

Mr Stark (a postman) was injured when a part of his bicycle broke.
Counsel for Mr Stark argued that PUWER 6(1) does not say anything about ‘reasonably practicable’. Therefore the duty is absolute and applies at all times.
The court found for Mr Stark.

It was clear that the obligation of maintenance was an absolute one and applied at all times. It did not matter that the cause of some maintenance failure caused the accident. If it can be proved that some piece of working equipment has in fact failed, that was sufficient.

4.5 Managing the risk

Risk management is defined as ‘the process whereby decisions are made to accept a known or assessed risk and/or the implementation of actions to reduce the consequences or probability of occurrence’ (BS 4778). A well-known cliché is ‘You cannot manage what you cannot measure’. Therefore, a logical and systematic means is required to:

1. identify conditions and situations that may result in an unacceptable level of safety
2. provide a measure of the technical airworthiness risk which is defined as the chance of exposure to an unacceptable level of safety
3. control the implementation of risk reduction measures

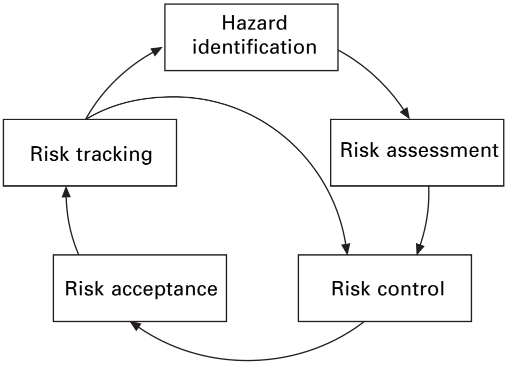
4. accept the level of risk
5. track the risk to make sure it does not change.

These five elements are illustrated in Fig. 4.6. The flowchart in Fig. 4.7 illustrates another way to consider a typical risk management process.

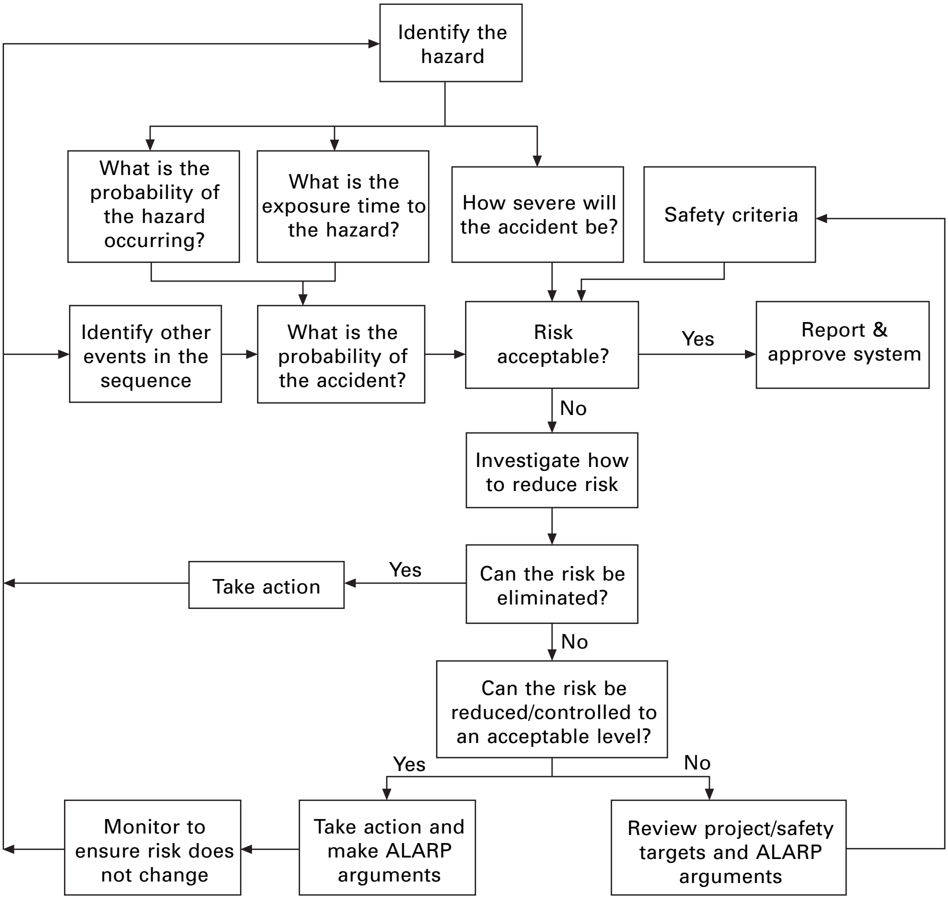
When it comes to evaluating risk, the popular question 'Is it safe?' has to be rephrased 'Are the risks low enough for the public/authorities to tolerate?' Safety management is not about removal of all risks. Rather, the key principle is that risk is reduced to 'as low as reasonably practicable' (ALARP).

Risk management of a system is not simply about reducing risk; it relates to striking a balance between the benefits from reduced risk and the expense of that reduction. However, some risks (such as a polio outbreak) may be completely unacceptable and not subject for balancing against expense. Risk management strategies include:

- **Eliminate** – get rid of the hazard that could cause the accident.
- **Spread out** – spread the loss exposure responsibility out among different entities, across operations, or across time.
- **Transfer** – make others accept loss exposure responsibility.
- **Accept** – live with the current loss exposure level or responsibility.
- **Avoid** – cancel or delay the activity that involves the risk, or do not operate. equipment that involves the risk. Make processes inherently safer by eliminating hazards (e.g. eliminate energy sources such as pressure, heat, potential energy, kinetic energy, etc. Do not use hazardous materials and materials that can generate hazardous energy. Use other, less hazardous, materials in place of more hazardous materials.
- **Reduce** – do something to reduce the accident potential. Accidents can be well controlled at any point in the chain of events producing the accident. The goal is to get the most for your money by doing the things that are most effective. Options to consider include:
  – reduce the likelihood of initiating events (e.g., eliminate error-likely situations that set people up for failure; make sure that sufficient competent people are assigned to operations and maintenance departments; improve design ratings and factors of safety).



4.6 The five elements in risk management.


Identify the hazard
What is the probability of the hazard occurring?
What is the exposure time to the hazard?
How severe will the accident be?
Safety criteria
Identify other events in the sequence
What is the probability of the accident?
Risk acceptable?
Yes
Report & approve system
No
Investigate how to reduce risk
Take action
Yes
Can the risk be eliminated?
No
Can the risk be reduced/controlled to an acceptable level?
Yes
No
Monitor to ensure risk does not change
Take action and make ALARP arguments
Review project/safety targets and ALARP arguments

4.7 Risk management process (note the iterative nature of the risk management process).

– provide multiple layers of safeguards, sometimes called layers of protection, in critical applications (e.g., add additional instrumentation, equipment, or safety interlocks, especially items with different design and operation; make the operators perform more surveillance and checks during operations).
– reduce the chance of safeguard failures (e.g., perform additional or more frequent inspections, tests, and preventive maintenance).
– make processes inherently safer by reducing the severity of consequences (e.g., reduce energy stored or generated as pressure, heat, potential energy, kinetic energy, etc; keep only small inventories of hazardous materials and materials that can generate hazardous energy; provide shutdown and alarm/response systems to limit consequences; protect people and other valuables from consequences by providing emergency response training, personal protective equipment, etc).

MIL-STD-882C (para 4.4) provides the following useful guidance when considering the order of precedence for resolving identified hazards:

1. **Design for minimum risk.** From the start, design to eliminate risk. If an identified hazard cannot be eliminated, the risks associated with that hazard should be controlled through design selection.
2. **Safety devices.** Hazards that cannot be eliminated or have their associated risks sufficiently mitigated through primary design selection, will be controlled by the use of fixed, automatic, or other protective safety design features or devices. Provision will be made for periodic functional checks of safety devices.
3. **Warning devices.** When neither design nor safety devices can effectively eliminate or control an identified hazard, devices will be used to detect the condition and to generate an adequate warning signal to correct the hazards or provide personnel evacuation. Warning signals and their application will be designed to minimise the probability of incorrect personnel reaction to the signals and will be standardised within like types of the system.
4. **Procedures and training.** Where it is impossible to eliminate a hazard or adequately control its associated risk through design selection or use of safety and warning devices, procedures and training will be used to mitigate the risk. Procedures may include the use of personal protective equipment or through the use of checklists. Precautionary notations must be standardised. Safety critical tasks and activities may require certification of personnel proficiency.

   However, too often we find that hazards are mitigated by procedures only. Remember, if something can go wrong, then one day it will go wrong. Remember the 50-50-90 rule: if at any time you have a 50-50 chance of getting something right, there's a 90% probability you'll get it wrong.

4.6 Summarising the risk-based approach

In essence any risk-based safety assessment process is made up of basic steps:

- identify the hazards
- classify severity of each accident
- determine the probability of each accident occurring
- assess the risks to people, property, and/or success of a mission or programme, in terms of both probability of occurrence and severity of consequences
- manage the risk.

Typical questions a risk-based approach can answer are:

- What is the likelihood that a particular unfavourable consequence (mission failure, loss of platform, programme delay, etc.) will happen?
- What are the most important drivers of overall risk (i.e. what factors should we concentrate our improvement effort on)?
- Which alternative gives less risk?
- Does a proposed action (e.g. modification, procedure or limitation) reduce risk-related costs enough to justify its cost?
- What risk factors have so much uncertainty that more testing or analysis is needed to define them better?

Advantages of the risk-based approach include:

- It provides clear guidance about the acceptability of the risk. It assists in identifying and prioritising the factors (design, operations, maintenance, management, environment, etc.) that contribute to risk, and evaluating the uncertainty that inevitably accompanies all estimates of risk.
- It is most effective when applied to major accidents, where the chances of occurrence are relatively low and operating experience very high.
- By expressing risk and costs in common units, the cost benefit analysis becomes a useful decision-making aid to project management.
- Safety targets can be set for total systems (i.e. human + equipment + procedures + training). The safety targets are based on the *consequences* of an undesired event.

Disadvantages/limitations of the risk-based approach include:

- Appropriate risk criteria need to be set (there are no universally acceptable criteria to define whether or not risks are tolerable) and agreed with all stakeholders (including those exposed to the risk).
- Be aware of the units of measurement employed during accident probability quantification. The term 'operating hour' (see Table 4.3) must be defined and consistently applied to ensure a 'level playing field' during risk comparison.
- When we look at the acceptability of risk – acceptable to whom? The general public? The engineer? The company? Risk is affected by perception, for instance, scientists/engineers may trade risk against long-term benefits, while society will focus on the consequences versus the immediate benefits.[6]
- Not all hazards necessarily lead to accidents. Furthermore, any one hazard can have many potential causes and consequences depending on the sequence of event. This is very dependent on how the hazard is defined (see example below, and also Chapter 6)
- Accident sequences have large number of variables and it is unrealistic always to consider them all. Risk assessment relies on judgemental decisions which integrate reliability, availability and maintainability (RAM) engineering analysis; statistics; decision theory; systems engineering; quality engineering; conventional engineering analysis, and even cognitive psychology. Estimating the probability of occurrence of each event in the accident sequence can become very subjective – especially when evaluating the probability of human response, and human error is invariably present in the accident sequence.[7] Even though quantitative assessments (see Appendix A)

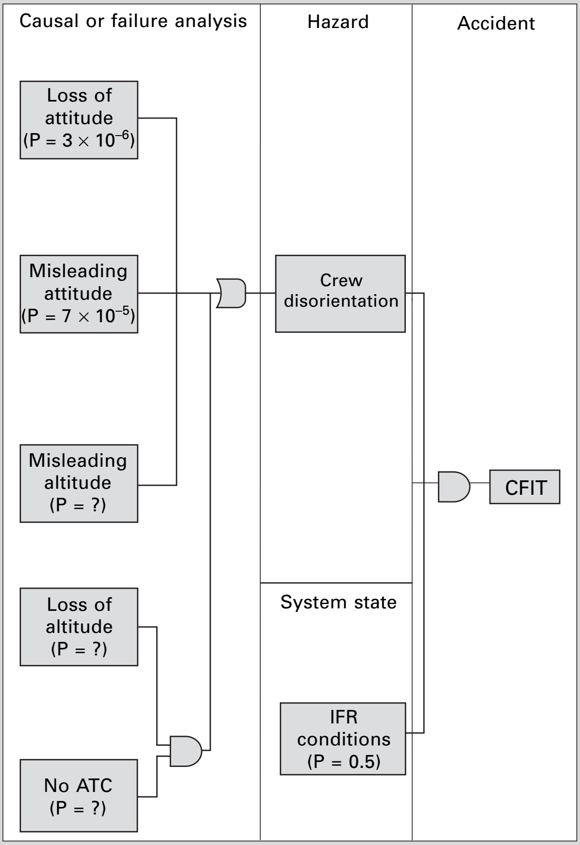
[6] When trying to convey risk to the public, put it in terms they can identify with. For instance: Equate cost of risk management in terms of a tax on the product (e.g. if one life = £1million, then each cigarette should be taxed 70 pence, and each soft drink should be taxed 2 pence).

[7] Stuart Matthews, President and CEO of the Flight Safety Foundation, reports that statistics show that human error features in more than 85% of all accidents. It should be no surprise that for some time now the primary concerns of the western aviation industry have revolved around human factors, particularly flight crew errors. Pilots are often the last link in the accident chain. In fact, pilots contribute to 65% of accidents (Matthews, 2004).

may look very objective, the core input data is often very subjective and/or predictive (e.g. see Ch. 10 para 6).

- ALARP requires cost-benefit analysis (i.e. simply meeting a risk target is not enough), which implies that a price needs to be put on the value of a human life in the explicit trade-off between safety and economics. Only the owner of the risk can make this decision.
- ALARP may not always be defensible in a court of law (see Section 4.4 above, and also Ch. 1).
- Risk-based decision-making may hamper/stifle innovation. For instance, would cars – or even glass – be allowed[8] if they were invented today?

Example: Consider an assessment where a company is contracted to upgrade the attitude display in an aircraft. Loss of attitude display could cause crew disorientation, which could lead to controlled flight into terrain (CFIT). However, the attitude display is not the only contributor to the hazard, and the contractor may not be responsible for doing a probabilistic assessment on the whole aircraft.


Causal or failure analysis
Hazard
Accident
Loss of attitude ($P = 3 \times 10^{-6}$)
Misleading attitude ($P = 7 \times 10^{-5}$)
Misleading altitude (P = ?)
Loss of altitude (P = ?)
No ATC (P = ?)
Crew disorientation
System state
IFR conditions (P = 0.5)
CFIT

- Accident severity:
  → Catastrophic
- Accident probability:
  → Unknown (until all 'P' are known)
  → Must be 'improbable' to be Risk C
- Risk:
  → Unknown (until all 'P' are known)
  → If 'improbable' then Risk C
  → If 'remote', then Risk B

[8] The solution in these instances is to take away the uncertainty factor, sell the benefits of innovation and communicate the risk in terms that people can understand (e.g. in France people who live near nuclear power stations get a substantial discount in their rates).

4.7 Discussion

Risk assessment seeks to answer relatively simple questions although, like many engineering questions, these are far easier to pose than to respond properly too. Table 4.4 summarises some of these questions and provides an indication of the processes needed to address them.

The general principles of safety risk management are (*FAA System Safety Handbook* (2000)):

- All system operations represent some degree of risk. Recognise that human interaction with elements of the system entails some element of risk.
- Keep hazards in proper perspective. Do not overreact to each identified risk, but make a conscious decision on how to deal with it. Dr Trevor Kletz is known to have said: ‘To maintain the balance in your risk exposure levels, when confronted by a new risk, just smoke 1 or 2 less cigarettes a day.’
- Weigh the risks and make judgements according to your own knowledge, inputs from subject matter experts, experience, and programme need. There may be no ‘single solution’ to a safety problem. There are usually a variety of directions to pursue. Each of these directions may produce varying degrees of risk reduction. A combination of approaches may provide the best solution.
- Risks are reduced asymptotically. Thus the closer to zero we get the more effort is needed. We thus need to know when enough is enough. A good decision made quickly is much better than a perfect decision made too late. Also, a good decision does not always result in a good outcome. The best we can hope for is to equip intelligent decision makers with good information based on a number of decision factors and the interests of stakeholders. On average, and over time, good decisions made through this process should provide the best outcomes. They will also provide logical explanations for decisions when the outcomes are not favourable.

Finally, remember that producing a risk assessment is simple enough, the challenge lies in demonstrating that risks have been identified in a structured and systematic way and that the risks are managed throughout the product life-cycle, i.e.,

- **Implement risk control.** Risk-management activities have no effect on risk until

Table 4.4 Risk assessment processes

Question	Risk assessment process	Useful tools & techniques (see Annex A)
What can go wrong?	Hazard identification	HAZOP, FHA, PRA, ZHA, etc.
How badly can it go wrong	Consequence modelling	Qualitative FTA, ETA, etc.
How often can it happen?	Frequency estimation	Quantitative FTA, ETA, etc.
So what?	Risk assessment (i.e. assess frequency relative to the consequence)	Risk matrix
What can I do about it?	Risk management (e.g. influence the frequency and/or the severity).	Bow tie analysis, FRACAS, DRACAS, SMS, CHIRP, etc.

the process of risk control is implemented to actually change the design, to add safety protective features or to alter working practices.

- **Assess risk continuously.** Assessment of technical risk depends on the quality and quantity of information available. There may be very little data available in the preliminary stage of a decision-making process. As the process progresses, the results of system safety analysis; failure mode, effects and criticality analysis; and compliance testing may provide the necessary information and details required to refine the risk assessment. Ultimately, actual operational use and airworthiness-related occurrences will provide the most valuable information. Even then, the risk changes as the system ages, or as operating or maintenance procedures (and personnel) alter.

4.8 Further reading

Conrow, E. *Effective Risk Management: Some Keys to Success*, American Institute of Aeronautics and Astronautics, 1801, Alexander Bell Drive, Restone, VA 20191, USA, 2003.

Duffey, R.B., Saull, J.W., *Know the Risk: Learning from Errors and Accidents – Safety and Risk in Today's Technology*, Butterworth-Heinemann, Linacre House, Jordan Hill, Oxford, OX2 8DP, UK, 2003.

5
Goal-based approach

In absence of clearly defined goals, we become strangely loyal to performing daily acts of trivia

Unknown

5.1 Introduction

An acceptable level of safety for aviation is normally defined in terms of an acceptable aircraft accident rate. There are two primary causes of aircraft accidents:

- operational (such as pilot error, weather and operating procedures) and
- technical (such as design errors, manufacturing errors, maintenance errors and part failures).

When certifying a new (or modified) system, designers concentrate on the technical integrity of the system which has been designed around an operational requirement. For a number of years, aeroplane systems were evaluated to specific requirements, to the ‘single fault’ criterion, or to the ‘fail-safe design’ concept (see Chapter 7).

As later-generation aeroplanes were developed, more safety-critical functions were required to be performed. This generally resulted in an increase in the complexity of the systems designed to perform these functions. The likely hazards to the aeroplane and its occupants that could arise in the event of loss of one or more functions (provided by a system or that system’s malfunction) had to be considered, as also did the potential interaction between systems performing different functions.

The application of the fail-safe concept thus had to be supplemented by some sort of safety target (i.e. goal) against which the integrity of the system architecture could be evaluated.

5.2 Probability targets vs. failure severity levels

In assessing the acceptability of a design it was recognised that rational failure probability values would have to be established. The civil regulatory authorities implemented the following logic (AMC25.1309 to CS25) for large commercial transport aircraft:

> Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours

> of flight.[1] Furthermore, about 10 per cent of the total were attributed to failure conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is reasonable to expect that the probability of a serious accident from all such failure conditions be not greater than one per ten million flight hours or 1×10^{-7} per flight hour for a newly designed aeroplane.

Most civilian airworthiness authorities have thus determined that an acceptable aircraft accident rate attributable to *technical cause factors* for large commercial transport aircraft is of the order of 1 per 10 million hours,[2] provided the probability of occurrence does not vary from flight to flight.[3]

The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically. A typical transport category aircraft type design has many individual systems that may influence the safe flight and landing of an aircraft. Without a full system safety analysis it is difficult, if not impossible, to consider the contribution of each individual system to the overall accident rate.

For most aircraft types it is therefore assumed (refer, *inter alia*, ACJ25.1309 para 6.a) that as many as 100 individual system failure conditions may exist which could prevent continued safe flight and landing. The target allowable probability of 1×10^{-7} is thus apportioned equally among these conditions, resulting in a probability allocation of not greater than 1×10^{-9} per flight hour to each.[4]

This upper probability limit establishes an approximate probability value for the term 'extremely improbable'. Failure conditions having less severe effects could be

[1] To put this (i.e. one accident in a million flying hours) in perspective (Howard 2000, Section 1) there are were about 13,000 large jet aircraft in the world at the start of this millennium, flying a total of about 50 million hours per year whilst occurring about 50 fatal accidents.

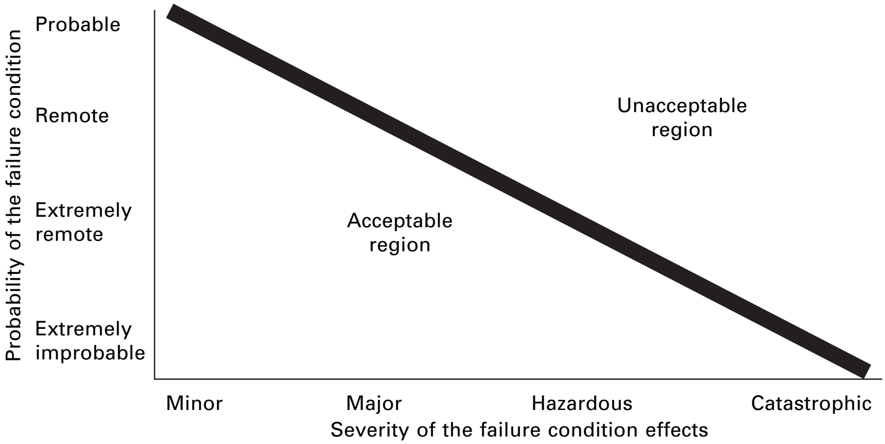
[2] This leads to an accident probability of 0.0000001 (10^{-7}) per hour for technical cause factors. Therefore, for transport category aircraft, most civil airworthiness authorities require that aircraft systems and associated components (considered separately and in relation to other systems) be designed in a manner such that the occurrence of any failure condition which would prevent the continued safe flight and landing of the aircraft should virtually never occur in the life of an aircraft type.

[3] The probability of occurrence does vary from flight to flight in many situations, such as structural fatigue where the probability of failure increases with cumulative exposure. However, measures such as placing life limits on critical parts and mandatory structural integrity inspections are introduced during type certification of the aircraft type to avoid these types of failures. The following two situations require special consideration (i) the deferral of known aircraft defects when higher risk may be accepted for a short-term and (ii) the delayed implementation of necessary risk reduction corrective action for practical reasons, such as operational impact or production capacity. These two situations are generally considered acceptable because the exposure time at the increased risk level is relatively short in comparison to the total flying time for the aircraft type. Therefore, although the probability of an accident on any particular flight may be greater, the effect on the overall accident rate may be imperceptible.

[4] The same logic has been applied by the FAA to single-engine airplanes under 6,000 pounds to establish a probabilty target of 1×10^{-3} per flight hour (i.e. three orders of magnitude different from large transport aircraft). For more information, see AC23.1309 Figure 2.

relatively more likely to occur based on the principle that an inverse relationship should exist between the probability of an occurrence and the degree of hazard inherent in its effect.[5]

This led to the general principle that an inverse relationship should exist between the probability of loss of function(s) or malfunction(s) leading to a serious failure condition and the degree of hazard to the aeroplane and its occupants arising therefrom. This 'degree of hazard' is commonly referred to as the *severity of the consequence*. The civil aviation authorities use this inverse relationship between Consequence and Frequency to substantiate safety against prescribed hazard definitions and allocated probability targets as illustrated in Fig. 5.1.



5.1 Inverse relationship between the consequence and the frequency of a failure (AMC25.1309 to CS25).

Failure effects are therefore regulated by requiring an inverse relationship between the severity of the failures and their frequency of occurrence.[6] The broad intention is that effects of a catastrophic nature should virtually never occur in the fleet of a type of aircraft. Where the effects are less hazardous, they are permitted to occur more

[5] Military airworthiness authorities have generally not established acceptable levels of safety for technical failures. However, a higher risk level is generally considered acceptable for military aviation and a factor of 10 is often used when comparing acceptable accident rates for equivalent military and civilian aircraft types. Therefore, a probability of occurrence in the order of 10^{-8} per hour for a catastrophic severity effect for individual systems on a military transport category aircraft type (equivalent to a civil aircraft type) is often considered reasonable and achievable. See Appendix B for more information.

[6] Note the wide line in Fig. 5.1, which indicates the 'order of probability'. Component failure rate data are not always precise enough to enable accurate estimates of the probabilities of failure conditions (see chapter 10). This results in some degree of uncertainty, as indicated by the wide line on Fig. 5.1, and the expression 'on the order of' in the descriptions of the quantitative probability terms. When calculating the estimated probability of each failure condition, this uncertainty should be accounted for in a way that does not compromise safety.

frequently. Each failure mode classification can thus be allocated a quantitative or a qualitative safety objective based on its level of criticality as illustrated in the example in Table 5.1 (based on ACJ 25.1309).

Appropriate qualitative probability terms can then be defined, as per Table 5.2 (based on AMC25.1309) and are 'commonly accepted as aids to engineering judgement'. The International Civil Aviation Organisation advises (ICAO Airworthiness Manual, page IIA-4h-I) that where it is necessary to use numerical assessments, the values given in Table 5.3 may be used in providing a common point of reference.

These qualitative and quantitative objectives become safety requirements and provide a measure of performance against which the integrated product will be evaluated. The target probability[7] is set to assist the assessor in minimising the occurrences of hazards by applying a variety of defences and design disciplines appropriate to the severity of the safety target. Typically, the objectives are accomplished through the application of the fail-safe concept as discussed in Chapter 7.

5.3 Discussion

The goal-based approach to safety is applied as follows:

- identify potentially hazardous situations (e.g. failures or occurrences, not necessarily accidents)
- assess their impact on the system
- set safety targets according to the potential severity
- prove that these targets are met.

These safety targets can have an impact on all aspects of the design. If they are too severe they will impact on the costs, capability, performance, etc. If not severe enough the high failure rates experienced in service become unacceptable, resulting in loss of customer capability and resources, high damage costs, and loss of company reputation. The safety targets should therefore be agreed with the applicable airworthiness authority as early as possible within the product development lifecycle.

In essence any goal-based safety assessment process consists of three basic processes:

1. identifing the failure modes or hazardous situations/occurrences
2. allocating safety objectives to these failure modes
3. proving safety objective accomplishment.

Advantages of the goal-based approach include

- Accidents do not just happen – they need a sequence of events to combine in a particular fashion and are thus difficult to predict. This is especially true if the assessor is not the operator and therefore cannot control the final mitigations (such as human factors associated with personnel competence or exposure levels) which

[7] The target probability is sometimes referred to as the 'derived safety objective', especially if flowed down to system components via the application of techniques such as fault tree analysis.

Table 5.1 Typical safety objectives

Severity	No safety affect	Minor	Major	Hazardous (severe major)	Catastrophic
Effect	Failure conditions that may not have an effect on safety, operational capability or crew workload. At most a nuisance.	Slight reduction in safety margins. Slight increase in crew workload. Some inconvenience to occupants. May require operating limitations or emergency procedures.	Significant reduction in safety margins or functional capabilities. Significant increase in crew workload impairing crew efficiency. Some discomfort to occupants. Requires operating limitations or emergency procedures.	Large reduction in safety margins or functional capabilities. Higher workload or physical distress. Adverse effects upon occupants.	All conditions which prevent continuous safe flight and landing.
Allowable probability	Frequent (Probable)[1]	Reasonably probable (Probable)	Remote (Improbable)	Extremely remote (Improbable)	Extremely improbable (Extremely improbable)

Note: The level of criticality is taken from the effect/end result (i.e. accident, incident or deficiency) of that failure and/or occurrence on the aircraft system as a whole. This results in the allowable probability of the failure condition (not the probability of the accident occurring as used in the risk-based approach).

[1] Parentheses indicate FAR25.1309 classification, in contrast to the JAR25.1309 classification.

Table 5.2 Qualitative probability terms

Allowable probability	Frequent	Reasonably probable	Remote	Extremely remote	Extremely improbable
Qualitative definition	Conditions anticipated to occur several times	Conditions anticipated to occur one or more times during the entire operational life of each aeroplane	Conditions unlikely to occur to each aeroplane during its entire life but which may occur several times when considering the total operational life of a number of aeroplanes of this type	Conditions not anticipated to occur to each aeroplane during its operational life, but which may occur a few times when considering the total operational life of all aeroplanes of the type.	Conditions so unlikely to occur that they are not anticipated to occur during the entire operational life of all aeroplanes of the type.

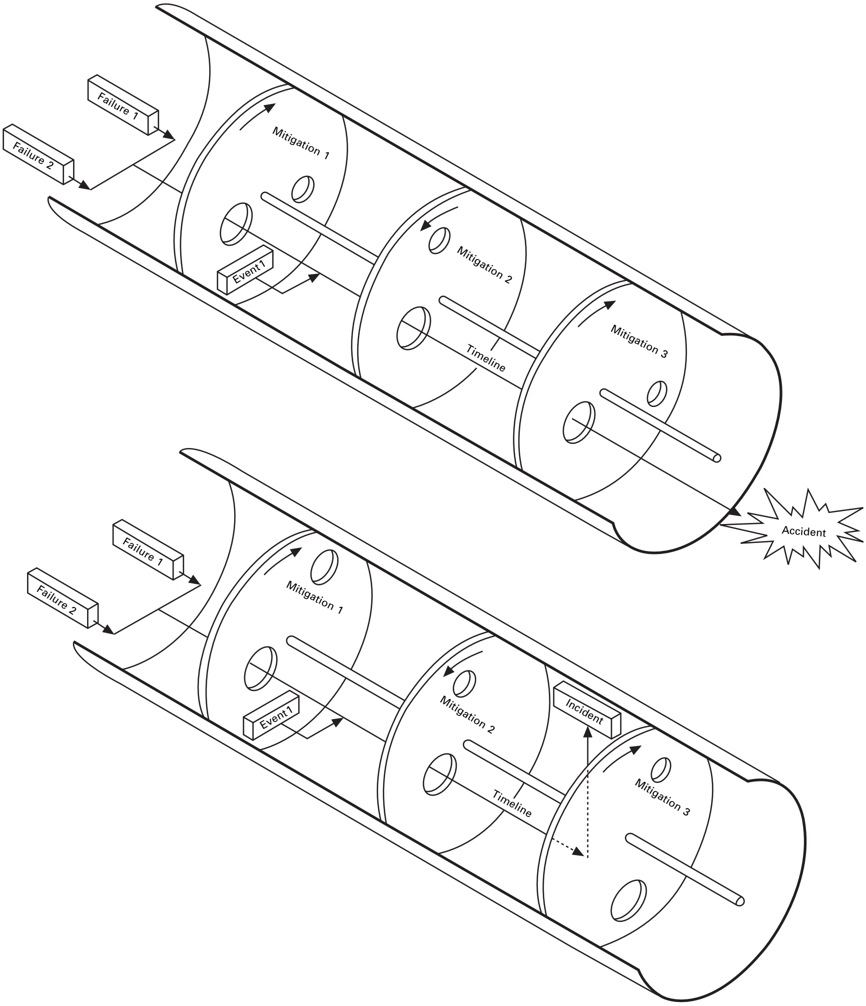
Table 5.3 Quantitative probability values[1]

Allowable probability	Frequent	Reasonably probable	Remote	Extremely remote	Extremely improbable
Quantitative definition	May be interpreted[2] as a probability of occurrence greater than 10^{-3} per hour of flight for the expected mean flight time of the type of aeroplane involved	May be interpreted[2] as a probability of occurrence greater than 10^{-5} but less than 10^{-3} per hour of flight for the expected mean flight time of the type of aeroplane involved. A reasonably probable effect could arise several times in the aircraft fleet	May be interpreted as a probability of occurrence greater than 10^{-7} but less than 10^{-5} per hour of flight for the expected mean flight time of the type of aeroplane involved. A Remote effect might arise once in the life of each aircraft, and several times for the fleet.	May be interpreted as a probability of occurrence greater than 10^{-9} but less than 10^{-7} per hour of flight for the expected mean flight time of the type of aeroplane involved. An Extremely Remote effect might arise once in the whole fleet life.	May be interpreted as a probability of occurrence of less than 10^{-9} per hour of flight for the expected mean flight time of the type of aeroplane involved. An Extremely Improbable effect would be unlikely to occur in the whole fleet.

Note: ICAO advises that 'These numerical values are goals rather than precise values and judgement should be used in their application. The probability should be established taking into account the appropriate length of time at risk. Such statistical methods should be used to complement engineering judgement and should not be regarded as a substitute'.

[1] Sourced from ICAO Airworthiness Manual, Appendix H to Chapter 4, page IIA-4h-I as well as CS25 (AMC25.1309).

[2] AMC25.1309 (to CS25) advises that: 'A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for minor failure conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly accepted industry practice.'



5.2 Simple accident sequence (adapted from James Reason's Swiss Cheese Model (Reason, 1997).

make the distinction between an accident and an incident (see Fig. 5.2). Technical failures do happen and are easier to predict.

- The goal-based approach provides clear guidance about the severity of a particular system failure and, in so doing, gives clear minimum safety objectives which need to be accomplished for that system to be satisfactory. These objectives can be determined quickly and efficiently (using Table 5.1) and allocated to responsible parties to accomplish. The goal-based approach is thus particularly useful for designers of systems (see example on page 65).
- The application of internationally accepted safety criteria provides for a level playing field in the integration and certification of projects with international participation/subcontractors and customers/operators.

Example: consider again the example in Section 4.6 where a company is contracted to upgrade the attitude display in an aircraft. Display of attitude in the cockpit is a critical function. Loss of all attitude display, including standby attitude, is a critical failure and must be extremely improbable (refer also AC25-11). Note that:

- extremely improbable implies a 'catastrophic' failure condition
- if a quantitative assessment is required (see Table B.5) then the system designer needs to prove that this failure condition has a probability of $p < 1 \times 10^{-9}$ per flight hour.

Limitations of the goal-based approach:

- If 'Historical evidence indicates that the risk of a serious accident due to operational and airframe-related causes is approximately 1 per million hours of flight', then (with reference to Fig. 13.2), the rationale used for the goal allocation may no longer remain acceptable to society if there is to be one large aircraft accident every 7–10 days by the year 2010. For more on this, see *Planning for Super Safety* by R. Howard (2000).
- It usually does not distinguish between different accident severities (i.e. the death of one person vs. the death of 100 people). It concentrates on the probabilities of technical failures only.
- It is primarily used to consider failures and malfunctions to systems only. It does not consider operational hazards, nor does it include human errors. Only a minority of accidents can be attributed to system failure or malfunction only. Accidents seldom occur due to isolated events. More often than not they are the result of a series of failures, events and/or failing mitigations. Events are influencing external factors, for instance lightning strikes, or flying in VMC conditions, or being under enemy fire. Mitigations put in place with the intention to block the accident path can be divided into three main types:
  - those that reduce the likelihood of the error taking place
  - those that aid error detection
  - those that aid error recovery.

  Mitigations can involve the human (e.g. training and supervision), the machine (e.g. alert devices) or procedures (e.g. emergency procedures). Mitigations are not perfect in blocking the error and when the holes line up, error is allowed to continue along its path to an accident. Figure 5.2 illustrates this roulette of changing circumstances which needs to align to result in an accident.

So, although the goal-based approach provides a designer with acceptable levels of safety which need to be accomplished in the design (as in Chapter 8), the user of the system will need to conduct further assessments (as in Chapter 9) to consider how the system is put into operational use and what risks said use will hold.

5.4 Combining the risk- and goal-based criteria

A valid question would be to ask whether the risk-based[8] and goal-based[9] criteria can be combined in a single set of tables.

The FAA's internal Safety Management System (ASD-100-SSE-1) combines the two approaches by classifying hazard severity as shown in Table 5.4; allocating consequence probability as shown in Table 5.5; and then assessing risk according to the matrix shown in Fig. 5.3.

Table 5.4 Hazard severity

Catastrophic	Results in multiple fatalities
Hazardous	Reduces the capability of the system or the operator ability to cope with adverse conditions to the extent that there would be a large reduction in safety margin or functional capability. Crew physical distress/excessive workload is such that operators cannot be relied upon to perform required tasks accurately or completely Serious or fatal injury to small number of persons (other than flightcrew)
Major	Reduces the capability of the system or the operators to cope with adverse operating condition to the extent that there would be a significant reduction in safety margin or functional capability, a significant increase in operator workload and conditions impairing operator efficiency or creating significant discomfort or physical distress to occupants of aircraft (except operator) including injuries Major occupational illness and/or major environmental damage, and/or major property damage
Minor	Does not significantly reduce system safety. Actions required by operators are well within their capabilities. Includes a slight reduction in safety margin or functional capabilities, a slight increase in workload such as routine flight plan changes and some physical discomfort to occupants of aircraft (except operators) Minor occupational illness and/or minor environmental damage, and/or minor property damage
No safety effect	Has no effect on safety

Author's note: strictly speaking, these are not hazards but the worst-case consequences of a hazard (see Chapter 6). Furthermore, be aware that this approach may cause confusion (e.g. will a 'hazardous' condition reduce the capability or will it cause serious/fatal injuries? Surely the latter should be more severe?)

It is thus shown that great care should be taken when following these two approaches. Personally, the author has found it far simpler and more efficient to consistently keep a clear distinction between 'airworthiness/failure criteria' and 'accident criteria' (as

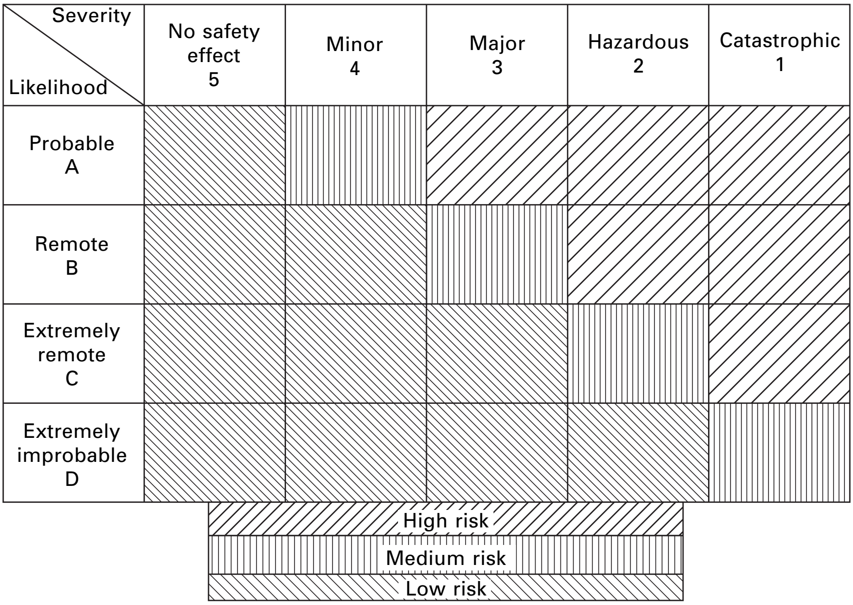
[8] The risk-based approach (commonly used by many engineering facilities where there are many potential hazards and generally fewer safeguards to prevent escalation) combines a large number of events, often using generic frequency studies, to distinguish between the severities of different types of accident.

[9] The goal-based approach (commonly used in the aviation and nuclear industry for the certification of their products) emphasises the frequency of an undesired event (e.g. system failure).

Table 5.5 Consequence probability

Probable	*Qualitative:* anticipated to occur one or more times during the entire system/operational life of an item. *Quantitative:* probability of occurrence per operational hour is equal to or greater than 1×10^{-5}
Remote	*Qualitative:* unlikely to occur to each item during its total life. May occur several times in the life of an entire system or fleet. *Quantitative:* probability of occurrence per operational hour is less than 1×10^{-5}, but greater than 1×10^{-7}
Extremely remote	*Qualitative:* not anticipated to occur to each item during its total life. May occur a few times in the life of an entire system or fleet. *Quantitative:* probability of occurrence per operational hour is less than 1×10^{-7} but greater than 1×10^{-9}
Extremely improbable	*Qualitative:* so unlikely that it is not anticipated to occur during the entire operational life of an entire system or fleet. *Quantitative:* probability of occurrence per operational hour is less than 1×10^{-9}

Author's note: it is unclear whether these probabilities are for the failure condition targets or targets for the worst-case consequence (i.e. the probability of the accident).



Severity / Likelihood	No safety effect 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Probable A	▧	▥	▨	▨	▨
Remote B	▧	▧	▥	▨	▨
Extremely remote C	▧	▧	▧	▥	▨
Extremely improbable D	▧	▧	▧	▧	▥

▨ High risk
▥ Medium risk
▧ Low risk

High risk: tracking in a hazard tracking system is required until the risk is reduced or accepted at the appropriate level of management.
Medium risk: acceptable with review by the appropriate level of management. Tracking in a hazard tracking system is required.
Low risk: acceptable without review.
This matrix also classifies risk of each hazard into three levels: high, medium, and low. This matrix is useful if there is a need to allocate a risk allocation to the JAR/FAR criteria. However, be careful to distinguish between hazards and accidents, which could both be allocated the same risk level. For instance, an accident which has a remote probability of killing a small number of persons should surely have a higher risk level that a hazardous failure condition (such as loss of attitude data) which is also remote in occurrence.

5.3 Risk assessment matrix.

discussed in Chapter 8), with the key differentiating factor in the two approaches being that:

- the goal-based approach emphasis the frequency of an event/failure (which is the nuclear and civil aviation industry approach), whilst
- the risk-based approach looks at a large number of events to evaluate the probability of an accident occurring (which is the approach used by many operators and facilities. The UK MoD has also adopted this approach in DEF STAN 00-56).

This differentiating approach is also adopted by the Australian Defence Force. SAAP 7001.054((AM1), Section 2 Chapter 1)), which states:

> System safety objectives for aircraft acquisitions and modification projects are different to those for the management of in-service aircraft. During acquisition and modification projects, the system safety objective is to procure an aircraft with an acceptable level of safety … Once in service, the system safety objective is to ensure that the aircraft's inherent level of safety is maintained.

The goal-based and risk-based approaches can be combined in the same assessment by:

- showing an inverse relationship between failure severity and failure probability (i.e. the goal-based approach) during system certification
- from these causes/failures, identifying the hazards that could lead to an accident (i.e. the risk-based approach) during the operational application of the system. For instance, ten different causes/failures (e.g. components which could release toxic fumes) may all lead to one hazard (e.g. intoxication), which in turn could cause one (or more) types of accident (e.g. death of a technician, or death of all passengers).
- assessing the probability of this hazard becoming an accident. If the hazard (and resulting accident) has a technical failure as a contributing cause, then the probability of said technical failure would need to be obtained from the system provider.
- Determining the risk by combining the accident severity with its probability.

6
Hazards

Imagine a world with no hypothetical situations ...

6.1 Understanding hazards and their causes

Safety is freedom from accidents. Accidents are caused by hazards. But what exactly do we understand the term ‘hazard’ to mean? It goes by many (often confusing) definitions, such as:

- an accident (i.e. injury to personnel, damage to property or pollution of environment) waiting to happen
- a physical condition of a platform that threatens the safety of personnel of the platform, i.e., that can lead to an accident, or has the potential to cause harm
- a condition of the platform that, unless mitigated, can develop into an accident through a sequence of events and actions
- natural events such as bird strikes, lightning, windshear, etc.
- a potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof (ARP 4761)
- a situation that could occur during the lifetime of a product, system or plant that has the potential for human injury, damage to property, damage to the environment or economic loss (BS 4778).
- a situation with the potential for human injury, damage to property/assets or the environment (Rhys, 2002, page 4).
- a set of conditions in the operation of a product with the potential for initiating or contributing to events that could result in personal injury, damage to property or harm to the environment
- exposure of vulnerability to injury, loss, evil, etc. A thing likely to cause injury, etc. (Collins English Dictionary, 2003).

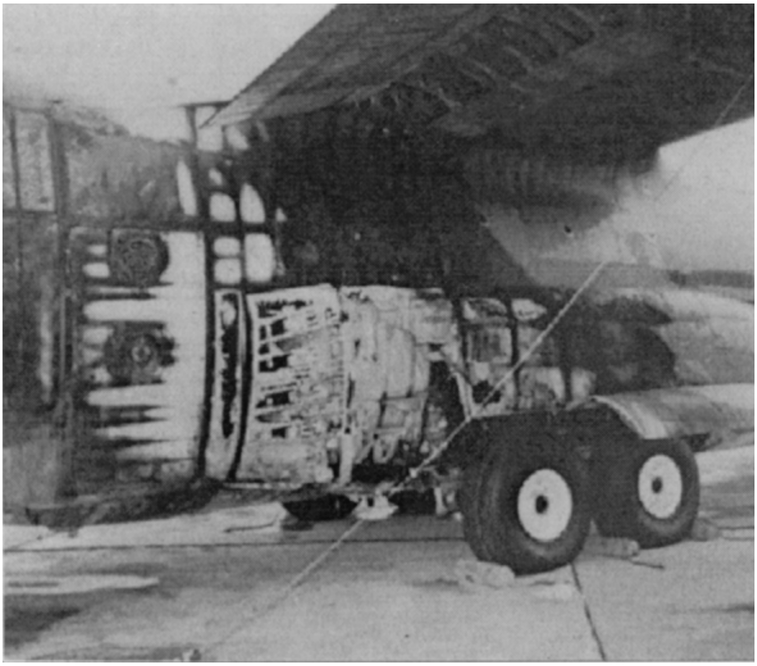
Note that the presence of a hazard does not make an accident inevitable. From the discussions in this chapter, it is proposed that an all-encompassing definition might thus rather be: ‘A hazard is a prerequisite condition that can develop into an accident through a sequence of failures, events and actions in the process of meeting an objective.’

Example: making the distinction between hazards and their causes

Is 'aircraft brakes overheat' a hazard? No, the real hazards are:

- loss of braking (i.e. a functional hazard)
- fire due to brakes overheating (i.e. a physical hazard (Fig. 6.1))
- any other direct consequence

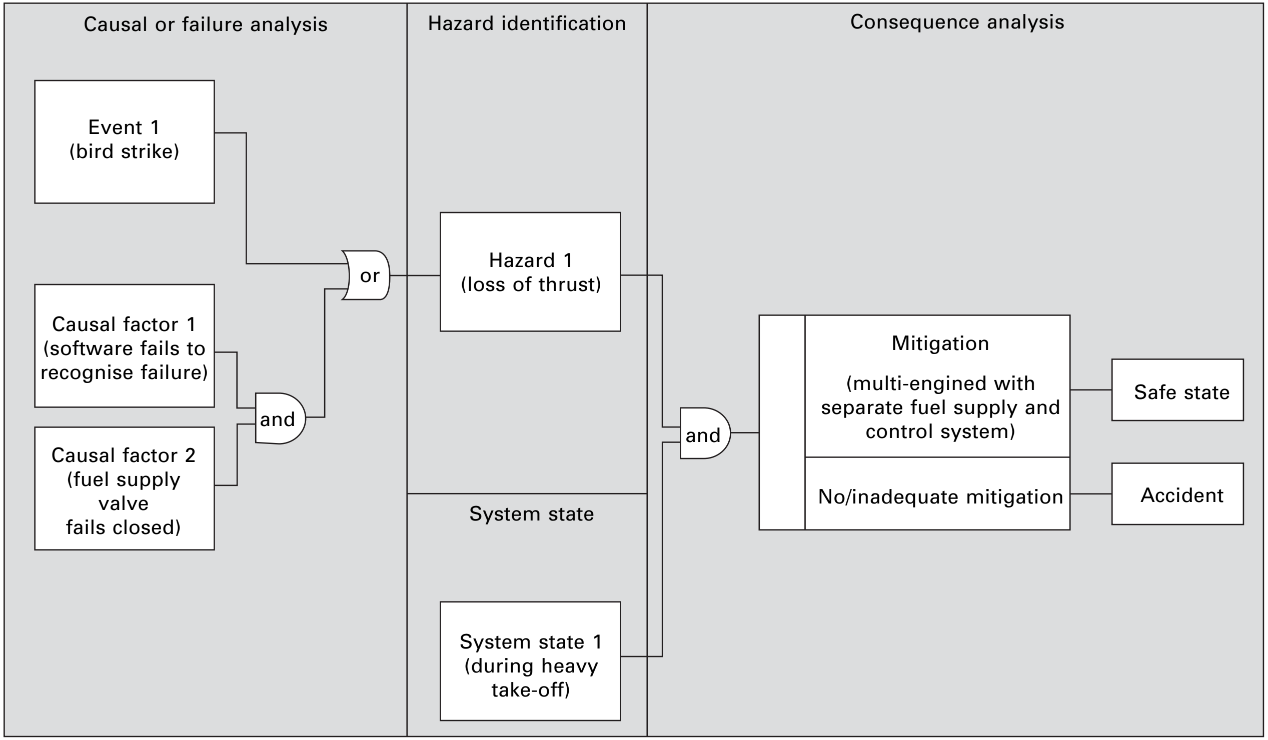
So, do not confuse causes with hazards (i.e. loss of brakes can be caused by brakes overheating).



6.1 C-130 main landing gear fire (obtained with kind permission from *Lockheed Martin Service News* Vol. 4 No. 3, July–Sept 1977 (second printing Aug 1982).

A Safety Assessment involves detailed predictions of the likely hazardous behaviour of a system, often before it enters service. Before such an assessment can be made it is necessary to understand the nature of hazards and how system failures/inadequacies contribute to accidents and incidents. There is a causal chain from causes to hazards to accidents. Rhys (2002, page 4) defines an accident as: 'an unintended event or sequence of events which causes death, injury, environmental damage or material damage'. The accident is the undesired outcome, rather than the initiating event or any intermediate state or hazard.

Figure 6.2 shows the relationship between a hazard, the causes that can lead to it occurring and the consequence or accident that follows the occurrence. Understanding


Causal or failure analysis
Hazard identification
Consequence analysis
Event 1 (bird strike)
Causal factor 1 (software fails to recognise failure)
Causal factor 2 (fuel supply valve fails closed)
and
or
Hazard 1 (loss of thrust)
System state
System state 1 (during heavy take-off)
and
Mitigation
(multi-engined with separate fuel supply and control system)
No/inadequate mitigation
Safe state
Accident

6.2 Accident, hazard and cause relationship.

this model leads to better management of the term 'hazard' by separating (but not ignoring) the consequences and the causes. Note that any single hazard may lead to a variety of different outcomes, some of which will be accidents and some relatively unimportant.

Example

The release of toxic fumes (the hazard) may have several outcomes (accidents), such as

- a few individuals becoming ill
- death of a single maintenance person
- multiple fatalities of crew and passengers.

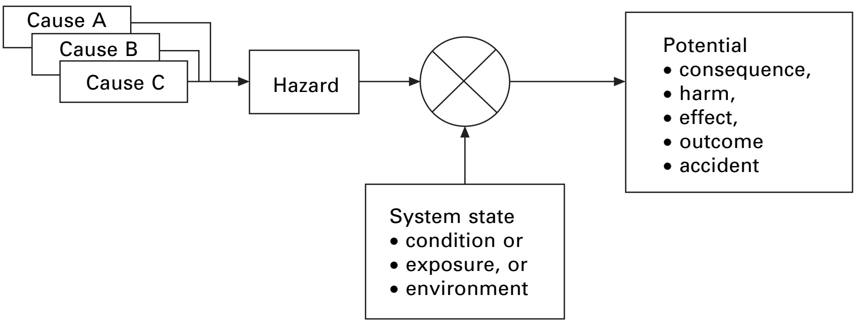
Similarly a particular hazard may have several possible causes, either acting alone or together.

Example

Consider the hazard 'loss of engine power'. This could be caused by:

- water in the fuel system
- no fuel in the tank
- crimped fuel line
- loss of ignition
- any other cause.

The FAA (ASD-100-SSE-1 Rev 7D, Fig. 4.1-1) also make this distinction between hazards and their causes as illustrated in Fig. 6.3. The causes are events that lead to a hazard or hazardous condition. Causes can occur by themselves or in combinations and can be technical and procedural in nature. The hazard is the adverse event that occurs as a result of the cause(s). A hazard is defined as 'anything real or potential,



6.3 Hazard vs. causes.

that could make possible or contribute to an accident. A condition that is a prerequisite to an accident.' It is vital to link the hazards to the accidents they could cause because the risk assessment is applied to the accident outcome (see Chapter 4).

Hazard control is concerned both with preventing the hazardous condition from happening and from stopping it from becoming an accident (e.g. by managed mitigations, as illustrated in Fig. 5.2). Note that once a hazard exists, it does not always turn into an accident and for any accident there is rarely only one single cause. Generally there are a number of causes and events which combine like links in a chain to create an accident. The illustrations in Figs 5.2, 6.1 and 6.2 are quite successfully demonstrated in the NASA Challenger accident:[1]

Example: the NASA Challenger accident

In 1986, the space shuttle Challenger exploded 73 seconds after lift-off from the Kennedy Space Center in Florida. The following sections describe the chain of events involved in this catastrophic loss.

Hazard

- fuel (liquid hydrogen and liquid oxygen) tank ignition.

Incident (initiating event)

- lift-off of a shuttle when the ambient temperature was low.

Accident

- Flight 51-L explodes 73 seconds after lift-off.

Consequences

- loss of seven astronauts
- loss of a multi-billion-dollar shuttle
- suspension of the shuttle programme for almost three years
- safety culture of NASA considered suspect.

Direct causes

- Solid rocket motor rubber O-ring failed to seal properly because of its reduced pliability from exposure to low temperature prior to launch.
- Heavy wind shear during the last 45 seconds of the flight caused higher than normal bending of the joints of the solid rocket motor sealed by the rubber O-ring.
- High-pressure hot exhaust gases from the solid rocket motor eroded through the cold rubber O-ring (aided by the higher-than-normal bending of the joint) and contacted the external fuel tank.

[1] Tailored from http://www.uscg.mil/hq/g-m/risk/e-guidelines/html/vol2/01/v2-01-01.htm#121 (last available in September 2004).

Systemic causes

- ineffective management assessment of identified issues
- temperature effects on O-rings not well understood by launch safety personnel
- no definite operating envelope was set for O-rings
- design specification did not include a temperature range
- prior evidence of O-ring problems was not viewed as a problem
- O-ring damage was observed on 15 of 25 missions
- eventually, O-ring damage was viewed as acceptable.

Safeguards not provided (causes)

- effective O-ring design
- timely communication of temperature limit for O-rings in this service.

6.2 Identifying hazards

When we look at any system we can distinguish between two distinct groups of hazards: endogenous and exogenous – see Table 6.1 (which is a useful reminder to consider hazards resulting from causes outside the system's boundary).

Once a hazard is identified, we need to decide on the severity of the hazard (if we are using the goal-based approach) or the severity of the potential accident (if we are using the risk-based approach). The severity is determined by considering the effect (or harm) of the potential outcome of the hazard within the context of the system state.

For this explanation to make sense, a few clarifying explanations are needed:

- A *system* can be defined (ASD-100-SSE-1 Rev 7D) as: 'a composite of people, procedures, materials, tools, equipment, facilities, and software operating in a

Table 6.1 Hazards

Endogenous hazards	Exogenous hazards
Arise from causes within the system	Causes by external influences outside the system boundary
It implies that something has gone wrong due to: • system faults, which are a specific state of a system (e.g. cross connection of wires) • physical hazards, which are always present in a system (e.g. hot surfaces, sharp corners, etc.) • functional failures, which usually require an initiating event (e.g. components or equipment failures) • human failures (e.g. controlling errors, maintaining errors, monitoring errors, etc.), both with or without functional failures.	Results from the following environmental causes: • physical (e.g. weather) • peer platforms (e.g. other aircraft), • people (e.g. sabotage, hijacking, etc.).

specific environment to perform a specific task or achieve a specific purpose, support, or mission requirement.'

- *Hazards* are properties of an entire system and may be defined at any system level.[2] However, it is essential to select the right level:
  - A common mistake is to select it too low (e.g. within a Piece-Part FMECA, see Appendix A), which results in too many hazards, no system properties, expensive (impossible) to track and over-engineering.
  - If it is selected too high, then it is hard to ensure the identification and management of all hazards.

Example of hazard levels

To continue our braking example from paragraph 1 above, the hazards can be broken down into its constituent elements/subsystems as follows:

1.	loss of controllability	– Level A
1.1	braking	
1.1.1	loss of braking	– Level B
	• brake pipe ruptures	– Level C
	• no brake fluid	– Level C
	• brake booster failure	– Level C
1.1.2	uncommanded braking	– Level B
1.2	steering	
1.2.1	loss of steering control	– Level B
1.2.2	over-steer	
1.2.3	etc.	

This example demonstrates that the Level B hazards would probably (but not necessarily) be the appropriate hazard level to manage, because: Level A might be too vague by not focusing on any specific system, and Level C is designated as contributing causes/failures to the level of hazard, whereas Level B directly leads to the accident.

- The *system state* is an expression of the various conditions, characterised by quantities or qualities, in which the system can exist. For any given hazard, the system state can be described in any of the following terms:
  - operational/ procedural terms
    (e.g. air-to-air refuelling, instrument landing system (ILS) approach, etc.),
  - conditional terms
    (e.g. instrument (IMC) vs. visual meteorological conditions (VMC), low altitude, rough terrain, etc.)
  - physical terms
    (e.g. electromagnetic environment effects, precipitation, low rotor speed, low hydraulic pressure, high impedance, etc.).

[2] See also Chapter 8 for more information regarding a 'system'.

For any given hazard, not all system states result in equal severity ratings.

Example

Loss of one engine in a multi-engined aircraft at mid-altitude and airspeed, would not be likely to result in a catastrophic accident. However:

- Loss of one engine at low airspeed, low altitude and high gross weight has the potential to result in loss of control or lift. In this system state, the end result of the hazard would be catastrophic.
- Loss of an engine due to uncontained failure (e.g. loss of a propeller) at high altitude may cause explosive decompression if the fuselage is at a high pressure differential. In this system state, the end result of the hazard is likely to be hazardous.

Most regulatory authorities expect the assessment to consider the worst-case system state. If desired, other system states may be considered, but only in addition to the worst case.

The following sections will consider some of the causes which can lead to a hazardous situation. Thereafter we will briefly consider some of the safety assessment tools and techniques available to identify and assess these hazards and their causes.

6.3 Equipment failures and faults

A failure can be classified as the inability of an item to perform its intended function within previously specified limits. The following section will attempt to distinguish between various types of failure, as well as provide some advice on how to mitigate them.

6.3.1 Active vs. passive failure

Active failure

An active failure is one that produces immediate adverse effect (e.g. loss or degraded engine functionality). This type of failure can be permanent or intermittent.

Example: Antonov AN-28, Ulemiste Airport, Tallinn, Estonia, 10 Feb 2004

Witnesses reported a ‘loud noise’ coming from the aircraft as it was climbing through 130 ft after take-off in darkness with snow and sleet. It veered right, lost height and crashed about 1 km from the runway. Two fatalities. The flight engineer, injured in the accident, reported an engine ‘explosion’.

Flight International, 20–26 Jan 2004

Passive/latent/dormant failure

In some systems there can be a fault in one channel which leaves the system operating but the presence of the fault is undetected. This type of failure produces no immediately adverse effects and goes by unnoticed. Usually not harmful in isolation but can interact with other situations to become very active (e.g. failure of a back-up system). Can be permanent or intermittent. These are usually mitigated through the use of monitors or specific checks (such as during maintenance or via flight check-lists).

Example: BAC1-11, Blossburg, 23 June 1967

The probable cause of this accident was the loss of integrity of the empennage pitch control due to a destructive undetected in-flight fire, which originated in the airframe plenum chamber.

6.3.2 Obvious vs. non-obvious failures

These are a derivative of active/passive failure conditions, but with a novel twist brought in during the introduction of digital technology. Many computer-based information systems act in an advisory manner, where an obvious failure can be tolerated but a 'plausible but wrong' output is hazardous.

Example: Boeing 747-200F, London Stansted, December 1999

Thirty-seven seconds after take-off the aircraft began a left turn as part of the departure routing. Eighteen seconds later, the aircraft was pitched at 40° nose down and banked left close to 90° just prior to impact with the ground. During the investigation the commander of the previous flight of the accident aircraft reported that the captain's attitude indicator (ADI) was unreliable and would indicate wings level during turns in either direction.

ICAO Journal Number 1, 2002, p. 14.

Note that a fail-safe design (see Chapter 7) may include monitoring software running in parallel with the actual application, providing a sanity check on the outputs displayed. In this instance, a significant issue is how to avoid common cause or latent failures, such as the operating system failing to run the monitor. One way to address the latter is to introduce a 'hardware watchdog' to confirm the execution of the monitoring function.

6.3.3 Independent vs. dependent failure

Independent failures

Independent failures, which separately do not degrade safety significantly, may combine to produce a hazardous situation. There may be a combination of active failures and passive failures, such as dormant failure of a standby system before the main system fails or an undetected leak of flammable vapour followed by a spark caused by an electrical failure.

Example: Antonov An-24, Ndjole, Gabon, 17 Jan 2004

The aircraft circled, apparently with navigation equipment failure following a total electrical failure. The crew failed to locate their airfield and eventually the aircraft ran out of fuel and hit a low hill. Seven fatalities (all on board).

Flight International, 20–26 Jan 2004.

Dependent failures

These failures are those caused by common modes or events, or which have a cascading effect. High levels of safety needed from essential systems are usually achieved by some form of 'fail-safe' design as detailed in Chapter 7. However, in spite of these precautions, there are various threats to the independence of the channels of redundant systems which may lead to multiple failures at higher rates than would be forecast by calculating the multiple rates from the failure rates of the component channels alone (Lloyd and Tye, 1995).

A common cause (or a common mode) failure concerns the possibility that system failure involving multiple item failure may occur due to a common cause, i.e., the loss (during some critical period) of multiple or redundant paths/components/parts/functions due to an underlying common mechanisms/faults/phenomenon. A common mode failure is a failure which has the potential to fail more than one function and to possibly cause an initiating event, or other event(s), simultaneously.

One of the most widely used assumptions in quantitative analyses is that failures of components or sub-systems are independent of any other failures. This assumption greatly simplifies the analysis and is therefore very convenient. Although most essential and critical systems employ some sort of redundant technique, closer scrutiny soon makes it apparent that many of these systems have a 'single element' (or 'common point'), the failure of which will cause multiple channel failures. This means that any conclusions drawn from these results need to be evaluated for sensitivity to common cause failures. We need to constantly ask ourselves whether this assumption is realistic and, if it is not, whether the analyses need to be modified to take account of any common cause failures.

Example: common part failure

Three totally independent flying control systems may merge together in a common part – the pilot's control column. A failure of this common part causes total system failure.

Example: DC10, Paris, 5 March 1974

Defective closing mechanism of cargo door caused it to detatch in flight. Sudden depressurisation led to disruption of floor structure, causing six passengers and parts of the aircraft to be ejected, rendering no. 2 engine inoperative and impairing the flight controls (tail surfaces) so that it was impossible for the crew to regain control of the aircraft.

Example: common cause failures

- A fire in a compartment might destroy all the channels of a system running through that compartment.
- Contaminated hydraulic fluid could cause all the channels of the hydraulic system to fail.
- Mechanical failures in an electrical loom (due to chafing and then short-circuit).
- Identical software in a dual redundant system will fail when exposed to the same inputs; jamming of a mechanical system (either due to failure or due to FOD); overheating of avionic equipment, etc.

Protection can be provided by careful design, as well as through the use of disconnect devices.

Example: cascade failure

A single failure may overload the remaining channels, thereby increasing the probability of their failure. For example, In a two-channel system, each channel with a failure rate of 1 in 1000 hrs, the probability of any one of the channels failing is 3×10^{-3}. So in a period of a million hrs, there will be 2000 failures. The probability of two channels failing is $(10^{-3})^2$, i.e., one double failure in a million hrs. However, if the failure of the first channel will cause a ten-fold increase in the probability of the second channel also failing, then the probability of total failure is $(1/1000) \times (1/100)$, i.e., ten such double failures in a million hrs.

From this example it is therefore evident that the combined failure rates increase proportionally with increase of risk under the added load and hence, it is important to take this into account and preferably design channels to cope with the added load without materially worsening the failure rate (Lloyd and Tye, 1995). Using MTBF data alone to obtain the multiple failure probability is thus bound to be flawed, because the MTBF does not take account of the 'overstrain' condition.

Example: Concorde SST, Flight 4590, Paris, 25 July 2005

An initial minor failure (e.g. a deflated tyre) causes a cascade of events. The Concorde caught fire shortly after takeoff from Charles de Gaulle Airport on a charter flight to New York. The pilots lost control and the plane crashed into a hotel restaurant. Subsequent investigation revealed that a metal strip left on the runway by another plane gashed one of the Concorde's tyres which blew out sending a piece of rubber into the underside of the wing which sent a shockwave which ruptured a seam in the fuel tank. An electrical wire severed by another piece of rubber sparked and ignited leaking fuel that started an uncontrollable fire. Power was lost to the No. 1 and No. 2 engines which led to loss of control of the aircraft and subsequent crash.

The essence of the problem is that we cannot actually construct and operate absolutely independent systems which are not vulnerable to some sort of common failure. The challenge lies in:

- identifying those parts of a system which are vulnerable to common cause failures
- identifying all reasonable foreseeable sources of common cause failure
- accounting for the probability of common cause failure is our safety justification for the application of the following defences:
  - segregation (i.e. mechanically and electrically) of redundant systems
  - use of dissimilar redundancy[3] (e.g. VC10 flying control system, where the elevators and ailerons are powered by the main electrical systems (i.e. electro-hydraulic actuators) and the tailplane and spoilers are powered by the main hydraulic system).

6.3.4 Wear-out vs. random failures

Wear-out

Wear-out occurs at the end of useful life. These modes are reasonably well understood and their rate of occurrence is generally considered to have a 'bathtub' characteristic (i.e. relatively high failure rate during both the early and late phase, with a middle portion of useful life where the rate is relatively low and constant as illustrated in Fig. 10.2).

Random

Random failures occur, as the name suggests, randomly and are the result of degradation mechanisms within the system. Often evaluated by means of failure rates (e.g. failures per hour of operation) or due to physical causes involving a range of mechanisms (e.g. lighting or problems during manufacture, installation or maintenance). Generally it is possible to quantitatively predict, with reasonable accuracy, failure rates for this type of failure.

6.4 Hazards of a normal functioning system

We can distinguish between normal functioning and degraded functioning.

[3] Regarding dissimilar redundancy: dissimilarity can be both in hardware and software. Software dissimilarity is achieved by producing two separate software requirements/solutions and by the use of two separate teams. Increased workload is countered by being able to limit the amount of testing by virtue of the replication of computation. The two software lines run asynchronously in two processes and their outputs are 'added' or compared to ensure that no demand is made incorrectly. This achieves high integrity but at the expense of availability, so that where passivity cannot be tolerated (e.g. fly-by-wire control systems) such architectures must have an alternative central lane in the event of a failure.

6.4.1 Normal functioning system

The safety issues associated with the system when it is working correctly should not be neglected. In this context, 'working correctly' means that the way hardware and software (which have not failed) perform together as a system (including the people involved) results in an unsafe situation. Typical examples of a normal functioning system causing hazardous conditions include a missile system that locks on to the wrong target, unwanted operation of stick-pusher near the ground, pilot error, etc.).

Example: DC8, Toronto, 5 July 1970

Preliminary information from the flight recorder indicates that, during the approach-to-land, the approved procedure for arming the ground spoilers for automatic touch-down was not followed. For an undetermined reason the ground spoilers were prematurely deployed, momentarily, resulting in a rapid descent, heavy impact with the runway causing 109 fatalities and structural damage to the aircraft.

The subject 'pilot error' is sufficiently wide to justify several volumes. However, although many accidents are attributed to pilot error, the arrangements of equipment (e.g. displays, controls, levers, switches) and their method of operation is often such that, taking account of human fallibility (or Murphy's Law[4]), the accident was one day bound to happen (Lloyd and Tye, 1995) (see example on page 82).

Errors classifed in terms of the part of the human information processing system at which the fault occurs (Edwards, 1999) are given in Table 6.2.

Table 6.2 Human processing errors

Type of error	Possible causal factors
Failure to detect signal	Input overload; adverse environment
Incorrect identification of signal	Lack of differential cues; inappropriate expectation.
Incorrect signal recalled	Confusion in short-term memory; distraction before task completed
Incorrect assessment of priority	Values inadequately defined; complex evaluation required
Wrong action selected	Consequences of action misjudged; correct action inhibited
Incorrect execution of action	Clumsiness due to excessive haste; selection of wrong control device

[4] 'Murphy's Law' has numerous variations, but in this context 'if it is possible for something to be done wrongly then one day it will be done wrongly'.

Example: 747-400, Jeddah, 7 April 1999

The pilots failed to switch on their pitot/static heating systems as the 747-400 entered icing conditions not long after leaving Jeddah. Frozen pitot and static ports 'robbed' the aircraft of airspeed and altitude information leading to crash and death of two pilots and four cabin crew members (no passengers on board). The reports cited inattention by the crew, who were talking to the cabin crew on the flight deck at the time the flight entered icing conditions.

The general approach to understanding the hazards associated with a 'normal functioning system' is to achieve a good understanding of the way the system performs and hence build confidence in its safety integrity. It should be noted that no specific measurements or numerical probabilities are produced, it is simply confidence from clear understanding. It follows that the methods (e.g. SFD, block text diagrams, SLD, etc., see Appendix A) used to achieve this understanding are not strictly formal and vary with the system complexity. The basic steps are:

- Identify the top events (i.e. the feared event).
- Delineate the system functions (hardware, software and human interactions) for each scenario (the way the system is prepared and used) to achieve an understanding of how they relate to each top event in turn.
- Deduce the following:
  - probability of an accident occurring as a result of normal operation
  - the benefits of safety redundancy
  - any operator or maintainer activities which are vital for safe operation. Where an analysis identifies some indication to, and/or action by, the flight crew, cabin crew or maintenance personnel, the following activities should be accomplished:
    (i) Verify that any identified indications are actually provided by the system.
    (ii) Verify that any identified indications will, in fact, be recognised.
    (iii) Verify that any actions required have a reasonable expectation of being accomplished in a reasonable manner.

6.4.2 Degraded functionality/performance

The performance of a system is the degree of accuracy with which it performs its intended function. Performance can be affected by the following factors:

- Failure-free operation. When operating without failure the factors affecting performance may be the variation of tolerances within the system itself; the variations of aircraft response; the effect of environmental conditions (e.g. turbulence, windshear, temperature, icing, runway surfaces, etc.); and the variances of other influencing systems (e.g. ground systems which affect approach, navigation and auto-landing systems) (Lloyd and Tye, 1995).

  Lloyd and Tye (p. 119) arbitrarily allocated different reasons for performance variations into three main groups:

  (i) Those which directly affect the physical make-up of the system (e.g. manufacturing tolerances, maintenance adjustments, etc.). These can lead to variations in the response of the system to particular stimuli.
  (ii) The basic competence of the system in carrying out the job it is designed to do.
  (iii) Those which indirectly affect the way the system responds in given circumstances. These are largely environmental (in that temperature, vibration, etc., are prime contributors to system performance) and also include characteristics of input supplies (e.g. voltages, hydraulic pressures, pilot action/inaction, etc.).

- Failures. A failure can result in degraded performance. These failures could be active or passive (see also section 6.3.1):
  - Active failures would result in immediate performance deviations. For example, the ability to maintain control after the loss of one engine on a multi-engined platform.
  - Passive (or dormant) failures could result in degraded performance without giving a definitive indication to the crew. This could go undetected until discovery during maintenance checks, or until discovered too late at a time when functionality is required. An example of the latter would be a dormant failure in an auto-land system where accuracy of the ILS centre line may be compromised.

Accidents produced by a lack of system performance have usually been in the field of powerplant or control systems performance (e.g. lack of sufficient controllability to recover from flight upsets) or navigation systems (e.g. automatic landing systems degraded due to variations produced by the ground equipment, accuracy of ILS receivers, auto-pilot accuracy during ILS approach). Minimum performance standards have been developed for many of these systems, either by the regulatory authorities (e.g. FAA), or by organisations such as the Radio Technical Commission for Aeronautics (RTCA).

To a large extent, system performance is not an airworthiness concern unless it affects an essential or flight-critical function. This is even more applicable to circumstances where the cues for pilot detection are uncertain, or if there is insufficient time for the pilot to react and recover from a performance deficiency. Degraded performance may require a reduced operating envelope (e.g. reduced speed or altitude) or reduced demand on the system by shedding loads (e.g. electrical) or by altering the flight plan. Alternatively, it may be practical to demonstrate that the combined probability of the failure and that of other conditions (e.g. gusts) necessary to produce a hazardous situation is acceptably remote.

A method of performance analysis involves establishing a statistical distribution for each critical performance parameter (when carrying out the tasks assigned to it, the 'output' of a system can be expressed as statistical distribution which describes the probabilities that the system output will reach or exceed any particular values). From such a distribution determine the probability that the performance of the system will be such as not to create an unacceptable hazard/risk.

In taking account of all these variables, it may be unreasonable to assume that each variable is at its most disadvantageous limit, so that it is necessary to take account of the statistical distribution of the variables in order to arrive at sensible conclusions. For more information on evaluating system performance, see Lloyd and Tye (1995, Chapter 8, pp. 60–67).

6.4.3 Unwanted operation

A system can operate, and in doing so, cause a hazard because it does so when not required or expected. For example, during low-level flight, unwanted operation of the 'stick shaker' could be hazardous. Likewise the unwanted operation of a warning system when there is nothing wrong with the monitored system. It could either add to crew workload, or lead to the crew not trusting the warning system (like the boy that cried 'wolf' once too often).

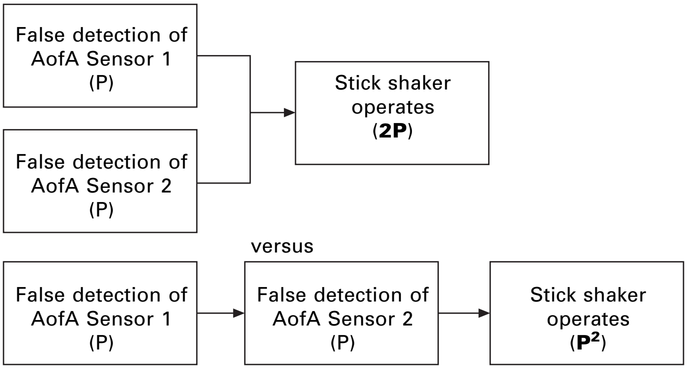
Example: Delta Airlines 737, September 2004. Salt Lake City

The co-pilot suffered a burned retina when a high-power laser 'painted' his aircraft on final approach. The aircraft landed safely and the US Transport Security Administration is now investigating the case.

Sourced from *Aerospace International*, Nov. 2004, p. 8

Note: High-power lasers are being used in missile protection systems such as DIRCM (directional infra-red countermeasures). As shown by this example, these lasers can cause eye injuries to third parties.

The safety assessment therefore needs to consider the implication of unwanted operation (for instance via the functional hazard assessment as a specific functional failure mode applied to specific flight phases). The usual design practice (to ensure high system integrity) is to design parallel multiplex systems. However, when it is important to avoid unwanted operation, items may be put in series to avoid unwanted operation (Lloyd and Tye, p. 47) as demonstrated for the angle-of-attack (A of A) sensors in Fig. 6.4.


False detection of AofA Sensor 1 (P)
False detection of AofA Sensor 2 (P)
Stick shaker operates (**2P**)
versus
False detection of AofA Sensor 1 (P)
False detection of AofA Sensor 2 (P)
Stick shaker operates (**P²**)

6.4 Example comparing system reliability for parallel vs. series architectures.

The second solution above has its limitations. For instance, the series system would also mean that if one detector fails to function, then the system may fail to operate when required to do so. Practical judgement will be required to balance the probability of failure to operate when wanted against the probability of operating when not required. It may be more desirable to add a ‘comparator’, which compares the results of the two detectors, monitors correct functionality and then prompts the stick shaker to respond. However, bear in mind that the comparator also has failure modes (which could include a dormant failure).

6.5 Systemic failures[5]

Systemic failures are due to human errors (e.g. mistakes, misconceptions, miscommunications, omissions) in the specification, design, build, operation and/or maintenance of the system. Errors in this case are taken to include both mistakes and omissions. Errors can be introduced during any part of the lifecycle and errors are caused by failures in design, manufacture, installation or maintenance. Systematic failures occur whenever a set of particular conditions is met and are therefore repeatable (i.e. items subjected to the same set of conditions will fail consistently) and thus apply to both hardware and software. It is difficult to quantify the rate at which systemic failures will occur and a qualitative figure based on the robustness of the development/build process is normally used. The probability of systemic failures is often evaluated by means of safety integrity (or development assurance) levels.

Systemic failures are often seen as indefensible (i.e. should not occur) but are hard to prevent. Any system is vulnerable to the vague fallibility of human beings. As the level of complexity increases, the proportion of systemic failures tends to increase. They play a major part in accidents and may in themselves lead to:

- errors by the crew because of poor arrangement of controls or instruments or warning systems
- errors by the maintenance staff because of a lack of proper information or because the design allows incorrect assembly (i.e. by cross-connection).

Systemic failures may arise from:

- a concept which is inherently flawed (i.e. a bad idea)
- specification (i.e. designing the wrong thing, e.g. due to omissions in the specification (see TWA 800 example on page 86))
- design or manufacture (i.e. building the thing incorrectly). For instance, failure to re-establish proper restraint of electrical cable looms relative to moving parts (such as control cables) has not only produced serious electrical failures (see Fig. 6.5), but has also resulted in severance of the control cables.
- Use and maintenance (i.e. mistakes, poor procedures, violating designers’ intentions (see faulty rigging example on page 86)).

[5] Often referred to as ‘systematic failures’.

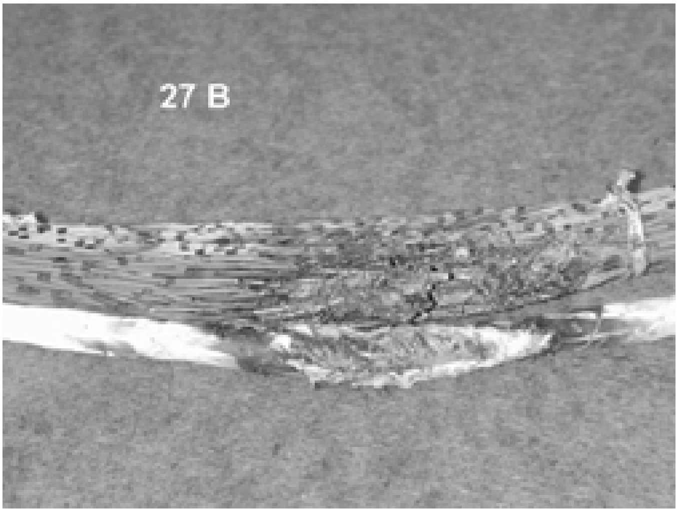


Photo courtesy of Lectromec
(http://www.lectromec.org/)

6.5 Short circuit on aircraft wing.

Example: TWA 800, New York July 1996

On 17 July 1996 a 25-year old Boeing Model 747 aircraft was involved in an in-flight break-up after takeoff from Kennedy International Airport in New York, resulting in 230 casualties. The accident investigation conducted by the National Transportation and Safety Board (NTSB) indicated that the centre wing fuel tank exploded due to an unknown ignition source. Although the ignition source could not be determined with certainty, the NTSB determined that the most likely source was a short circuit outside the centre wing fuel tank that allowed excessive voltages to enter the tank through electrical wiring associated with the fuel quantity indication (FQIS).

Opening remarks at the TWA800 hearing included (SFAR88):

> '…This investigation and several others have brought to light some broader issues regarding aircraft certification. For example, there are questions about the adequacy of the risk analyses that are used as the basis for demonstrating compliance with many certification requirements.'

Example: micro-switch rigging

An inadvertent stick-pusher operation was caused by the faulty rigging of duplicated micro-switches (the function of which was to change the datum settings of the system relative to incidence).

(Lloyd and Tye, 1995, p. 85)

Sources of design/development error include:

- failure to account for all likely environmental conditions (e.g. temperature effects, icing, etc). Failures caused by environmental effects may be minimised by proper design and installation, by experience of the components selected, by production quality control, and by appropriate environmental testing. However, should environmental failures occur, they could be common to all channels of a system employing similar hardware.
- the poor segregation of critical systems so that cascade or other multiple failures can occur
- the mixing of flammable substances and sources of ignition
- the location of electrical equipment below sources of contamination (e.g. toilets, galleys, etc.).
- software errors. Software does not 'fail' in the traditional sense of the word. If it does not perform its intended function, then a design error exists which must have been present since the software was first created. Software cannot directly *cause* harm (it is not toxic, does not have high levels of energy, etc.). Software can, however, *contribute* to accidents by causing failures through systems it controls and by misleading operators. The risk is increasing due to its growing scale and complexity, as well as playing an increasingly important role (e.g. authority). All software 'failures' are systemic failures.[6]
- manufacturing errors are potentially a prime source of common mode failures, particularly with electrical and avionic equipment. One of the objectives of the Safety Assessment should be to identify critical parts so that the manufacturing techniques and controls can be clearly specified. Manufacturing errors are basically caused by:

  - insufficient information on drawings (e.g. critical tolerances, stress relieving)
  - inadequate control of quality (e.g. not conforming to the design)
  - contamination (e.g. oil/grease in oxygen supply components)
  - damage (e.g. static electricity damage to circuit boards).

- maintenance errors have been the root cause of many accidents. Some of the following examples could have been avoided by design precautions, others by imposed procedures or labelling:

  - incorrect assembly (e.g. cross connection, fitting of wrong part, fitting valves the wrong way round, etc.)

[6] Determining the likely probability of these failure modes may be complicated, due to the fact that many functions may be routed through the same LRU. The effect of a processing error may be variable depending to some extent on the nature of the computation being made at the time. Moreover (Lloyd and Tye, 1995 p. 133), because of the discontinuous nature of digital computation, a correct outcome cannot necessarily be inferred or forecast from the correct completion of a 'bottom-up' (hardware) analysis. Even 'top-down' analysis (e.g. FTA) is not amenable to this type of problem.

Example: Viscount 732, 2 December 1958

Elevator spring tab operated in the reversed sense. This caused involuntary manoeuvres which overstressed the aircraft and caused the wing to break off. Work done to the spring tab mechanism during overhaul had been carried out incorrectly and the inspectors failed to observe the faulty operation of the tab.

- carrying forward defects or the incorrect diagnosis of defects
- leaving loose objects (e.g. tools) in places where they can cause damage, electrical shortage, or inhibit control surface movement
- putting wrong fluids into vital systems
- to lack of good housekeeping when making modifications and repairs (e.g. the leaving of swarf and loose rivets in fuel tanks)
- changing the maintenance schedule and/or philosophy (see MD83 example below)
- Damage inflicted during maintenance (see DC10 example below)

Example: MD83, Alaska Airlines, Jan 2000

At 28,000 feet, the crew reported that they were unable to control the pitch of the aircraft. Descending through 23,000 feet, the crew reported that they had regained control, declared an emergency, and received vectors to land. Shortly thereafter, control of the aircraft was lost and the MD-83 was seen ‘tumbling, spinning, nose down, continuous roll, corkscrewing and inverted’. The aircraft crashed off Point Mugu in 650 feet deep water with loss of 88 lives.

Probable cause was found to be a loss of airplane pitch control resulting from the in-flight failure of the horizontal stabiliser trim system jackscrew assembly’s acme nut threads. The thread failure was caused by excessive wear resulting from Alaska Airlines’ insufficient lubrication of the jackscrew assembly.

Contributing to the accident were Alaska Airlines’ extended lubrication interval, which increased the likelihood that a missed or inadequate lubrication would result in excessive wear of the acme nut threads. Alaska Airlines also extended the end play check interval, which allowed the excessive wear of the acme nut threads to progress to failure without the opportunity for detection.

Information tailored from:

- http://aviation-safety.net/database/record.php?id=20000131-0
- http://www.airdisaster.com/cgi-bin/view_details.cgi?date=01312000&reg=N963AS&airline=Alaska+Airlines

Example: DC10, Chicago, 25 May 1980

NTSB determined that the probable cause of the accident was the asymmetrical stall and the ensuing roll of the aircraft because of the uncommanded retraction of the left wing outboard leading edge slats and the loss of stall warning and slat disagreement indication systems. This resulted from maintenance-induced damage and led to the separation of the no. 1 engine and pylon assembly at a critical point during take-off. The separation resulted from damage caused by improper maintenance procedures which led to the failure of the pylon structure. Contributing to the cause of the accident were:

- the vulnerability of the design of the pylon attachment points to maintenance damage
- the vulnerability of the design of the leading edge slat system which produced asymmetry
- deficiencies in the FAA surveillance and reporting system which failed to detect and prevent the use of improper maintenance procedures
- deficiencies in the practices and communication among the operators, the manufacturer and the FAA, which failed to determine and disseminate the particulars regarding previous maintenance damage incidents
- the intolerance of the prescribed operation procedures to this unique emergency.

The probability of systemic failure cannot be determined. These risks cannot be quantified because no scientific law exists to characterise the vague possibilities of human beings in their intellectual endeavour (Murphy, 1991). Hazards due to systemic failures are dependent upon conditions that will not follow any predictable model or time based distribution. If a design deficiency exists it will manifest itself only when the circumstances are 'right', but equally it will always manifest itself when the circumstances are again 'right' (i.e. those systems subjected to the same conditions will fail consistently). Failures can be replicated and are predictable but not accurate.

Design deficiencies can occur at any stage of the design and development activities, from the early contract negotiation phase where general ideas and assumptions are being discussed, through to the detailed design and testing phases. Areas of particular risk are:

- designs which are very complex and hence difficult for one person to understand and probably impossible to test in all circumstances
- designs which are perceived to be very simple and attract very little effort or interest
- the interface between design areas, which is often constrained by departmental/company organisation and systems that incorporate items previously developed and accepted, but are not fully understood when integrated into the new systems and its new circumstances.

Do not forget to consider the behaviour of passengers. Many events such as the one below, which was probably caused by a cigarette, are predictable and have to be contained by careful design.

Example: Boeing 707, Paris, 11 July 1973

The probable cause of the accident was a fire, which appears to have started in the wash-basin unit of the aft toilet. It was detected because smoke had entered the adjacent left toilet. The difficulty in locating the fire made the actions of cabin personnel ineffective. The flight crew did not have the facilities to intervene usefully (from the cockpit) against the spread of fire and invasion of smoke. The lack of visibility in the cockpit prompted the crew to decide on a forced landing. At touch-down the fire was confined to the area of the aft toilets. The occupants of the passenger cabin were poisoned, to varying degrees, by carbon monoxide and other combustible products.

Unfortunately, identifying all the circumstances leading to systemic failures is seldom feasible. Design deficiencies cannot be eliminated, but they may be minimised. As we cannot cope with design deficiencies by 'analysis' and 'comparison' with an acceptable requirement, a radical approach is necessary. For this reason the required level of protection against systemic failures uses the concepts of:

- safety integrity level (SIL) (refer IEC 61508), or
- development assurance levels (see RTCA-DO-178B), or
- checklists (e.g. CCA and PRA, see Annex A), and
- regulatory requirements (see Chapter 3).

Safety integrity levels (SILs) and design assurance levels (DALs) are allocated to systems commensurate with the significance of any residual malfunctions. Essentially we establish the safety significance of the design and initiate a commensurate amount of 'design rigour' to minimise the risk of malfunction and to concentrate effort where it is most needed.

In accordance with IEC 61508, the required integrity level shall be inherited by (or passed down to) the components that implement the function. The initial SIL allocation shall consider:

- the degree of control that the function has over the system
- the independence of the other functions provided for the purpose of preventing the hazard occurring directly
- the time allowed for independent safety systems to intervene and mitigate the hazard
- the severity caused by the loss of function, degraded function, function provided when not required or the function provided inadvertently.

Guidelines such as RTCA DO-178B and IEC 61508,[7] contain much useful information which this book shall not attempt to duplicate, other than summarising that:

Development assurance is a process involving specific planned and systematic

[7] See Table B6 in EN61508-2: 2001 and Annex B in EN61508-7: 2001 for a useful overview of techniques and measures to avoid systemic failures.

actions that together provide confidence that errors or omissions in requirements or design have been identified and corrected to the degree that the system, as implemented, satisfies applicable certification requirements.

All systems are vulnerable to systemic failures and hence any safety analysis process should take into account their occurrence.

6.6 Safety assessment tools and techniques

There are a variety of tools and techniques available for assessing safety, which can broadly be classified into two categories. ‘Top-down’ analysis starts by identifying the accidents or failure conditions to be investigated, and then proceeds to derive the combination of failures and/or events which can produce them. ‘Bottom-up’ analysis starts with hardware failure modes which can occur and analyses the effects of these on the system and aircraft in order to determine the hazardous conditions which can occur. The objectives of these techniques fall into three broad categories:

1. Hazard identification techniques.
2. Causal techniques (looking back to see how hazards and accidents might possibly be caused).
3. Consequence techniques (looking forward to see what an event or situation might develop into).

Some of the techniques available serve more than one purpose; they not only identify hazards but examine consequences too. Nevertheless, it is vital to choose the correct combination of techniques and to tailor them to the particular system being assessed.

Why do we need all these assessment techniques? The reasons include:

- first, highly integrated and complex systems present greater opportunities for development error and undesirable, unintended effects.[8] It is generally not practical – and may not even be possible – to develop a finite test suite which conclusively demonstrates that there is no hazard residue
- the second reason is due to the variety of hazards and their causes. This was explored in the previous paragraphs which clearly show that we need an arsenal of analytical techniques, each with their own strengths and weaknesses. There is bound to be some overlap but that should only strengthen the safety argument and should not lead to additional work if cross-referenced properly
- finally, tools and techniques used should add value to the process by improving understanding of systems and its hazards.

The table in Appendix A provides a brief synopsis of the tools and techniques available. It also includes an indication (often very subjective) of the main advantages and limitations of each.

[8] Refer also to SAE ARP4754 Section 3.1.

6.7 Discussion

A safety assessment is an iterative process within the overall development of the system. The techniques and approaches touched on in this section can be used to different depths at different stages in the development process. Different projects use a variety of safety tools/techniques in numerous combinations. There is much guidance material and many standards available on this subject (e.g. SAE ARP4761, DEF STAN 00-56, MIL-STD-882, etc.).

Unfortunately, safety assessment tools and techniques are not agreed upon before contract closure and are used 'after the fact' to satisfy safety questions, and not as a useful tool to influence and optimise the design. Tools and techniques used should add value to the process by improving understanding of systems and hazards.

For this to occur we need to:

- be clear what the output should be by identifying safety effects clearly so as to provide a set of meaningful, useful recommendations
- pick the correct tools for the job, and use these tools at the appropriate stage in the process
- avoid overcomplication and to try to be as consistent as possible
- beware of increasing common mode failures with increased system complexity
- apply considerable judgement. Do not regard it as a 'write only' exercise.

An assessment to identify and classify failure conditions is necessarily qualitative. On the other hand, an assessment of the probability of a failure condition may be either qualitative or quantitative.

The extent to which structured methods/tools/techniques are applied is a function of the system's complexity and the system failure consequence, and will be more rigorous with increasing system complexity and severity of consequence (ACJ 25.1309 para 7.e). An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may (or may not) include estimated numerical probabilities. The depth and scope of an analysis depends on the types of functions performed by the system, the severities of failure conditions, and whether or not the system is complex. In considering the likely failure sequences, Lloyd and Tye (1995, p. 75) remind us to take account of the fact that, following a series of failures, the pilot himself will be under increased stress and may be more likely to make mistakes. Regardless of its type, an analysis should show that the system and its installation could tolerate hazards and failures to the extent that the applicable safety targets are accomplished in an auditable fashion.

Be careful of using too many techniques, as this could cause conflicts and confusion. However, ensure that you have used a sufficient range of tools that will ensure that something is not missed or overlooked. Remember that it is not the identified hazard which is the problem. If you have identified it, you can measure it, you can fix it, and you can control it. It is the unidentified hazard that causes concern. A hazard not identified is a hazard not managed. Do not take it too far (i.e. too low in system decomposition), as this will produce lots of output with little extra understanding. It is better to do it well, with insight, at high level, than merely mechanically at more detailed level.

Be careful of rigid, restrictive models and methods which can be counter-productive because they involve an inevitable simplification of the project domain and discourage subsequent free thought about the domain. Using a rigid model simply shifts the real analysis work backwards to the creation of the model itself. Sometimes exaggerated claims for the benefits of certain methods are made, but no particular method should ever be seen as a panacea. For example, a formal method may be just one of a number of techniques that, when applied judiciously, may result in a system of high integrity.

Particular techniques and notations should not be applied merely as a means of demonstrating a company's ability. Similarly, they should not be used to satisfy management whim, or merely as a result of peer pressure. Before a particular approach is applied, it should be determined whether it is really necessary. Potential reasons may be to:

- increase confidence in the system
- satisfy a particular standard required by procurers
- aid in tackling complexity, etc.

The identification of the failures and hazards should be carried out by a cross-functional team of pilots, engineers, logisticians and maintenance personnel, working in a series of facilitated brain-storming workshops. Ideally, all those involved must be current practitioners of the process under consideration, and involve a range of seniority and experience levels.

Complementary methods should not be dismissed lightly. Despite the mathematical basis of formal methods, they have no guarantee of correctness; they are applied by humans, with all the potential for error that this brings. Since system development is essentially a human activity, most methods depend on the quality and suitability of the personnel involved in applying the techniques. All of these require considerable judgement, and the careful identification and application of assumptions.

7
The fail-safe dimension

The best car safety device is a rear-view mirror with a cop in it.

Dudley Moore (1935–2002)

7.1 Introduction

There are many reasons why systems may fail. Murphy (1991) groups some of these reasons as follows:

- Failures due to component. These include failures of circuit breakers, capacitors, connectors, wiring, valves, pumps, etc.
- Failures due to performance and functional limitations. For instance, the accuracy of both the transmitters and receivers of an instrument landing system (ILS) on an aircraft. See also Section 6.4.2.
- System failures due to operator error: For instance, when the pilot does not select the correct autopilot mode to initiate a 'Go-around' manoeuvre.
- Failures due to design deficiencies. Software errors provide a typical example of this failure category, where failure will be repeatable under the exact same conditions. See also Section 6.5.
- Failures due to production deficiencies. Actual manufacturing tolerances may be greater than anticipated.
- Failures due to interference. Electromagnetic vulnerability of electrical parts of a system may lead to inadvertent or incorrect operation.
- Failures due to maintenance deficiencies. For instance, blocked pitot-static ports on an aircraft.
- Failures due to environmental deficiencies. Excessive environmental conditions (e.g. vibration, temperature, etc.) could cause premature failures.

7.2 Defences against failures

The first line of defence against hazardous failure conditions is avoidance, in which design and management techniques should be applied to minimise the likelihood of faults arising from random or systemic causes (see Section 6.5). The second line of defence is based on the provision of fault tolerance as a means of dynamic protection during system operation. Possible approaches include:

- fault masking, where the system or component is designed to survive potential failures with full functionality

- graceful degradation (sometimes referred to as fail-soft), where the system or component is designed so that in the event of a failure its operation will be maintained but with some loss of functionality and
- fail-safe, where in the event of a failure, the system or component automatically reverts to one of a small set of states known to be safe, and thereafter operates in a highly restricted mode. This may involve complete loss of functionality, or reverting to back-up/redundant features.

The high levels of functional safety needed from essential systems are usually achieved by some form of fail-safe design. The fail-safe design concept considers the effects of failures and combinations of failure in defining a 'safe' design. The application of the fail-safe concept is probably the most important discipline involved in the design of systems and operations. It has evolved over many years.[1] The definition first appeared in the dictionary in the mid-1950s after the final reports on the Comet disasters were published.

The Collins Dictionary (2003) defines fail-safe as:

- 'designed to return to a safe condition in the event of a failure or malfunction'
- '(in the case of a nuclear weapon) capable of being deactivated in the event of a failure or accident'
- 'unlikely to fail; foolproof'
- 'to return to a safe condition in the event of a failure or malfunction'.

The fail-safe concept implies the acceptance of the notion that there is no single element or process in any part of a system that can ever have a sufficient level of reliability to be relied upon without some manner of alternative back-up or protection.[2]

The CS/JAR/FAR25.1309 airworthiness standards are based on the fail-safe design concept. The following basic objectives pertaining to failures apply (*AMJ*25.1309, 2000):

- 'In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.
- Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be Extremely Improbable.'

[1] The evolutionary development of the fail-safe concept is described via real-world examples in an article in the *RAeS Aeronautical Journal*, see Howard (2000) paragraph 4.

[2] In general, the authorities (e.g. FAA) do not accept a probabilistic determination that a single failure be extremely improbable. However, experienced engineering judgement may enable an assessment that such a failure is not foreseeable. The assessment logic and rationale should be readily obvious so that a knowledgeable, experienced person would unequivocally conclude that the failure condition simply would not occur. When making such an assessment, all possible and relevant considerations should be taken into account, including all relevant attributes of the design. Extensive service experience alone showing that the failure condition has not yet occurred is not a sufficient reason to indicate that a single failure condition cannot exist.

7.3 Fail-safe principles

The fail-safe design concept uses the following design principles or techniques in order to ensure a 'safe' design (refer, *inter alia*[3], AMJ25.1309):

- **Designed integrity and quality, including life limits**, ensures intended functional reliability by minimising the occurrence and/or the effects of failures.

> Examples
>
> - Automatic retraction of spoilers/speed brakes in an emergency full-throttle climb.
> - Using safe-life, fatigue and fracture mechanics principles to schedule preventative and/or corrective maintenance actions.

- **Redundancy or back-up systems** enable continued function after any single (or other defined number of) failure(s). It also enables performance of an intended function even though a fault has occurred. Redundancy can also be used for diagnostics to detect faults. Redundancy is one way[4] to improve the functional reliability of a system. If critical elements can be duplicated the functional reliability of the system can be improved but with penalties of increased complexity, weight, space, power consumption and maintenance (i.e. preventative and corrective). Standby redundancy often involves switching over to additional units, which may or may not be identical to the ones that have failed. It is normally preferred to active redundancy if the associated disadvantages do not exclude it, since a greater reliability improvement can be expected if the standby units are operated less of the time. The disadvantages of standby redundancy are that the additional switching process has its own (possibly unacceptable) unreliability, the delay involved in switching over from a failed unit may be safety critical, and it does increase the risk of dormant failures.

There are three forms of active redundancy:

1. Full active redundancy is when any one of the two or three (or more) parallel units can satisfy the required function.
2. Partial active redundancy is when, for example, two or three parallel units must continue to operate in order to satisfy the required function.
3. Conditional active redundancy involves a 'voting system' and is used in applications such as digital/analog data processing when there is no simple way of identifying a failure.

Mauri (2000, p 21) advises that these are four ways in which redundancy can be employed:

[3] See also http://www.airweb.faa.gov/regulatory_and_guidance_library/rgfinalrule.nsf/frpart/f035bc081c98a51686256a4700642e17?OpenDocument

[4] Other ways to improve reliability include protection against environmental factors (e.g. use shock-absorbent mountings, de-rate parts, control temperature and humidity, etc.), improved design (reduce parts count, reduced stress, improve materials).

1. Hardware redundancy, e.g., one or more hardware components or 'channels'
2. software redundancy, e.g., different software versions doing the same task
3. time redundancy, i.e., enough time to initiate a safe recovery
4. information redundancy, e.g., data is coded in such a way that a certain number of bit errors can be detected or recovered.

- **Isolation** (especially electrical, physical and/or spatial separation/segration) and independence of systems, components and elements ensures that the failure of one does not cause the failure of another.

> Examples
>
> - Ensuring that fluid carrying hoses (and especially their connections) are not routed above sensitive electronics
> - Ensuring that redundant hydraulic systems are not vulnerable to a common cause of hydraulic fluid loss (e.g. common reservoir).

- **Proven reliability** ensures that multiple, independent failures are unlikely to occur during the same flight.

> Example
>
> - Continuation of flight after failure of one or more engines, hydraulic systems, flight control systems, etc.

- **Failure warning or indication** will provide detection of a condition before it can lead to a dangerous scenario.

> Examples
>
> - Failure flag showing false indication on a cockpit display
> - Applying 'leak before burst' criteria to pressurised pipes/vessels/containers.

- **Functional verification** is the capability for testing or checking the component's condition.

> Examples
>
> Using BIT (Built-in testing) for software driven avionics.

- **Flightcrew procedures** for use after failure detection enables continued safe flight and landing by specifying crew corrective action.

Example

The ability to override any malfunction of an automatic system such as an autopilot. Not only should the design facilitate the timely use of these recovery procedures, but also the cockpit management should seek out errors through constant cross-monitoring between crew members.

- **Checkability** provides the capability to check/monitor a system's/component's condition.

Example

Inspection windows to see if the landing gear is down and locked (or using miniature cameras installed for this purpose).

- **Failure containment** Limits the safety impact of a failure.

Example

Containing the effects which can result from a tyre burst or a turbine rotor becoming detached.

- **Designed failure path and damage tolerance** controls and directs the effects of a failure in a way that limits its safety impact.

Examples

- Crack propagation containment or through the use of alternative load paths
- Appropriately positioned structural sacrificial fuses
- Recovery after tyre burst during take-off/landing.

- **Fault tolerance** preserves the delivery of the expected (or a minimum) service despite the presence of errors caused by faults within the system itself (Avizienis, 1996).

Example

A failed generator disconnecting from a power supply bus, either automatically or manually, without loss of critical services. For instance, freezing a runaway actuator or trim system drive before dangerous control surface movement can be applied.

- **Error tolerance** considers probable human error in the operation, maintenance, and fabrication of the aeroplane

- **Margins or factors of safety** account for foreseeable but uncertain or undefined adverse conditions. The concept of margins of safety is central to the larger concept of aviation itself. Nothing is pushed or designed right to the edge.[5]

Example

Airframes are designed to take far more than the normal amount of abuse. Each bolt, for instance, is selected with a safety factor to cover possible material flaws, it is inserted into a fitting which is itself designed with a huge margin to cover possible fit problems and the fitting is part of an airframe design which was based on assumed flight loads which are likely never to occur.

- **Failure-survivability**, ensures that a failure does not result in a significant loss of performance. This is usually achieved by some form of separate back-up or multiple redundancy.

Examples

- standby instruments in the cockpit
- designing the electrical generation system to keep functioning after failure of one or more generators.

7.4 Applying fail-safe principles

The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design. Effective application of the fail-safe concept can result in the highest level of safety. However, its effectiveness is determined by the quality of the architectural design, the limits imposed by external influences and crew fail-safety. These three factors are now discussed.

[5] The advent of the 'cold war' led to efficient airframe requirements with materials 'pushed' closer and closer to their limits. At first, fatigue failures on these aircraft (i.e. B47, Comet) were attributed to poor static design. As the nature of fatigue in airframe structures became more understood, it was realised that even a 'correctly' designed airframe from a static load consideration would not necessarily reach its design life because of cyclic loading leading to fatigue. The 'safe life' approach was introduced with the primary aim to take into consideration the effects of cyclic loading on the airframe. Safe life involves rigorous fatigue testing of a full, representative airframe and certain components and subassemblies. Typically a 4¥-safety factor is used to take into account unknowns, assumptions and variables applicable to the fleet as a whole. The safe life approach however, does not take into account that high strength steel of limited toughness is used in critical, highly stressed parts of the structure. Steel in this category can fracture under load in the presence of relatively small defects, introduced at manufacture or during service. Fracture mechanics directly addresses the problem of the effect of a small flaw and the toughness of the material to predict time to failure at a given stress level.

7.4.1 Quality of the architectural design

The quality of the architectural design ensures redundancy, warning indications, etc. However, it is a fallacy to assume that survivability is assured just because redundancy is provided. Although most essential and critical systems employ some sort of redundant technique, closer scrutiny soon makes it apparent that many of these systems have a 'single element' (or 'common point'), the failure of which will cause multiple channel failures.

Examples

- It is not much use having two engines if false indication leads to the wrong one being shut down after an engine failure.
- Having two sets of independent instruments, but positioning them in such a manner as to prohibit frequent comparison of their displayed results.
- Having a dual redundant system but ignoring any potential common failure modes (e.g. common software, or common bus failure).

Howard (2000 para 4.37) advises that fail-safe architecture may be considered as comprising three main categories:

1. Primary/integral redundancy. This is often applied when it is the only practical fail-safe method possible.

Examples

- dual ignition on piston engines adopted in 1912 to counter the then notoriously bad reliability of spark plugs and magnetos
- dual tyres on nose-wheel landing gear
- triplicate hydraulic systems (i.e. utility-, booster- and auxiliary hydraulic systems)
- self-checking systems, such as CBIT (continuous built-in testing) in digital systems.

2. Secondary redundancy. Secondary redundancy architecture covers the range of design implementations and reconfigurations which can be referred to, or implemented, after failure of the primary system.

Examples

- standby instruments (such as the standby attitude indicator and the magnetic compass)
- mechanically lowering the landing gear following total hydraulic failure (e.g. due to loss of fluid).

3. Damage protection redundancy. This addresses failures which can cause hazardously cascading failure conditions (see Section 6.6.3) after a root cause

failure. Solutions involve aspects such as designing pressure vessels to leak before burst, using energy absorbing designs to contain high kinetic energy parts and providing survival equipment (e.g. oxygen systems and fire extinguishers), etc.

Example

Air France Concorde crash due to burst tyre rupturing the fuel tanks.

7.4.2 External influences

Any limits imposed by external influences, such as common-mode failures in redundant systems must be considered.

Examples

- Freezing of pitot-static ports robbing the aircraft of airspeed and altitude information.
- Duplicated system with each channel having a MTBF of 5000 hours. System failure probability should thus be 1×10^{-8} per hour, but if a common mode failure (e.g. HIRF) could find its way into the system at a rate of 1×10^{-5} per hour, then total failure probability reduces to
$(1 \times 10^{-8}) + (1 \times 10^{-5}) \approx 1 \times 10^{-5}$ per hour.

Due to the nature of cyclical loading on airframe structures and rotating parts in gas turbine engines, they are prone to fatigue. Mismanagement of fatigue in service may lead to the development of catastrophic events, which can occur without prior warning. Whilst system safety standards (such as FAR/JAR 25.1309) encourage redundant designs to achieve the fail-safe design concept, this becomes impractical for some critical structures and all critical engine rotating parts. However, a fail-safe design can still be effectively achieved applying factors of safety during design, applying life limits in service, and by ensuring responsible management of accumulated fatigue.

7.4.3 Crew operations

Fail-safety in crew operations is a subject which has become more prominent in the last decade (refer INT/POL/25/14), under terms such as ‘human factors engineering’. The fundamental principle is that if the design is vulnerable to human error, then an accident is bound to happen.

Example: Swissair MD-11 disaster, Nova Scotia, 1998 (229 fatalities)

Post-accident analysis showed that all onboard electrical power was lost at FL100 (FL = flight level). Crew diverted to an unfamiliar airport, at night with smoke in the cockpit and with oxygen masks on. In this high workload environment, a significant contributing factor to the crash was allocated to ‘disorientation of the flight crew and loss of control’ due to standby instrument location:

- In the MD-11, the small standby attitude, airspeed, altitude instruments were located at the bottom of the centre instrument panel, above the power levels.
- A retractable compass was installed at the top of the windshield to the left of its centre pillar.

A considerable vertical scan was required to complete an instrument cross-check, thereby risking Coriolis illusions from large up and down head or eye movements

(ICAO Safety Advisory Number 1 (2002), and *Avionics Magazine* (March 2002), p. 35)

The problem has become exacerbated due to increasing use of cockpit automation – especially for systems that do not keep the crew in the feedback loop and thus reduce their situational awareness.

Researchers from the University of Newcastle upon Tyne and the University of York have discovered that modern aircraft have computerised control systems that may over-tax the mental capability of pilots. The team says that although the air accident rate has been constantly decreasing over the last few decades, common cockpit designs are too complicated for pilots to make emergency decisions. The scientists found that during emergencies, pilots are overloaded with technical information which they are unable to process quickly enough. This could mean that wrong decisions are made at crucial moments. They are urging aircraft designers to achieve higher levels of safety by taking into account the psychological characteristics of pilots as well as their physical capabilities.

7.5 Summary

Fail-safe architecture stands squarely on the shoulders of basic reliability and system integrity:

- for hazards related to loss of a function, the reliability expected above can usually be achieved only through redundancy
- for hazards related to incorrect or misleading provision of a function, reliability and integrity must usually be sought through independent monitoring or comparison of redundant units
- for hazards related to the provision of a function when not desired, interlocks or other appropriate fail-safe mechanisms are normally used.

Fail-safety is effectively a large package of different techniques used for surviving failure and hence giving high functional integrity levels. No other design discipline makes a bigger contribution to safety than the correct application of the fail-safe design concept. Howard advises (2000, p. 517) that all accidents can be attributed to fail-safety implementations either breaking down, not having been adequately provided or are due to extremely remote multiple coincident failures.

Any design/safety analysis should consider the application of the fail-safe design concept. Special attention should be given to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally-similar functions. When considering such common-cause failures or other events[6] consequential or cascading effects should be taken into account in deciding whether they would be inevitable or reasonably likely.

[6] Some examples of such potential common-cause failures or other events would include rapid release of energy from concentrated sources such as uncontained failures of rotating parts or pressure vessels, pressure differentials, non-catastrophic structural failures, loss of environmental conditioning, disconnection of more than one subsystem or component by over-temperature protection devices, contamination by fluids, damage from localised fires, loss of power, excessive voltage, physical or environmental interactions among parts, human or machine errors, or events external to the system or to the aeroplane.

8

The system safety assessment

Life can only be understood backwards, but it must be lived forwards

Søren Kierkegaard (1813–1855)

8.1 History

Lloyd and Tye (1995) recall that the airworthiness requirements (e.g. BCAR and FAR) of the mid-20th century 'were devised to suit the circumstances. Separate sets of requirements were stated for each type of system and they dealt with the engineering detail intended to secure sufficient reliability'. Where the system was such that its failure could result in a serious hazard, the degree of redundancy (i.e. multiplication of the primary systems or provision of emergency systems) was stipulated. Compliance was generally shown by some sort of an FMEA.[1] For simple, self-contained systems this approach had its merits. However, systems rapidly became more complex. Complex systems[2] have a considerable amount of interfaces and cross/interconnections between the electrical, avionic, hydraulic and mechanical systems.[3] In addition, there are essential interfaces with the pilot, maintenance personnel and flight performance of the aircraft. The aircraft designer is thus faced not only with the analysis of each individual system independently, but also needs to consider how these systems act in concert with other systems.

Airworthiness Authorities could therefore not continue to issue detailed engineering requirements for each new application. Firstly, this would lead to a mountain of regulatory requirements and, secondly, this approach would inhibit innovation by leading designers into sub-optimum solutions. It therefore became necessary to have some basic objective requirement (see Section 5.2) related to an acceptable level of safety, which could be applied to the safety certification and release to service (RTS) of any system or function.

It was the auto-land system of the 1960s which first precipitated this new approach (Lloyd and Tye, 1995; Cherry, 1995) which, for civil transport aircraft, resulted in regulations such as JAR 25.1309 and its supporting Advisory Circular (AC25.1309,

[1] Failure mode and effects analysis, see Appendix A.

[2] A complex system can be identified as one whose architecture and logic are difficult to comprehend without the aid of analytical tools, whose safety cannot be shown solely by tests, and whose systems are not self contained (i.e. failure of one can influence the safe operation of another).

[3] Examples of such systems include those which enable automatic landing, high-authority auto stabilisation, full authority digital engine control (FADEC), etc.

undated). Only in the event of specific concerns are supplementary detailed requirements developed for particular types of systems or hazards. Examples of these additional requirements are:

- Special Federal Aviation Regulation (SFAR) 88 was developed to counter the fuel tank ignition concerns following the in-flight explosion of TWA800 in 1996.[4]
- Advisory Circular (AC) 20-138 was issued for airworthiness approval of global positioning system (GPS) navigation equipment for use as a VFR and IFR supplemental navigation system (AC20-138, undated).

This new approach required that, for safety certification, the designers conduct a thorough assessment of potential failures and evaluate the degree of hazard inherent in the effect of failures. With complex critical systems and functions the designer has not only to consider the effect of single failures, but also the effects of possible multiple failures – particularly if some of these failures are passive (see Chapter 6). The designers need to show that there is an inverse relationship (see Chapter 5) between the probability of occurrence and the degree of hazard inherent in its effect.

The designers also need to consider whether the design is such that it can lead unnecessarily to errors during manufacture, maintenance or operation by the crew. Furthermore, the designer needs to consider the environment that the systems would be exposed to, which could involve large variations in atmospheric temperature, pressure, acceleration (e.g. due to gusts), vibration, and other hostile events such as lightning strikes and icing.

The vehicle to report this demonstration, for the purposes of safety certification and release to service (RTS), became known as the system safety assessment (SSA). A system safety assessment can therefore be defined as: ‘a structured body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment. It is a collection of documents that, taken together, provides objective evidence that a system, if used in accordance with the listed recommendations and limitations, can be certified as being ‘safe enough’ to be released into service’

8.2 Aims and objectives of a system safety assessment

8.2.1 System safety aim

The aim of the system safety assessment programme is to ensure that (refer, *inter alia*, MIL-STD-882C para 4):

- Safety is designed into the system in a timely and cost-effective manner.

[4] The Boeing 747-400 centre wing fuel tank exploded due to an unknown ignition source. The NTSB determined that the most likely source was a short circuit outside the centre wing fuel tank that allowed excessive voltages to enter the tank through electrical wiring associated with the fuel quantity indication system (FQIS). Opening remarks at the hearing also indicated:‘…This investigation and several others have brought to light some broader issues regarding aircraft certification. For example, there are questions about the adequacy of the risk analyses that are used as the basis for demonstrating compliance with many certification requirements.’

- Hazards associated with each aircraft sub-system are identified, tracked, evaluated and eliminated or the associated risk reduced to an acceptable level.
- Historical safety data, including lessons learned from other systems are considered and used.
- Minimum risk is sought in accepting and using new technology, materials, or designs and new production, test and operational techniques.
- Actions taken to eliminate hazards or reduce risk to an acceptable level are documented.
- Retrofit actions required to improve safety are minimised through the timely inclusion of safety features.
- Changes in design, configuration, or mission requirements are accomplished in a manner that limits the risk from any hazard to an agreed acceptable level.
- Procedural and training requirements to support and maintain safety assumptions and assertions are identified.
- Design criteria for inadequate or overly restrictive requirements regarding safety are reviewed and new design criteria supported by study, analysis or test data are recommended.
- The programme team are made aware of system safety and how the design can be used to mitigate risks.
- Unwarranted complexity and novelty for novelty's sake are avoided.

8.2.2 System safety objectives

The system safety assessment's objectives are to:

- demonstrate that there is an inverse relationship between the probability of occurrence and the degree of hazard inherent in its effect
- demonstrate that the design is such that it cannot lead unnecessarily to errors during manufacture, maintenance or operation by the crew
- demonstrate that the systems are suitable for the environment that the systems will be exposed to.

The latter could involve large variations in atmospheric temperature, pressure, acceleration (e.g. due to gusts), vibration, and other hostile events such as lightning strikes and icing.

8.2.3 System safety design requirements

Safety is built in, not added on (see also fail-safe in Chapter 7). Safety requirements should thus be integrated in the design and development life-cycle, i.e., starting at concept generation. The general system safety design requirements include (refer, *inter alia*, AMC25.1309 and MIL-STD-882C:

- No single component failure, or single failure combined with a latent failure, shall result in a catastrophic event.
- For single component failures having a 'life dependent failure characteristic' (e.g. structural members) which can result in system loss, a failure rate and component

life must be established by means of accepted engineering mathematical models and methods, or accrued from actual tests (e.g. fatigue tests) or service experience.

- The elimination of identified hazards or reduce associated risk through design, including material selection or substitution. When hazardous materials must be used, those with least hazard risk throughout the life cycle of the system must be used.
- Hazardous substances, components and operations must be isolated from other activities, areas, personnel and incompatible materials.
- Equipment must be located so that access during operations, servicing, maintenance, repair or adjustment minimises personnel exposure to hazards such as burns, noise, electric shock, electromagnetic radiation, cutting edges, sharp points or toxic atmospheres.
- The severity and probability of any failure resulting from excessive environmental conditions such as temperatures, pressure, acceleration and vibration must be minimised.
- Warning information (instructions and warning/caution markings) to alert crew of unsafe system operating conditions must be provided.
- Design must minimise the severity and probability of human error in the operation or support of the system: incorporate fixed, automatic or other safety devices (with periodic functional checks); provide warning devices; develop procedures and training.
- Alternative approaches to minimise risk from hazards that cannot be eliminated must be considered. Such approaches include interlocks, redundancy, fail-safe design, system protection, fire suppression and protective clothing, equipment, devices and procedures.
- The power sources, controls and critical components of redundant sub-systems must be protected by physical and electrical separation and shielding.
- When alternative design approaches cannot eliminate the hazard, safety devices (e.g. alerts) and warning/caution notes must be provided.
- The severity of personnel injury or damage to equipment in the event of an accident (i.e. increase survivability) must be minimised.
- Software-controlled or monitored functions must be designed to minimise the probability of accidents or safety incidents.

8.3 The system and its relationship to safety

Before we can conduct a system safety assessment we first need to understand what we mean by the word ‘system’. A system is an assemblage of interrelated elements comprising a unified whole. From the Latin and Greek, the term ‘system’ means to combine, to set up, to place together. A sub-system is a system which is part of another system. When conducting a system safety assessment, the first step should therefore be to decide the level at which the safety assessment is aimed and scope the assessment accordingly.

DEF STAN 00-35 and SAE ARP4754 (Section 1.3) defines a system as ‘a combination of subsystems and/or items organised to perform a specified function or functions’ with:

- a subsystem is ‘a group of assemblies, designed together to form a major part of a system, complete in its own right performing a specific function or functions’
- a unit or assembly is ‘any part which is less than a subsystem, but whose performance can be independently assessed in terms of the overall performance of the subsystem’, and finally
- a part or component is ‘any item incapable of useful function at a lower level of assembly’.

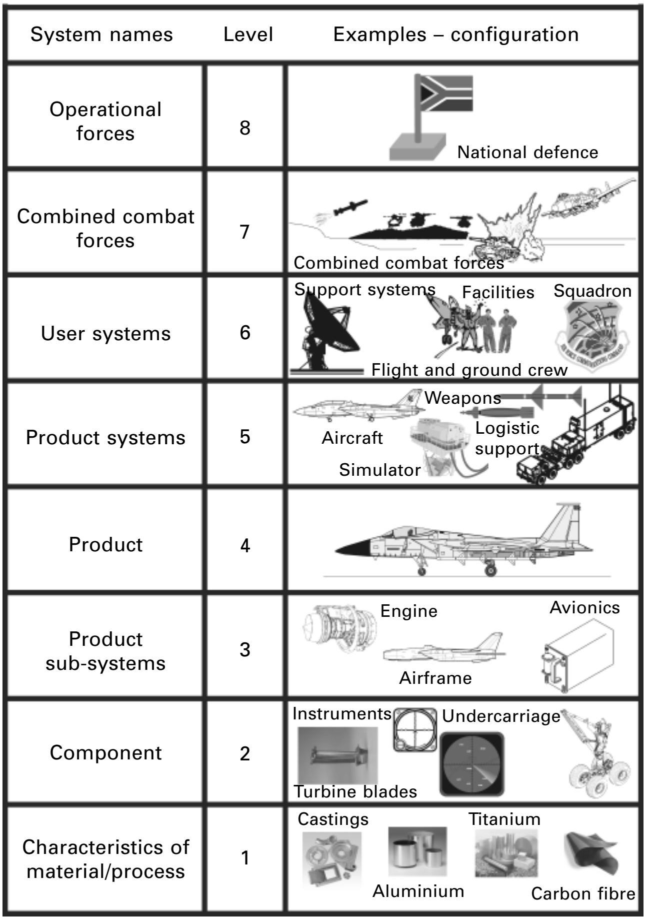
Safety is a system property. The safety of the whole cannot be argued from the claimed safety of the individual system elements alone. Any safety integrity claims for a part of a system (e.g. COTS[5] parts, assemblies or subsystems) without considering the whole (e.g. the aircraft) should be viewed with scepticism. The collection of component claims and supporting arguments and evidence do not make a complete safety assessment for the component/part. Rather, they form a partially constructed safety assessment with arguments (e.g. identified hazards, failure modes and their probability of occurrence) in ‘ready-to-use’ form. A system safety assessment must therefore consider not only all the elements within an individual system, but also the safety-related systems making up the total combination of the required functionality. These partial safety assessments can be thought of as safety assessment modules. It is important to understand the claims being made in these modules, the context assumed and the evidence presented (Kelly, 2003, p. 105). Only then can you intelligently apply this information within the context of your own system safety assessment.

System safety is more than the sum of the parts. In most situations, safety is achieved via the integration of a number of systems/sub-systems/ components, which rely on a variety of technologies (be they mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic, etc.), which is then put into an environment where it has to function safely as an operational system. It is this environment (i.e. physical installation as well as operational application) which highlights a deficiency in the DEF STAN 00-35 definition of a system, which does not clearly differentiate the various system levels available.

The South African Air Force (SAAF) make use of the illustration in Fig. 8.1 to distinguish between the different system levels for their logistic support strategy. This illustration can be applied to the system safety assessment as it helps us define what the system under consideration is. For instance:

- a component (Level 2) or sub-system (Level 3) does not possess safety as a property. Safety is a property of the product system (e.g. the aircraft) in its environment
- the integrating engineering authority must ensure that all components (including software) and sub-systems are fit for purpose (i.e. System Level 4), and the SSA is a useful design tool for the purpose (with the added benefit of showing the authorities how the regulatory requirements, such as FAR25.1309, are met)

[5] COTS, an acronym for ‘consumed off the shelf’ refers to equipment and sub-systems purchased ‘as seen’ usually with existing qualification data.



8.1 System hierarchy (reproduced with kind permission from the Armaments Corporation of South Africa (ARMSCOR)).

- The operators (and maintainers) need to ensure (via the Level 5/6 Safety Case[6] – see Chapter 9) that they operate (and maintain) the product in a manner that does not degrade the original design integrity, or cause any undue occupational hazards to the personnel exposed to the product.

The integration of various parts/sub-systems into an operable system is hardly ever simply one of acquiring COTS packages of technology. The hurdles with integrating various pieces of COTS equipment into a safety assessment are as follows:

- In the drive to 'divide and conquer' the assessor must be careful to ensure that the interaction between the systems are considered. The total is more than the sum of its parts. Seemingly established technologies may nonetheless be 'new' in terms of the issues and problems that are presented in the particular circumstances.

[6] Figure 8.1 is useful to illustrate a concept only. The exact destination of system level as applied to safety is to be defined by the assessor (preferably in conjunction with the certifying authority).

- Non-conforming safety criteria; if there is a common understanding of exactly what the definitions of terms such as improbable, probable, unlikely, minor, major, hazardous, catastrophic, etc., mean, the effort to integrate the safety argument into a system safety assessment will be greatly reduced and auditability will be improved.
- Failure to consider interactions between sub-system safety assessments could lead to either disproportionate effort, duplication of effort, or, nugatory effort, allocated across the overall safety assessment development.

An underlying cause of these problems is a poor understanding of the overall structure of the SSA argument and how the various arguments link together.[7] The loss of efficiency can be prevented by clearly defining the scope and boundaries of each sub-system's safety assessment. A co-operative relationship within the organisation and with sub-contractors is required. A target driven top-down approach (i.e. using measurable safety objectives) will assist in ensuring that proportional levels of effort are put into each part's safety assessment. Explicit planning (at an early stage of the life cycle), and managing the safety assessment argument can alleviate these problems. If the system safety assessment is not managed from the top-level system down to all its components, then the hurdles discussed above are bound to occur. The old adage is true: if you fail to plan, you plan to fail.

8.4 Planning the safety assessment

The content of a safety assessment varies considerably depending on factors such as the complexity of the system, how critical the system is to flight safety, what volume of experience is available on the type of system being used and the novelty and complexity of the technologies being used. If the safety assessment is to substantiate that the developed products are 'safe enough' to be taken into use (or deployed), then the safety assessment should be planned and managed to provide the necessary assurance that all relevant hazards and failure conditions have been identified and that all significant combinations of hazards and failures which could cause those conditions have been considered.[8] Furthermore, the safety assessment must be comprehensible to all parties concerned, not just the analyst. The assessment must assist the designer and management in making decisions. It must make clear what the critical features of each system are and upon which special manufacturing techniques, inspection, testing, crew drills and maintenance practice they are critically dependent (Lloyd and Tye, 1995, p. 19).

A strategy is therefore needed to facilitate the planning of a system safety assessment. Not only does it ensure that we do not run into the hurdles discussed above, but it also assists a third party such as the customer, the certification authorities (e.g. CAA), your fellow designers, or even your boss, to read and understand the methodology used to argue and validate/prove safety. How do we compile a safety assessment strategy? The following basic elements have to be considered:

[7] See also 'System of Systems (SoS)' research by DARPA, http://www.cs.york.ac.uk/hise/darp/index.php?link=resources/pdp.php

[8] Remember: a hazard not identified is a hazard not managed.

- The stakeholders. We need to identify the problem owners/decision makers who have a stake in the assessment. These will include the project manager, the client, the regulatory authorities be they military (e.g. MoD) or civilian (e.g. CAA), the independent safety auditors and the internal departments/teams and subcontractors. The success of the safety assessment requires a close working relationship and mutual understanding between all these stakeholders
- The safety/risk criteria. The safety/risk criteria establish the top-level system safety requirements, or objectives. Regulatory authorities may have different definitions for the various categories of hazards/accidents. To be able objectively to distinguish and evaluate the various hazards present, it is important to define the exact terminology and to allocate a measure of performance.[9] This is an important (and arguably most neglected) topic as it is the 'safety acceptance' criteria the system is expected to achieve, and hence the measure (or standard) the assessment will compare the system against. For more detail on safety criteria, see Appendix B.
- The system level. Define the systems level at which safety is to be assessed. The importance of this step is explained in Section 8.3 above. A safety assessment by a supplier of a component (e.g. a flare dispenser) will vastly differ in scope and approach to a safety assessment for a product (e.g. an aircraft) or user system (e.g. a facility).
- The system description. The system will need to be defined in terms of its physical and functional operation and interfaces. The description will include the systems (e.g. equipment) included; the functions these perform – including any modes of operation; its operating environment/envelope; the interface with other systems and where the functional and physical boundary lies between them; and, in the event of a modification, any deletions from the existing system.[10] If the boundaries are not clear to everyone involved in the assessment, some vital part may be overlooked. Furthermore, boundaries help with responsibility allocation, especially when products from sub-contractors are integrated into a more complex system.

  It is said that a picture is worth a thousand words. For the sake of brevity – and to facilitate rapid comprehension by both the reader and the assessor – it is useful to include diagrams (e.g. electrical diagrams, functional block diagrams,[11] etc.) illustrating the functional and physical interrelationships of the systems under consideration. These may be far more informative than a long narrative.
- The argument. Define the safety argument, i.e., how are you going to prove that the system is acceptably safe? Traditionally this is accomplished by a statement in

[9] Under certain circumstances the safety criteria may be amended to suit the specific programme requirements (e.g. UAV safety criteria, or Military Operational Safety Criteria). However, this is subject to substantiation and agreement by the applicable regulatory authority, thus the declaration of the safety criteria (either in a separate safety criteria report, or as part of a safety plan or an early release of a preliminary system safety assessment).

[10] Deletions could have a unexpected negative impact on other sub-systems.

[11] Functional Block Diagrams are an economical way of conveying functional interrelationships and it simplifies the safety assessment process – especially when conducting the Functional Hazard Assessment.

a safety plan or in the preliminary[12] safety assessment which explains and validates the safety assessment tools and techniques (Appendix A) used in the safety assessment process.

A new technique available for graphically portraying the safety argument is goal structured notation (GSN), where goals ▭ are broken into sub-goals, and eventually supported by evidence (solutions) ○ whilst making clear the strategies ▱ adopted, the rationale for the approach (assumptions, justifications) ⬭ and the context ▢ in which goals are stated. See Appendix C for more information.

Although some regulatory authorities have preferences for certain hazard identification techniques, it is up to the designer to use the most appropriate methods all integrated into a logical argument. This choice of tools/technique must therefore be substantiated and be adequate so as to ensure that nothing falls between the cracks.

- The programme plan. We then need to decide which safety activities will be conducted when and by whom. Safety activities are undertaken throughout the life of a system but it is vital that the right ones are done at the right time. If this is not done, then there are two possible undesirable outcomes (Rhys, 2002):
  - introducing an unsafe system into service (i.e. excessive safety risk)
  - major delays, cancellation or cost overruns if safety problems are discovered late (i.e. excessive project risk).

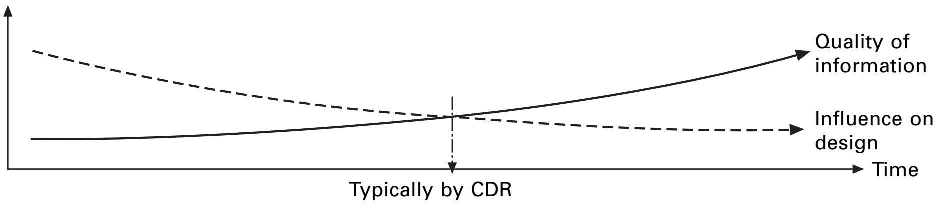
If the system safety assessment is to determine the safety requirements and influence the design, then the safety programme plan needs to be integrated into the development process.

8.5 Safety during the development process

The aim of the development process is to produce a system which is fit for purpose, and meets the contractual requirements. Many design drivers have to be satisfied. Safety is one of those design drivers. The safety assessment process is thus an inherent part of the development process.

At the conceptual stages of design, designers have great freedom and the cost of design and design changes are minimal. As the design matures, design freedom is decreased and the subsequent costs associated with design changes increase. Figure 8.2 illustrates that the ability to influence a system's characteristics diminishes rapidly

[12] A preliminary system safety assessment (PSSA) is essential in order to determine (and agree) the depth of assessment needed, the criteria utilised and the manner in which the safety objectives are to be accomplished. The PSSA concentrates on the functions and vulnerabilities of the system instead of the detailed analysis, and can thus be conducted prior to the definition of the system's architecture. The PSSA remains a live document until the final SSA can be issued. By the preliminary design review (PDR), the PSSA should include: functional failure consequences to the aircraft and its occupants; consequences of other possible malfunctions of a system (e.g. overheating) and their effects on surrounding systems; consequences to the system of failure in other systems or parts of the aircraft. identification of any possible common-mode failures or cascade failures which my need detailed investigation; the identification of possible vulnerabilities to flight crew or maintenance error.

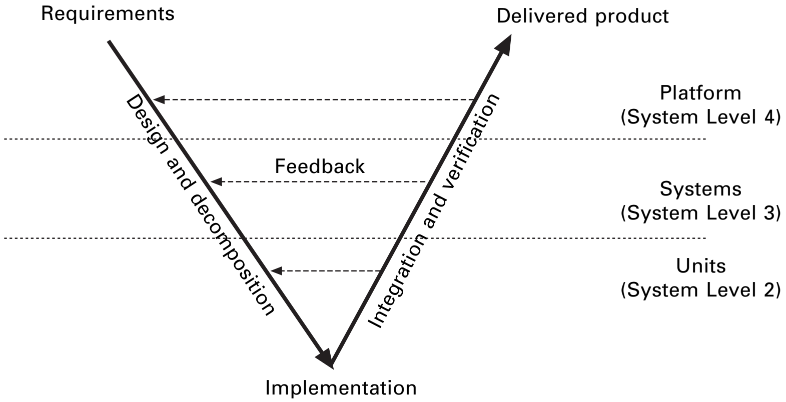


8.2 Safety influence vs. product life cycle.

as the system proceeds from one phase of its life cycle to the next. This illustrates that problems experienced downstream are symptoms of neglect upstream.

The required analysis must be conducted as early as possible in the development process because of the influence that it may have on system architecture. However, confirmation may not always be feasible until implementation is complete.

As stated in Section 8.2.3 above, safety is built in, not added on. In order to understand how we achieve a 'safe' design we must briefly consider the development process. The V-diagram in Fig. 8.3 presents a simplified illustration of the design process. The left branch represents the assessment of the design as it progresses towards low-level components. The right branch illustrates how these components are systemically integrated into sub-systems and systems, whilst continuously verifying integrity at each level.



8.3 The development process.

Safety must be an integral part of this process if we are to design effectively. Hence the basic safety activities are:

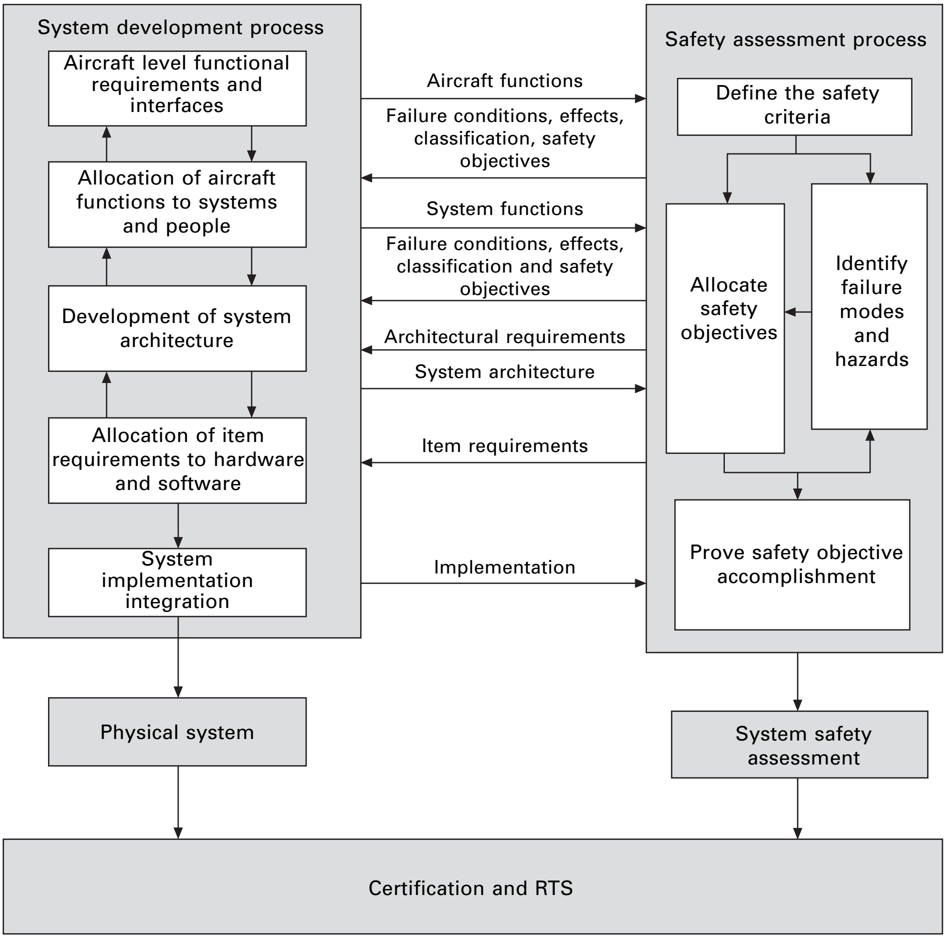
- Determining the safety requirements (i.e. qualitative and/or quantitative safety objectives commensurate with the particular hazard), starting with the appropriate system level and flowing those requirements down to the required sub-system/ unit/component level.[13] This is the purpose of the PSSAs.

[13] Note: These 'flowed-down' safety objectives are sometimes referred to as the 'Derived Safety Criteria'.

- Quantitatively and/or qualitatively assessing the proposed design and taking action where design is inadequate with respect to safety requirements.
- Gathering evidence for the safety assessment showing that an acceptable process has been followed to ensure that an acceptable level of safety is integrated into the delivered system. This evidence is gradually added to each re-issue of the PSSA until the final SSA can be issued.

This relationship between the safety assessment process and the system development process for aircraft is illustrated in SAE ARP4754[14] of which a tailored version can be seen in Fig. 8.4.

We can thus see that the safety assessment process includes requirements generation and verification, which supports the development activities. Just like other development activities, it too is iterative in nature. However, it does progress along with the development process:


System development process
Aircraft level functional requirements and interfaces
Allocation of aircraft functions to systems and people
Development of system architecture
Allocation of item requirements to hardware and software
System implementation integration
Aircraft functions
Failure conditions, effects, classification, safety objectives
System functions
Failure conditions, effects, classification and safety objectives
Architectural requirements
System architecture
Item requirements
Implementation
Safety assessment process
Define the safety criteria
Allocate safety objectives
Identify failure modes and hazards
Prove safety objective accomplishment
Physical system
System safety assessment
Certification and RTS

8.4 Safety assessment during system development.

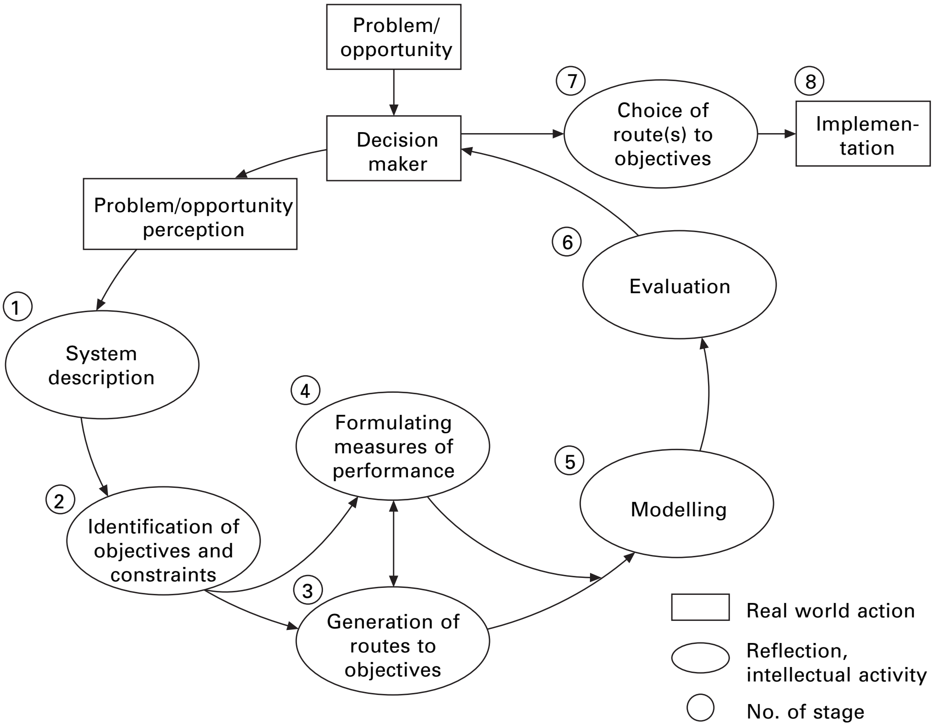
[14] See SAE ARP 4754 Fig. 3 and Appendix A.

- It begins with the concept design and derives the safety requirements for it.
- It then progresses into requirements verification which provides the evidence (justification) to support the modification activities leading up to certification.
- As the design evolves, changes are made that require re-assessment, which might influence the design again. Hazard and safety analysis help evaluate design trade-offs.
- The safety process finally produces the safety assessment, which substantiates the developed products as safe enough to be taken into use and/or verifies that the design meets the safety requirements (see also Fig. 8.8 on page 125 for an illustration of typical SSA activities against the product life cycle)

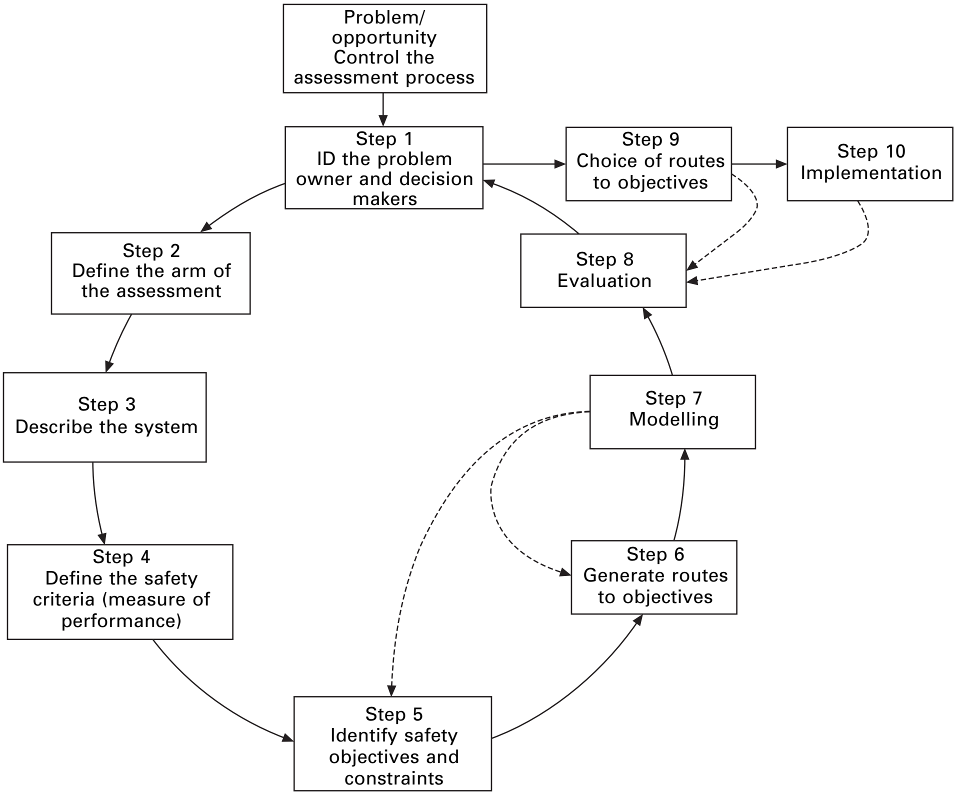
8.6 Modelling the safety assessment process

How do we portray the safety assessment process in a manner that safety novices (e.g. programme managers) can understand? There are various frameworks available with the Open University's (refer T840 Block 6 p. 26) hard systems approach (HSA) being particularly useful as a framework for modelling the safety assessment process.

The HSA is a problem-solving tool that considers both quantitative and qualitative issues within the framework of the defined system. It is useful for problems which can be well defined, fairly limited in extent and with agreed objectives (defined future state, such as a system which meets its safety targets). The HSA process is iterative in nature and is summarised in Fig. 8.5 The hard systems approach can be tailored to the safety assessment process as shown in Fig. 8.6.


Problem/ opportunity
Decision maker
7
Choice of route(s) to objectives
8
Implemen- tation
Problem/opportunity perception
6
Evaluation
1
System description
4
Formulating measures of performance
5
Modelling
2
Identification of objectives and constraints
3
Generation of routes to objectives
Real world action
Reflection, intellectual activity
No. of stage

8.5 Hard systems approach.


Problem/ opportunity Control the assessment process
Step 1 ID the problem owner and decision makers
Step 2 Define the arm of the assessment
Step 3 Describe the system
Step 4 Define the safety criteria (measure of performance)
Step 5 Identify safety objectives and constraints
Step 6 Generate routes to objectives
Step 7 Modelling
Step 8 Evaluation
Step 9 Choice of routes to objectives
Step 10 Implementation

8.6 A model of the SSA process.

Step 1: identify and involve the problem owner/decision maker

The owners/decision makers may include the project manager, the client and the accepting authorities (be they military (e.g. MoD) or civil (e.g. CAA)). These stakeholders decide the criteria in Step 4 chosen for the assessments, as well as provide the resources to implement any required solution (Step 9).

Step 2: define the aim of the assessment

The problem statement could be user-defined or extracted from regulations such as JAR25.1309 para (b):

> The aeroplane systems … must be designed so that the occurrence of any failure condition which would prevent the continued safe flight and landing of the aeroplane is extremely improbable, and the occurrence of any failure condition which could reduce the capability of the aeroplane or the ability of the crew to cope with adverse operating conditions is improbable.

Step 3: describe the system

The system will need to be defined in terms of the function it performs, the equipment included, its environment, and where the boundary lies between it and other systems. If the boundaries are not clear to everyone involved in the assessment, some vital part may be overlooked (Vicente, 1999, p. 7). For more information, see Section 8.4.

Step 4: define the safety criteria (measure of performance)

In order to guide the safety assessment process, it is necessary firstly to define the criteria used to judge the acceptability of hazards. These definitions are fundamental to understanding the data presented, as the resultant 'safety acceptance criteria' form the baseline standards against which the system is then evaluated in the final system safety assessment (SSA) report. For more information, see Chapter 5 and Appendix B.

Step 5: identify safety objectives and constraints

Identify and classify the hazardous conditions attributable to:

- system functions (and combinations of functions). The most popular tool in the early stages of the design is the functional hazard assessment[15] (see Appendix A). As the design matures, the assessment is then supplemented by other failure predictive assessment techniques such as the zonal hazard assessment.

  All failure modes are classified according to their severity (e.g. minor, major, hazardous and catastrophic) depending an the safety criteria chosen. Each failure mode classification is allocated a numerical or a qualitative safety objective, which is agreed with the applicable airworthiness authority.

Example

An example quantitative objective statement: 'Flap system failure could present a potentially catastrophic situation and shall have a probability of occurrence of less that 10^{-9} per hour of flight.'

An example qualitative statement: 'Software error in the altitude display could present a catastrophic situation and shall have a Development Assurance Level A.'

Safety Constraints may be imposed by regulatory requirements and/or regulatory guidance.

Example

AC25-11 states that 'display of weather radar in the cockpit is a non-essential function; however, presentation of hazardously misleading information must be improbable'.

[15] This broad-brush initial analysis must be carried out very early during the feasibility phase to enable its findings to influence the incorporation of safety features and the design to be carried out with sufficient design rigour. It needs to be carried out in an iterative manner as the system definition gradually evolves and its implication is understood.

- Item characteristics (e.g. hazardous materials or working practices) if the aim in Step 2 required these to be addressed as well. These hazards could be identified via hazard identification tools/techniques such as the particular risk analysis, HAZOP, etc. (see Appendix A). Each hazard must then be allocated with either a numerical or a qualitative safety objective, which is agreed with the applicable airworthiness authority.

Example using DEF STAN 00-56 criteria

When using the DEF STAN 00-56 criteria (refer Appendix B) each hazard shall be allocated to the most credible possible accident it can cause. The severity of this potential accident is then classified as shown in Table B.8.

In order for the risk to be no more than a Risk Class C, the same tables can then be used to determine the acceptable probability of the accident occurring. The probability of the accident is constrained by the events in the accident sequence (i.e the model, see Step 7), so by determining the probability of all the events in the accident chain, the assessor will be able to allocate a probability target to the hazard.

Example goal statement

The probability of fire in the fuel tanks is catastrophic and must be extremely improbable in occurrence.

Example constraint

No single failure condition may cause an ignition source in the fuel tank, no matter how low the probability (refer SFAR88).

Step 6: generation of routes to objectives

We now need to decide how we are going to prove accomplishment of the safety objectives identified in Step 5:

- For the FHA, the level of detail needed for the various safety assessment activities is dependent on the aircraft level condition classification, the degree of integration, and the complexity of the system implementation. The JAA provide useful guidance in this regard, see the decision tree in Fig. B.1.
- For all risk-based criteria, the assessor will need to agree with the relevant authorities which hazards need to be broken down into full accident sequences (see Fig. 4.1).

Step 7: modelling[16]

By this stage the design has commenced in earnest and the system architecture is

[16] A model is any set of organised assumptions about a particular aspect of the world and the way it works. In essence, it is a representation of reality.

being formalised in models (e.g. test benches, scale models or paper designs). In turn, the safety assessment process needs to build qualitative and quantitative models in order to analyse the probability of an undesired event/failure occurring. Once any potential hazardous effects have been identified, the task is therefore to determine the system conditions which will produce these effects. An analysis has to be performed to identify all failure conditions, and combination of conditions, which would lead to any effect listed in the airworthiness objectives. This is done by considering the reliability of the equipment; the design of the system; the precautions taken in installation, operation and maintenance procedures; as well as the intended operational exposure. During this phase the failure analysis is conducted by means of three main approaches:

1. The 'top-down' methods start by identifying the failure condition to be investigated, and then proceeds to derive those failure modes which can produce the condition (e.g. safety requirements from the base events of the FTA lead to the requirements for FMEA, life testing, etc.).
2. The 'bottom-up' methods start with the hardware failures (e.g. identified via piece-part FMEAs) which can occur, and analyses the effects of these on the system (e.g. the FTA basic events get their failure rates from the FMES).
3. Taking account of combinations of failures and dependent failure conditions from both internal and external causes (e.g. via the CCA).

As a result of this, design changes may well be required, which means the analysis becomes of an iterative nature until the required objectives are met. Any significant failure conditions not previously identified in the safety assessment need to be picked up and fed back in the safety management process.

Step 8: evaluation

In this step the achieved probability (qualitative or quantitative) is compared against the objective as defined in Step 5:

- For the goal-based approach, all deviations will require dispensation from the approval authority.
- For the risk-based approach, we may find that some accidents have a higher risk classification than we originally desired. Appropriate action is defined in Section 4.5.

Step 9: choice of routes to objectives

Ideally the design (i.e. the selection of components, the system architecture and the means of integration) should now be implemented in such a way as to ensure that the safety objectives are accomplished. The best route(s) to achieving the objectives must be chosen. Qualitative objectives and constraints will come into play here through the influence of the different stakeholders (especially the decision-makers who control the purse strings). A trade-off may be required in terms of a cost-benefit-analysis to ensure that certain hazards are indeed ALARP.

Step 10: implementation

Implementation is action orientated and represents the detailed work necessary to actually complete a design that should meet all required objectives. Ideally, from the point of view of a smooth development process, requirements should be validated before design implementation commences. However, in practice, particularly for complex and integrated systems, the necessary visibility of the whole set of consequences that flow from the requirements may not be obtainable until the implemented system is available and can be tested in its operational context. In consequence, validation is normally a staged process contributing through the development cycle. At each stage the validation activity provides increasing confidence in the correctness and completeness of the requirements.

8.7 Conducting a safety assessment

There is no one correct way of conducting a safety assessment. It all depends on the system complexity and on the safety assessment approach utilised (see Chapter 2). That does not mean to say that the assessment has to be analysed from a single approach only for, more often than not, a combined approach is far more feasible to identify and analyse the range of possible hazards (see Chapter 6). The following section will broadly contrast/compare the manner in which the goal-based approach (Chapter 5) and the risk-based approach (Chapter 4) are applied during a system safety assessment.

8.7.1 Goal-based safety assessment

Identify failures/hazards

A good starting point is the functional hazard assessment (FHA), starting from the highest system level possible. The FHA considers functional interaction and provides a methodology to evaluate the system's functions and the design of sub-systems performing those functions. Note that functional division may cut across systems (and therefore organisation boundaries). Multiple systems may contribute to the performance of a particular safety function. Similarly, systems may contribute to the performance of more than one safety function. See SAE ARP 4761 for guidance on conducting a FHA. Other useful tools for identifying hazards include the PRA, CMA, ZHA, etc. (see Appendix A).

Classify the severity of the hazard

The severity of the worst-case consequence (i.e. the hazardous situation) is typically classified using the safety criteria as defined in Table 5.1. It is advisable to consult individuals with operational experience (e.g. operating and maintenance crews) when analysing the effects of a potential hazard so that the severity can be properly determined and any assumptions validated.

Allocate the safety targets/objectives

This provides an indication of the acceptable probability of occurrence for the hazard/failure condition and is typically done by using the criteria in Table 5.2.

Prove safety objective accomplishment

For each hazardous effect, it should be determined how the aircraft/system will satisfy the safety objectives. This could mean that an analysis might need to be performed to identify all failure conditions (e.g. sub-system or LRU failures) which could lead to the hazardous effect. Each of these failure conditions is either allocated a derived safety objective (i.e. safety objectives have been set for the systems/functions, then apportioned to sub-functions/sub-systems, then apportioned to components) or, in the case of COTS equipment, existing data is used and the system architecture is manipulated to obtain the safety objectives discussed above.

Example: using goal-based approach

Consider what happens if the loss of aircraft engine power occurs at low altitude, low airspeed, or at high gross weight. The effects would include loss of attitude control, stall, high rate of descent and terrain collision. These obviously have the potential for catastrophic losses. Using the goal-based approach in Chapter 5, this hazard (loss of power) would be rated 'catastrophic' at low altitude, airspeed, or at high gross weight and should be 'extremely improbable' in occurrence for this system state. We next need to determine what the likelihood is of the hazard occurring (i.e. the probability of occurrence) and how often the 'effects or harm' will occur, considering the worst-case system state.

Here's how it works.
First, determine how often the hazard is expected to occur. This can be a quantified or a qualified estimate. Usually it is a function of the likelihood of the combinations of the cause(s), but sometimes this can be determined by evaluating incident or accident databases to see how often the hazard has been recorded in the field. Let us assume that the likelihood for 'loss of engine power' turns out to be 0.0001 per operational hour.

We then need to make an estimate of the likelihood of the worst-case system state. This estimate also can be quantified or qualified. In many systems the operational or system description will provide many clues that will allow the development of this answer. For this example, assume that the likelihood of being in the worst-case system state (low altitude, low airspeed, high gross weight) is 0.002 per operational hour.

For the effects to be manifested in the worst case both the hazard (loss of power) and the worst-case system state (low altitude, etc.) must occur at the same time. The likelihood of the worst-case effect is thus $0.0001 \times 0.002 = 0.0000002$ or 2×10^{-7} per operational hour. Using the definitions in Chapter 5, this would lead to a characterisation of the likelihood as 'remote', which does not meet the safety objective. The options open to the designer are to either apply for a deviation from the approval authority, or increase the reliability of the system, or add instruction in the flight manual and flight cards so as to limit operational exposure to this system state.

8.7.2 Risk-based safety assessment

Identify hazards

The hazard identification process should be planned and managed to provide the necessary assurance that all relevant hazards have been identified (see Chapter 4 for the definition of hazards). There are a variety of tools and techniques available to identify hazards. The application of these tools and techniques depend on the specific product/process being considered, its complexity, the product lifecycle phase, etc. The most common tools and techniques used are: FHAs, HAZOPs, occupation health hazard analysis, historical records, etc. (for more details on these tools, see Appendix A).

Classify accident severity

Each identified hazard is allocated severity classification according to the defined safety criteria. Accident severity categories are defined to provide a qualitative measure of the consequences resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies or system, sub-system or component failures. The severity is the worst credible consequence of a hazard (i.e. the worst accident) and is independent of random or systemic failure modes.

Determine the probability of the accident

The purpose is to identify circumstances which could lead to the accident under credible conditions. In order to do this we need to identify all the contributing failures and events which need to combine to cause the accident (see Fig. 4.1). This may require a number of hazard assessment techniques in order to identify appropriate contributing failures and events.

Assess the risk

The risk is the combination of the severity and the probability of the accident, see Chapter 4.

Reduce or manage the risk

This is accomplished by influencing any of the failures or events in the accident sequence in order to reduce the probability of the undesired outcome.

Example: using risk-based approach

Consider again what happens if the loss of aircraft engine power occurs at low altitude, low airspeed, or at high gross weight. Using the risk-based approach in Chapter 4, the accident would be classified as either ‘critical’ or ‘catastrophic’ depending on the amount of people on the aircraft. To be able to calculate the risk we then need to determine the probability of the accident occurring.

Here's how it might work.
Let us again assume that the likelihood of being in the worst-case system state is 0.002 per operational hour and that the likelihood for 'loss of engine power' is 0.0001 per operational hour. For the accident to occur, it means that the pilots were unable to recover the situation in time. Now, determining this likelihood is very subjective. Let us assume that there is a 50% chance that the pilot can recover the situation. The likelihood of this accident is thus $0.0001 \times 0.002 \times 0.5 = 1 \times 10^{-7}$ per operational hour which is classified as 'occasional'.

The risk of the 'catastrophic' event is thus Risk Class A, which is deemed as being 'intolerable' and shall be removed by the use of safety features. These may include warning devices of impending degraded performance, which could allow the crew to cope better once the hazard occurs.

The risk of a 'critical' event is thus Risk Class B, which is considered as being 'undesirable', and shall only be accepted when risk reduction is impracticable. A cost-benefit analysis may just result in no further action being taken to mitigate this hazard.

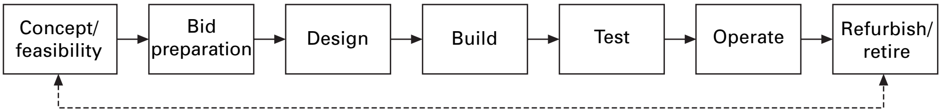
8.8 Generating the system safety assessment report

The system safety assessment (SSA) is an evolving document that provides the evidence (justification) to support the major procurement milestones and modification activities leading up to certification, acceptance into service and subsequent changes of design and operational use. It is the means for demonstrating that all the safety issues relating to the design and development task have been addressed.

Ideally, from the point of view of a smooth development process, requirements should be validated before design implementation commences. However, in practice (particularly for complex and integrated systems), the necessary visibility of the whole set of consequences that flow from the requirements may not be obtainable until the implemented system is available and can be tested in its operational context. In consequence, validation is normally a staged process contributing through the development cycle. At each stage the validation activity provides increasing confidence in the correctness and completeness of the requirements.

The safety assessment process thus remains live throughout the development life cycle. From the earliest stages it should be known what type of evidence will be required to demonstrate that safety will be achieved. The process must take into account any additional complexities and interdependencies which arise during integration. Incremental development of the safety assessment is thus very important. The first iteration is all about intentions rather than claims. It provides an opportunity to provide safety objectives, design constraints, assumptions, justifications, etc., to the system engineers who are developing the architecture, layout and draft specifications. Subsequent versions should develop the argument further and populate the structure with references out of the supportive evidence, with the plans of how to achieve the outstanding results.

Although the safety assessment process is iterative in nature, it does progress along with the development process.



8.7 Product life cycle.

- It begins with the concept design and derives the safety requirements for it.
- As the design evolves, changes are made that require re-assessment, which might influence the design again. Hazard and safety analysis help evaluate design trade offs.
- The safety process produces the safety assessment, which substantiates the developed products as safe enough to be taken into use and/or verifies that the design meets the safety requirements.

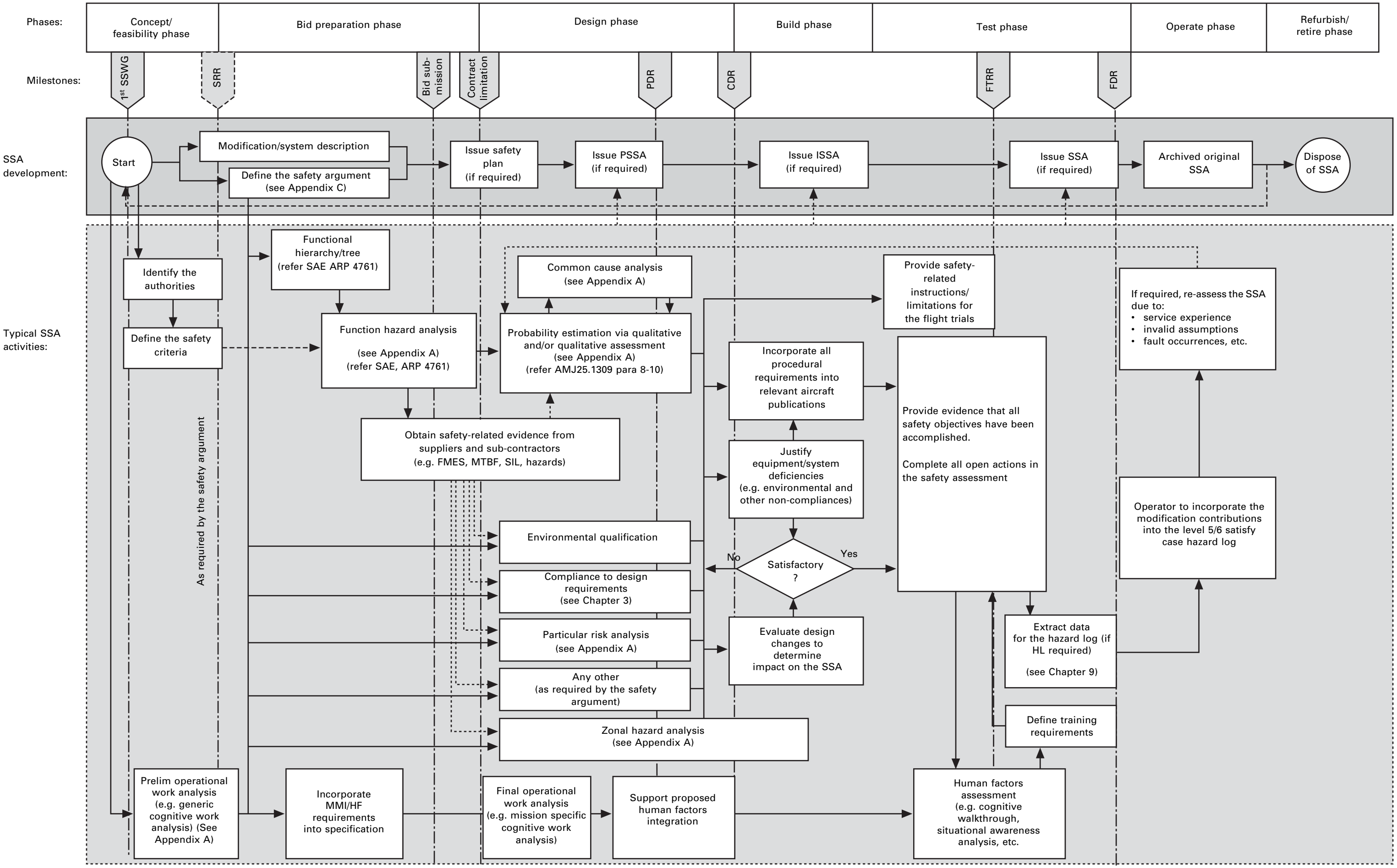
The flowchart in Fig. 8.7 shows a typical aircraft product life cycle from concept through to disposal at the end of the product's useful life.

Applying the most commonly used (refer, *inter alia*, SAE ARP4761) safety assessment tools and techniques, Fig. 8.8 takes this product life cycle and shows the safety assessment activities which may typically[17] follow for each phase.

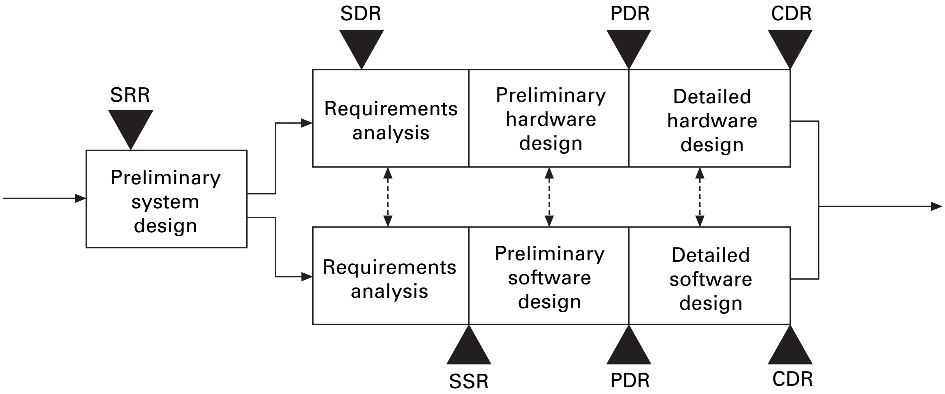
For complex or large programmes, it may be useful to divide the design phase up into discrete elements and milestones as shown in Fig. 8.9.

- *System requirements review (SRR)*: the SRR is the first top-level, multi-disciplinary, internal review of the perceived system requirements (including regulatory requirements). It is effectively a sanity check upon what the system is required to achieve, a top-level overview of requirements and review against the original objectives. This review may be held during the feasibility phase. Successful attainment of this milestone leads to a preliminary system design, in turn to the parallel development of the hardware and software requirements analysis, albeit with significant co-ordination between the two.
- *System design review (SDR)*: the hardware SDR immediately follows the preliminary design phase and will encompass a top-level review of the system hardware characteristics such that preliminary design may proceed with confidence. Key hardware characteristics will be reviewed at this stage to ensure that there are no major mismatches between the system requirements and what the hardware is capable of supporting.
- *Software specification review (SSR)*: the SSR is essentially a similar process to the hardware SDR but applying to the software when a better appreciation of the software requirements has become apparent and possibly embracing any limitations such as throughput, timing or memory which the adopted hardware solution may impose. Both the SDR and SSR allow the preliminary design to be developed up to the PDR.

[17] Individual projects may vary from the model in Fig. 8.8, however, it is a sufficiently good portrayal to illustrate the role of system safety engineering activities during the development life cycle and can be tailored to meet the unique requirements of the system under consideration.


Phases:
Concept/ feasibility phase
Bid preparation phase
Design phase
Build phase
Test phase
Operate phase
Refurbish/ retire phase
Milestones:
1st SSWG
SRR
Bid sub-mission
Contract limitation
PDR
CDR
FTRR
FDR
SSA development:
Start
Modification/system description
Define the safety argument (see Appendix C)
Issue safety plan (if required)
Issue PSSA (if required)
Issue ISSA (if required)
Issue SSA (if required)
Archived original SSA
Dispose of SSA
Typical SSA activities:
Identify the authorities
Define the safety criteria
As required by the safety argument
Functional hierarchy/tree (refer SAE ARP 4761)
Function hazard analysis (see Appendix A) (refer SAE, ARP 4761)
Common cause analysis (see Appendix A)
Probability estimation via qualitative and/or qualitative assessment (see Appendix A) (refer AMJ25.1309 para 8-10)
Obtain safety-related evidence from suppliers and sub-contractors (e.g. FMES, MTBF, SIL, hazards)
Environmental qualification
Compliance to design requirements (see Chapter 3)
Particular risk analysis (see Appendix A)
Any other (as required by the safety argument)
Zonal hazard analysis (see Appendix A)
Provide safety-related instructions/ limitations for the flight trials
Incorporate all procedural requirements into relevant aircraft publications
Justify equipment/system deficiencies (e.g. environmental and other non-compliances)
Satisfactory ?
No
Yes
Evaluate design changes to determine impact on the SSA
Provide evidence that all safety objectives have been accomplished.
Complete all open actions in the safety assessment
Extract data for the hazard log (if HL required) (see Chapter 9)
Define training requirements
If required, re-assess the SSA due to:
• service experience
• invalid assumptions
• fault occurrences, etc.
Operator to incorporate the modification contributions into the level 5/6 satisfy case hazard log
Prelim operational work analysis (e.g. generic cognitive work analysis) (See Appendix A)
Incorporate MMI/HF requirements into specification
Final operational work analysis (e.g. mission specific cognitive work analysis)
Support proposed human factors integration
Human factors assessment (e.g. cognitive walkthrough, situational awareness analysis, etc.

8.8 Typical SSA activities during the product life cycle.



8.9 Design life cycle.

- *Preliminary design review (PDR)*: the PDR process is the first detailed review of the initial design (H/W & S/W) versus the derived requirements. This is usually the last review before commencing major design resources to the detailed design process and often involves the customer. The status of specification and certification compliance is reviewed, as this stage in the design process is the last before major commitments to providing the necessary programme resources and investment.
- *Critical design review (CDR)*: by the time of the CDR major effort will have been committed to the programme design effort. The CDR offers the possibility of identifying final design flaws or, more likely, trading the risks of one implementation path versus another. The CDR represents the last opportunity to review and alter the direction of the design before very large commitments and final design decisions are taken. As such the customer participates in the CDR. Major changes in system design (H/W & S/W) after the CDR will result in severe impact on programme costs and schedule.

Figure 8.8 then considers the milestones after the design phase:

- *Flight trials readiness review (FTRR)*: this is conducted to challenge the preparedness of the whole test team. Senior representatives of the flight test organisation, including some from outside the specific programme undertake to examine all the safety and support aspects of the trial. Only when the entire review team are satisfied can the trial progress to the flying phase. The safety of flight test is paramount and risks need to be understood and bounded from the outset. Familiarity with the fundamentals of design, the anticipated aircraft behaviour and safety procedures applicable are reviewed, and if necessary, rehearsed and practised to retain a high degree of proficiency.
- *Final design review (FDR)*: the goal of the review is to convince the executives in charge that the design is mature enough to be released into service. All safety objectives should be accomplished and continued airworthiness activities published.

In general the safety assessment can be a very large document, so we need strategies to break it into manageable chunks. Not all evidence has to be fully contained in it (often the evidence is found in reports that were generated for other purposes), but the data should be sufficient to convince a third party, who may have had no prior insight into the programme. This implies strict configuration control requirements. If a reference document (such as a test report, or a flammability assessment) is updated, then its implication on the safety assessment needs to be considered. The challenge of assembling a safety assessment brings all of the elements of the SMS into sharp focus.

A SSA is not a repository for a forest of FTAs and FMEAs bound in a dust-gathering tome. Instead, a SSA is

- a written argument, supported by evidence,[18] that it is safe to operate a particular service, system or process
- a document which
  - describes the service, system or process
  - lists the principal hazards associated with operation
  - links to each hazard the design safety principles and operating safety principles which govern safe operation, use, maintenance, etc.
  - references (or includes) compliance to regulatory requirements (e.g. compliance check-list) and assesses any deviations from these requirements.

The safety assessment report should be

- accurate and concise
- easy to understand by those persons who need to make use of it
- suit the purpose for which it was intended
- be accessible and maintainable.

8.9 Discussion

There are[19] two primary causes of aircraft accidents:

- operational, such as pilot error, weather and operating procedures
- technical, such as design errors (including those that can cause pilot error), manufacturing errors, maintenance errors and part failures.

The Level 4 (refer Fig. 8.1) system safety assessment is interested in the latter (i.e. technical failure probability).

The safety assessment is an evolving document that provides the evidence (i.e. justification) to support the modification activities leading up to certification – and any subsequent changes of design and operational use thereafter. It is the means for demonstrating that all the safety issues relating to the design and development task have been addressed. The system designer’s task of producing a safety assessment is not only to satisfy the airworthiness authorities. Although the assessment is aimed primarily at obtaining a balance between the probability of system failure and the associated effect, this is not the only benefit. In practice, it is the critical and logical

[18] Argument without evidence is unfounded. Evidence without argument is unexplained.

[19] Refer C-05-005-001/AG-001 para 5.1.1.3 as well as Chapter 5 (paragraph 2).

scrutiny of the systems that is of most value, and not the precision of the numerical conclusions. The design itself is likely to benefit from lessons learned from a systematic assessment of safety (Rhys, 2002).

In all cases involving integrated systems, the safety assessment process is of fundamental importance in establishing appropriate safety objectives for the system and determining that the implementation satisfies these objectives. The safety assessment process should be planned and managed to provide the necessary assurance that all relevant failure conditions have been identified and that all significant combinations of failures which could cause those failure conditions have been considered. The safety assessment process is thus an inherent part of the design process and should be initiated at the earliest possible stage so that hazards are identified and dealt with while the opportunities for their exclusion exist.

There is no doubt that a well-executed (i.e. complete, consistent and correct) safety assessment can provide a reasonable basis upon which system certification can be based. It must be remembered, however, that the analysis can only be as good as the failure cases it identifies and the rates of failure predicted/assumed. The system should therefore be amenable to the safety assessment tools and techniques employed, so apply them appropriately.

9
The safety case

The superior man, when resting in safety, does not forget that danger may come.
When in a state of security he does not forget the possibility of ruin.
When all is orderly, he does not forget that disorder may come

Confucius (551–479 BC)

9.1 History

The development of the Safety Case as a European approach to safety management can be traced though a series of major accidents.

Aberfan, UK (21 Oct. 1966)

Wet weather conditions in this Welsh mining village allowed a colliery waste tip to become unstable and, without warning, the whole tip (half a million tons of coal waste) slid down a hill and enveloped some buildings – including the village school. There were a total of 144 casualties, including 116 children (mostly aged between 7–10).

This accident had a defining influence on UK legislation[1] and led ultimately to the Health and Safety at Work Etc[2] Act of 1974 (after the Flixborough disaster (Health and Safety Executive, 1975)). The fundamental effect of this legislation was to require companies to demonstrate that their works were safe and that workers were adequately trained. This was the start of the Safety Case concept (McLean (1997) and http://www.nuff.ox.ac.uk/politics/aberfan/eoafinal.htm).[3]

Flixborough, UK (1 June 1974)

The Caprolactam plant was a modern well-designed facility. However, following modifications to the plant, a large-diameter pipe failed, leading to the release of 40

[1] The tragic accident at Aberfan led to the Mines and Quarries (Tips) Act (1969) and the 1971 Regulations. These charge quarry owners with securing the safety of solid and liquid tips and provide for design, supervision, inspection, notification, records and the making of tipping rules. The 1969 Act also places duties on local authorities in respect of disused tips.

[2] The ‘Etc’ importantly covers offsite people. It is understood that the Act was used as a ‘vehicle’ upon which to trundle a few other legislative safety related ‘bits and pieces’ through parliament, hence the ‘etc’ aspect – for example, changes to Building Regulations, Public Health Act, and so on.

[3] See also http://www.politicalreviewnet.com/polrev/reviews/JCCM/R_0966_0879_030_19457.asp

tons of pressurised cyclohexane, which drifted across the site until an ignition source was encountered. The explosion immediately killed 28 plant operators and damaged hundreds of homes. The accident could have been much worse had it not happened over the weekend when most employees were not at work. The investigation showed[4] that:

- The plant modification occurred without a full assessment of the potential consequences. Only limited calculations were undertaken on the integrity of the bypass line. No calculations were undertaken for the dog-legged shaped line or for the bellows. No drawing of the proposed modification was produced.
- No pressure testing was carried out on the installed pipework modification.
- Those concerned with the design, construction and layout of the plant did not consider the potential for a major disaster happening instantaneously.
- The incident happened during start up when critical decisions were made under operational stress. In particular the shortage of nitrogen for inerting would tend to inhibit the venting of off-gas as a method of pressure control/reduction.

This event led to the creation of the tri-partite (government, industry and union) Advisory Committee on Major Hazards, which developed a system for the regulation of major hazards in industry.[5]

Sevesco, Italy (10 July 1976)

On 10 July 1976, a safety plate on a reactor vessel burst in an industrial plant during the manufacture of trichlorophenol (TCP) near Sevesco, Italy, releasing a mixture of chemicals including 2-,3-,7-,8-tetrachlorodibenzo-p-dioxin (TCDD). As a result, several thousand people, many animals and much of the surrounding vegetation in the Sevesco area were exposed to an aerosol of TCDD. Fear by the authorities for the health of local residents was justified by the known high toxicity of TCDD in animals and its ability to cause cancer under experimental conditions. As soon as results allowed for the definition of the contaminated area, an immediate evacuation of the people living within this region was ordered. Medical examinations of this potentially exposed population began immediately with long-term studies continuing up to the present day.

The response to Sevesco (as well as other incidents such as Flixborough) was the ‘Sevesco Directive’ issued by the European Commission via Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. This directive aims at the prevention of major accidents which involve dangerous substances, and the limitation of their consequences for man and the environment, with a view to ensuring high levels of protection throughout the Community in a consistent and effective manner. It requires the demonstration of safe design and operation of hazardous facilities.

[4] Refer http://www.hse.gov.uk/comah/sragtech/caseflixboroug74.htm (9/8/05).

[5] Refer Health and Safety Executive, The Flixborough Disaster: Report of the Court of Inquiry, HMSO, ISBN 0113610750, 1975.

Herald of Free Enterprise, *Belgium (6 Mar. 1987)*

A vehicle and passenger ferry capsized at the entrance to Zeebrugge harbour. The bow doors were not closed at departure from Zeebrugge because the responsible crew member had overslept, the supervising officer failed to check and the master did not require a positive report – even though he could not see the doors from the bridge. Water flowed into the vehicle deck as the ship accelerated and the ship rolled from 0° to 90° within 90 seconds. There was no time to launch lifeboats or life rafts. The ship came to rest on a sandbank with the starboard side out of the water, from where survivors were rescued by helicopter. Of the estimated 539 people on board almost 200 died (the ship was certified to carry 1400 people).

The owner and operator of the vessel was charged with corporate manslaughter, although legal technicalities prevented an eventual conviction. Mr Justice Sheen's inquiry expanded the horizon of disaster investigation by not only looking for the direct responsibility, but also looking for the systemic causes. Mr Sheen's summation established the principle that every employee – however far removed from the front line – bears some responsibility for their company's safety record. This accident was instrumental in leading to the establishment of the International Safety Management (ISM) Code by the International Maritime Organisation (Kuo, 1990).

Kings Cross, UK (19 Nov. 1987)

A passenger noticed a fire on one of the Piccadilly line escalators, which he reported to station staff. Seventeen minutes later the fire had developed so rapidly that a flashover occurred, spreading the fire and thick smoke into the ticket hall and surrounding subways. Thirty-one people died.

The Fennell Investigation found several deficiencies in the management of safety by London Underground – made worse by the fact that there had been a history of similar fires with no remedial action initiated. In addition, there was a lack of emergency planning and command/control, and staff were inadequately trained to deal with fires and emergencies. The investigation recommended a more formal safety management system in London Underground Ltd. This initiated moves to transfer the Railway Inspectorate to the HSE from the Dept of transport and informal discussions commenced about implementing safety cases for the railways.

Clapham Junction, UK (12 Dec. 1988)

The driver of a Basingstoke to Waterloo train (carrying 700 passengers) stopped to telephone the signalman as he had noticed that the signals were malfunctioning. The signals behind his train should have automatically turned to danger, protecting his train while stationary. This did not occur, and a Poole to Waterloo train (carrying more than 500 passengers) ran into the back of the Basingstoke train. At the same time a third train (thankfully empty) was passing in the opposite direction on the adjacent track. The first two coaches of the Poole train were crushed between the oncoming and stationary trains. Thirty-five people were killed and 500 were injured.

The fault was traced to a short circuit in a signal box. This short circuit originated during maintenance a fortnight before when a wire was disconnected but not insulated or tied down. The subsequent investigation found a succession of individual and system failures at all levels of British Rail. These ranged from poor working practices; to lack of supervision and effective management; to lack of necessary skills, competence and training.

This accident accelerated the development and implementation by British Rail of its Total Quality Management Initiative with associated internal and external auditing. The Railway Inspectorate's remit in monitoring safety of the railways was extended and transferred from the Department of Transport to the Health and Safety Executive in order to improve its degree of independence. This accident was instrumental in the establishment of a requirement for railway Safety Cases.

The official inquiry report on the capsize of the *Herald of Free Enterprise* ferry included the following statements:

> A full investigation into the circumstances of the disaster leads inexorably to the conclusion that the underlying or cardinal faults lay higher up in the organisation. The Board of Directors did not appreciate their responsibility for the safety management of their ships.
>
> All concerned in management, from the members of the Board of Directors down to the junior superintendents, were guilty of fault in that all must be regarded as sharing responsibility for the failure of management. From the top to the bottom the body corporate was infected with the disease of sloppiness.
>
> It is apparent that the new top management has taken to heart the gravity of this catastrophe and the company has shown a determination to put its house in order.

9.1.1 Summary

Until quite recently only the people directly involved would have been held to blame for an accident. Now it is recognised that safety is everybody's concern. All stakholders have an obligation to assume responsibility. Key lessons learned for these disasters included (refer, *inter alia*, Kuo (1997a, Ch. 1):

- Engineering: visibility is needed of decisions/assumptions that effect safety. However, it is also recognised that engineering alone cannot guarantee safety.
- Operations: systems evolve, as do their operational application. Procedures and maintenance do affect safety. Frequent training can improve effectiveness.
- Management: responsible for the development of a safety culture in their organisations by defining safety policies and allocating resources in the development thereof.

Where an industry or activity is recognised as dangerous, it is common to have regulations instructing designers and operators what to do (and what not to do), to make it 'safe'. These rules and standards come from experts analysing accidents that have occurred (or might occur) and how they could be prevented in the future. Often the industry has a regulator or inspectorate who provides a licence for operation only when the safety standards are followed. As seen from the examples above, this approach has not stopped major accidents from happening in the regulated industries.

Some of the regulatory failings include (David, 2001):

- encouraging compliance only with minimal-level standards – there is no incentive to go beyond the safety standard defined in a regulation
- making operators/designers jump through the regulation hoop without encouraging them to think about safety. This does not encourage a 'safety culture' within a company
- making it difficult to apply to systems of novel technology – rules are struggling to keep up with engineering advances.

A new approach was therefore called for, and this was the safety case. The major push in the development of the safety case concept was the tri-partite (i.e. government, industry and unions) Advisory Committee on Major Hazards (ACMH), which was formed after the Flixborough disaster. The most important and far-reaching of their recommendations was that owners of major hazardous sites/facilities should develop a living safety case. This safety case concept became widely adopted in other industries (e.g. UK MoD) as good HSWA practice.

9.2 Developing the requirement

9.2.1 Defining the safety case

The Health and Safety Commission defines (refer, *inter alia*, JSP553, 1st edition (para 2.43))[6] a safety case as:

> a suite of documents providing a written demonstration that risks have been reduced as low as is reasonably practicable. It is intended to be a living dossier which underpins every safety-related decision made by the licensee.

In essence, the safety case is a documented description of the hazards that the operator of a system/facility faces and the means employed to control those hazards. It is the systematic and structured demonstration by a company to provide assurance, through comprehensive evidence and argument, that the company has an adequately safe operation. The company will have identified and assessed the hazards and safety risks and be able to demonstrate that they can manage them to levels which are as low as reasonably practicable.

Note that it is a living dossier (i.e. the 'through-life' concept is implied, even though not always explicitly), which requires that it needs continuous management to ensure its currency and validity. A safety case must be reviewed continuously while

[6] Following the Health and Safety Commission's recommendation (and the loss of Crown Immunity), the UK MOD also adopted the safety case concept and has applied it not only to facilities, but also to the application of systems (refer DPMG/TECH/320 (Ensuring Product Safety): 'The safety case system is a management tool for demonstrating safety throughout the life cycle of a project. The safety case is a structured body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment. The safety case provides the safety evidence (justification) to support the major procurement milestones, acceptance into service and changes of design and operational use. It is the means by which the project manager demonstrates that all the safety issues relating to a project have been addressed').

the system is in operation. It is necessary to consider not only changes to the system itself (e.g. due to wear in tear) but also the possible effects of current/intended maintenance and operational practices.

The safety case approach makes the system owner/manager responsible for proving that their activities are 'safe' – and continue to remain so. Every system owner/manager is thus required to undertake a formal assessment of the safety of their facility and develop a report which documented the hazards, safeguards, safety and management systems, and emergency response plans for the system/facility throughout its life cycle.

The purpose of this safety case is to assess the hazards of the specific system/facility; review preventive measures; and define adequate risk management and emergency response procedures.[7] This approach was a fundamental change from the prescriptive controls at the time, which had allowed owners to believe that they were safe based on compliance with these controls. Continuing accidents proved that this was an illusion. The application of modern technology is often complex, with many interactions and co-dependencies between systems and people. It was unrealistic, therefore, to assume that government departments and industry associations would be able to continue to generate prescriptive regulations and codes of practice in adequate detail to meet the continuously changing technology.

9.2.2 Why have a safety case?

The arguments against having a safety case range along the lines of:

- The industry is already heavily regulated.
- We already do everything safely.
- We have enough procedures and systems already.
- Most of our problems lie in human error and not in our systems.

If these arguments are considered individually, research by Edwards[8] has shown that:

- The regulations establish the minimum requirements for safe operations. However, not everybody will always meet those minima in the execution of their job, as performance cannot always be 100%. Indeed, minimum standards are exactly that. To ensure an adequate buffer above the regulated minima to cater for the less effective employees or the mistakes they make, a company should establish its own standards, at least meeting the regulated minima; however, where additional risk exists, the standards should be above those set by the regulators.
- Procedures do not, in themselves, solve the problem unless they are used systematically and reviewed frequently.
- The working systems of companies are frequently found to be not sufficiently robust, and reported accidents show this to be a fact. Understanding the underlying

[7] A useful tool in this regard is the Bow-Tie Model, see Appendix A.

[8] Extracts from a lecture by C.J. Edwards at the Aviation Safety Management Conference held in London, 20–21 May 1999.

causes of accidents or occurrences and the review of the actions subsequently taken supports this view. Many companies do not carry out systematic working reviews as part of the process of continuous improvement.

- Human error is undoubtedly the most significant problem faced but it is often not the will of the individual to do wrong that is at fault, but a combination of company systems and cognitive shortfalls, coupled with real or perceived pressures, that underlie the majority of occurrences.

9.2.3 The relationship between the system safety assessment and the safety case

Safety is not self-sustaining (SAE ARP5150). When a system (e.g. an aircraft) is delivered and in its pristine condition, it has an initial level of safety often justified by the prime contractor via some form of system safety assessment (i.e. managed at System Level 4 as illustrated in Fig. 8.1). However, the ongoing safety of a system depends on numerous factors, including the original design, manufacturing, operating crew and maintenance actions, operational and environmental effects, quality of parts, modifications and system managing (such as configuration control), etc.

Once released into service, the system is continually evolving and changing. As it is operated the level of safety is maintained though a continuing process of monitoring service experience, identifying safety related issues and opportunities and then addressing these issues or opportunities through appropriate product changes (e.g. repairs, modifications), or procedural changes (e.g. maintenance techniques and scheduling) or additional training. For these reasons, safety (i.e. maintaining and enhancing safety wherever possible) should also be continually reassessed during the 'in-service' phase of the product life cycle via the safety case (i.e. managed at System Level 5 or 6 as illustrated in Fig. 8.1).

In contrast to the safety case (Level 5 or 6), the safety assessment (Levels 1 to 4) is usually applicable to one specific point in time only and is deliverable to the system manager/owner or a certifying/accepting authority upon initial system delivery. With reference to Section 5.2 and Appendix B (para 3.3), only a minority of accidents are due to technical failures, so the safety case (Level 5 or 6) should not duplicate the lower level safety assessments.[9] Rather, it should extract from these lower level assessments the issues (e.g. hazards) and evidence required to manage the operator's risk of an accident.

A Safety Case receives its inputs from these lower level Safety Assessments, which are updated only if specifically contracted. For instance, when in-service monitoring[10] has identified an uncorrected assumption or some other deficiency

[9] The safety case should facilitate application of the Pareto principle: concentrate effort where it will yield optimal results. The safety case should not duplicate the certification effort – rather, it should enforce, and then rely on it.

[10] One important lesson from past disasters is that a safety assessment/review, once issued, cannot be considered finished. Assumptions made in assessments need to be validated (e.g. probability estimates may have been optimistic) and circumstances change (e.g. change in maintenance philosophy).

(such as lower than expected MTBFs), or when the author of the Level 4 safety assessment is contracted to incorporate a new lower level assessment (e.g. such as for a sub-system upgrade).

This distinction between a safety case and safety assessment may seem only like semantics, but the contractual expectations justify a clear distinction:

- a safety case is much wider in scope and term of duration
- the hazard identification process remains live throughout the product life cycle
- the process must take into account any additional complexities and interdependencies which arise during integration, operational application and disposal.

To summarise, the safety case is a living dossier that needs continuous management to maintain its validity. Its relevance and accuracy must continue to be reviewed. It should be updated if:

- the equipment/system is modified
- there are changes in how or where it is used
- there are changes in legislation or the safety requirements
- there is a deviation between actual performance and design intention.

Upon system delivery, the safety case should therefore fall within the remit of the system owner/manager/operator to ensure the application of the requisite on-going management functions.

9.3 Core components

The core components of a typical Level 5/6 (see Fig. 8.1) safety case are:

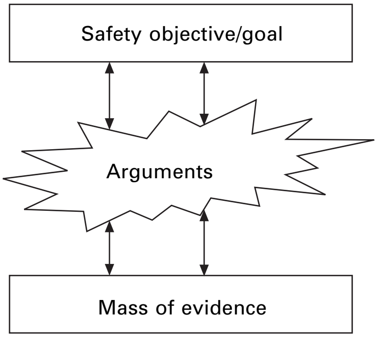
1. A safety argument, which summarises and justifies the claim that the system is adequately safe. This is discussed in Section 9.3.1 below.
2. A hazard log, which shows how identified hazards are managed, see Section 9.3.2 below.
3. A safety management system (SMS), which facilitates the above two points, see Section 9.3.3.

The safety case is a live, ‘virtual’, document containing all of the above. It is never complete, because the hazard log should never be closed (unless the product ceases to exist) and the SMS is a living process, tailored to effect the current roleplayers. When printed, the safety case report is a reflection of the safety case at a specific point in time (i.e. a snapshot).

9.3.1 Safety argument

Within the safety case, the safety argument needs to be able to stand scrutiny by a court of law, and should show that the owner of the system (i.e. platform or facility) did what is reasonably practicable (for a person in their position) to ensure the prevention of an accident. A convincing argument safety case requires three elements (see Fig. 9.1):

1. Safety objective(s) or goals



9.1 Proving safety.

2. Supporting evidence (e.g. FMECA, HAZOPs, etc.)
3. A clearly discernible 'thread' or argument that flows through the document (including any assumptions and justifications needed to support the argument).

An argument can be provided in textual format but is likely to be cumbersome and, for complex arguments, the 'devil may get lost in the detail'. It is easier with pictures – especially if the picture 'carries' the reader through the argument with sufficient, judiciously placed 'stepping stones' (i.e. sub-goals and sub-arguments down to an inevitable solution). Goal structured notation (GSN), see Appendix A, could be usefully applied here as it illustrates that 'discernible thread' to sustain a logical argument.

9.3.2 Hazard log

Clearly, without a robust list of hazards that require management (relevant to the activities covered in the safety case), the operator cannot be assured that effective controls have been established. A central part of any safety case is the capture, assessment and management of hazards. This is often done in some form of hazard log.

The hazard log is considered by the UK MoD as one of the most important tools for managing safety. The MoD defines the hazard log as a record of all significant hazards identified, and which acts as a directory for the safety justification by providing a summary of all safety activities[11] throughout the product life cycle. This hazard log provides traceability of how safety issues have been dealt with. Outstanding issues should be regularly reviewed by the project safety panel to make sure that safety-related actions are completed and unacceptable risks are resolved/mitigated.

The hazard log should contain all possible hazards and accidents for the system. This includes those that are considered tolerable, and those considered as not credible (such as an accident caused by volcanic ash or an earthquake). The hazard log will

[11] The MoD requires that all identified hazards should be recorded in the hazard log, irrespective of their perceived level of criticality and all subsequent actions recorded or referenced from there. There shall be an auditable trail from the hazards through to the safety properties identified and to the actual implementation, be that a physical design change, a documentation change or a procedural one.

show that they have been considered and provide the audit trail of reasons why they are closed. Should the circumstances change, for example, if the system is to be used in an earthquake zone, then the safety argument can be re-examined.

In order to compile a sensible list of hazards (i.e. sources of harm), a clear understanding will be required of what is meant by the term 'hazard'. As discussed in Chapter 5, a hazard is something that can lead to an undesirable[12] outcome in the process of meeting an objective. It is any situation with the potential for human injury, damage to property/assets or the environment. It is a set of conditions in the operation of a product with the potential for initiating or contributing to events that could result in personal injury, damage to property or harm to the environment.

Hazards are properties (states) of an entire system and may be defined at any level (see Fig. 8.1). However, it is essential to select the right level. A common fault is to select it too low, which results in too many hazards, no system properties, being expensive (or impossible) to track, and over-engineering. If you select it too high, then it is hard to ensure complete management.

Example: hazard identification in aircraft

Is 'flight management system (FMS) failure' or 'navigation display error' a hazard? No, the real hazard is 'loss of situational awareness'.

Distinguishing between hazards and their causes will assist in this regard with the above two failures being contributing causes.

Note that there are other causes to this hazard, e.g, coriolus illusions (caused by large head/eye movement during instrument scanning due to badly placed instrument); primary flight display (e.g. artificial horizon) failure, etc.

From a technical airworthiness perspective, a number of factors and inherent dangers exist, particularly for military aviation, that may influence the achievement of an acceptable level of aviation safety including the following:

- aircraft are very complex and highly integrated with a multitude of critical systems involving interfaces between hardware, software and operators
- as aviation technology advances, this complexity will increase, introducing new hazards and failure conditions
- aircraft are required to operate in a very demanding environment, especially military aircraft types
- weight restrictions require aircraft designs to be optimised with minimum margins of safety
- redundancy is often considered an unaffordable luxury, especially for military aircraft types
- design restrictions (e.g. space, weight, etc.) often place limitations on safety measures

[12] A hazard has the potential to cause harm. Physical hazards are always present in a system. Functional hazards usually require an initiating event (e.g. failure or operator error).

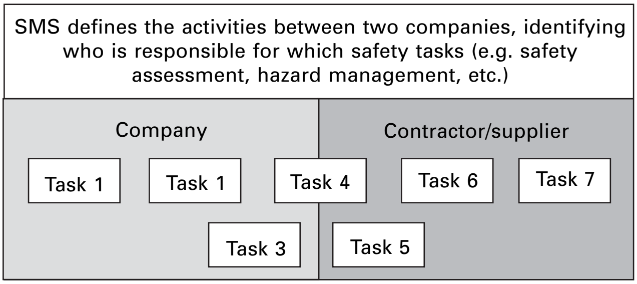
- actual testing under realistic environmental conditions is not possible in all cases, especially for systems which involve software
- despite testing, unexpected hazardous conditions (e.g. CFIT, flutter, stores separation, birdstrike, etc.) may occur
- other imperatives, such as mission accomplishment, available financial resources and schedule constraints may at times conflict with the technical airworthiness rules and standards.

It is therefore the objective of the hazard log, as a management[13] tool, to track the identification, mitigation and acceptance of risk and also the control of residual risks associated with the operation.

The hazard log is a live document which, throughout the life of the product provides an auditable record of the management of hazards for the specific system/facility/operation/activity. It should be a database which contains information to show how safety issues are being dealt with and resolved.[14] The big advantage of the hazard log is that all risks can be compared, prioritised, and (via the 'Pareto Principle') the operator can prioritise the hazard management effort on the most likely causes of an accident.

9.3.3 Safety management system

An essential part of any safety case is a safety management system (SMS).[15] A safety case may cover all, or part, of an operation and therefore there may be several safety cases but each will be managed by a single corporate safety management system (see Chapter 12). The choice of how the safety cases are delineated is made by the safety management system in such a manner that the resulting package (see Fig. 9.2) of safety cases covers all safety-critical activities.


SMS defines the activities between two companies, identifying who is responsible for which safety tasks (e.g. safety assessment, hazard management, etc.)
Company
Contractor/supplier
Task 1
Task 1
Task 4
Task 6
Task 7
Task 3
Task 5

9.2 Responsibilities in the safety case.

[13] The hazard log is not a safety assessment or hazard identification technique, only a management tool that is subservient to the safety management system. In fact, the hazard log can be thought of as an index to the mass of information held in the safety case. As such, the hazard log is a live document, which throughout the life of the product/facility/operation provides an auditable record of the management of hazards.

[14] The results of the hazard analysis carried out will lead to the identification of system and sub-system safety properties. These properties should be set so that they can be demonstrated and verified as achieved.

[15] Note, however, that the apposite is not necessarily true: a safety management system does not always require a safety case.

Each safety case is subordinate to its corporate safety management system (SMS), but used nevertheless to interact with the SMS. This results in each safety case, based on a specific part of the company's operation, using the SMS to assure and control hazards and receiving much of its input from narrowly scoped[16] safety assessments. Furthermore, the safety case should provide safety requirements/input/criteria for any future modification to the platform via the safety management system.

Example

An operator may require a contractor to install and certify the installation of a single standby instrument (for attitude, airspeed and altitude display).

The operator's safety case would have identified the hazard 'loss of situational awareness', and one of the contributing causes will be 'loss of primary flight data'.

Loss of primary flight data will require loss of primary display and loss of the standby.

Assuming the safety case allocated 'loss of primary flight data' an acceptable probability of 1×10^{-9} per flight hr, and the probability of loss of primary display has proven to be 1×10^{-7} per flight hour, then the safety case would accept a single standby instrument with a failure probability of 1×10^{-2} per flight hour (i.e. MTBF = 100 h).

Personnel associated with the design, manufacture, maintenance and material support of aeronautical products may be required to make a decision or recommendation involving a balance between aviation safety requirements and other imperatives such as cost, operational requirements, etc.). This is the role of the safety management system. As with a case in law, the safety case is a body of evidence presented as a reasoned argument. Unlike most areas of the law, the designers and operators are not presumed innocent until proven guilty; the safety case must proactively prove that a system is safe. The operator's safety management system is an important part of this evidence, as it demonstrates an ongoing commitment to continuous safety monitoring and improvement.

Safety management is intended to bring together all the facets of safety including engineering design, risk assessment (includes hazard identification, control and risk reduction), training, operation, maintenance, upkeep and disposal. Many modern systems are very complex and the consequences of possible accidents for them are enormous in scale. It is seldom possible to rely simply on designs and practices which have been 'safe' in the past. It is recognised that there is no such thing as absolute safety. Design and maintenance standards are established to ensure a minimum 'acceptable' level of safety is achieved, determined by such factors as community expectations; public, industry and government preparedness to pay; relativity of safety levels in other fields affecting overall safety, etc. These factors are not necessarily quantifiable. Whilst efforts are made to do so, inevitably judgements based on experience must be

[16] Safety assessments are, more often than not, scoped to consider a specific concern on specific part of a system.

made and continually reassessed. In other words, there is a risk; the judgement as to the acceptable level of risk is one of the prime functions of safety management.

Investigations of accidents show that there are often common themes as to why they happen:

- problems which have shown up as minor incidents but were never addressed
- no-one ever imagined that the circumstances of the accident could happen, so there were no systems or emergency procedures to deal with them
- people thinking that it is someone else's job to deal with safety
- sloppy work practices building up over time (e.g. because they are easier and cheaper to do)
- equipment being modified or used outside of their design intent
- people not reporting safety concerns because a blame culture exists in the organisation.

Safety management attempts to deal with these common root causes by emphasising a proactive approach; prevention, rather than reacting to harm once it has occurred. It is essential that a management system has procedures in place to identify and manage major hazards. Hazard management should consider methods of prevention, detection, control and mitigation to reduce the risks to 'as low as reasonably practicable' (ALARP).

A simple way of understanding the SMS is to consider five basic questions (refer *inter alia*, Kuo (1997a) Ch. 6).

1. **What could go wrong?** (i.e. hazard identification and analysis)
2. **What are the chances of it going wrong?** (i.e. probability assessment)
3. **How bad could it be?** (i.e. risk assessment)
4. **What has been done about it?** (i.e. hazard reduction/control plus supporting evidence)
5. **What if it happens?** (i.e. emergency and contingency arrangements)

The safety case should provide the answer to these questions. The safety management system should be the enabler.

9.4 The safety case report

In Section 9.2.1 we defined a safety case as a structured body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment. This 'evidence' is collated and presented in a safety case report, which is a snapshot of a defined point in time. It usually provides a traceable reference to evidence in test results, detailed safety analysis reports, etc.

The size and scope of a safety case can vary enormously and will be appropriate to the system complexity and the level of risk involved. Throughout the life of a system/facility/operation it will be necessary to abstract evidence from the safety case and present it in the form of a safety case report to support life-cycle milestones. Each safety case report will present a safety argument (a reasoned justification) that a safety claim or target has been met.

The safety case report should be readable by non-safety experts but have sufficient detail to assist senior management to review performance and provide authority to either proceed from one stage of the product life cycle to the next, or to fund/prioritise appropriate changes where required. Angove (1999) advises that a safety case report does not have to be a large set of documentation compiled at huge cost. Rather, a safety case report should be viewed as the result of a through-life practical and iterative development of evidence relating to safety risks and their tolerability. The following sub-sections provide information that will typically be contained in a safety case report.

9.4.1 Defining the system

In order to validate the safety of a system, we first need to provide an accurate definition of the system and description of its operation. Depending on the scope (see Section 9.4.2) of the safety case, this description will need to include issues such as:

- the specific equipment/system:
  - hierarchy and interface with other systems
  - functionality
  - configuration
  - build standard
  - performance
- the operating environment:
  - operating limits, flight conditions and envelope
  - the operational scenario
  - sortie profiles
  - any plausible environmental conditions
  - role changes (if applicable)
- the maintenance environment
- the design and certification authorities involved to date.

9.4.2 Aim, scope and objectives of the safety case

The next step for a successful safety case it to define its scope, aim and objectives:

(a) **Scope** defines the extent of the safety case. In effect we are establishing boundaries for our responsibilities. If the boundaries are not clear to everyone involved in the assessment, some vital part may be overlooked. Boundaries help with responsibility allocation, especially when products from sub-contractors are integrated into a more complex system. Furthermore, the scope may include activities during the development phase or may be limited to continuing the effort started during the aircraft design phase by beginning with the new type's introduction into service and continuing until retirement. It may also address a system in use for which there has been no official safety strategy or safety management system to date.

> Example scope
>
> A complete aircraft safety case would typically be scoped to address the safety of the platform (inclusive of its on-board systems and ground/test equipment); safety of operations; and safety during all maintenance activities.

(b) The **aim** of the safety case provides us with the general intent.

Example aim

'to ensure the aircraft is modified, maintained and operated with its intended level of safety throughout its operating life'.

(c) **Objectives** are measurable results against which the success of the safety case will be evaluated. These objectives are obviously dependent on the scope and aim.

Example objectives for an MoD aircraft

- Hazards have been, and are being, systematically identified.
- All identified hazards have been incorporated into the hazard log.
- All risks have been prioritised and reduced to ALARP.
- The cumulative probability of loss of an aircraft due to technical fault, and the cumulative probability of the aircraft (inclusive of its systems, structures and stores) which could result in the death of any air crew or passengers, has been assessed to be of the order of one in a million per flying hour (probability of occurrence 1×10^{-6} per flying hour) when operated within the conditions used for the airworthiness demonstration.

9.4.3 Safety requirements and safety criteria

Define all applicable safety requirements, targets and objectives that guide the hazard assessment process and are used to judge the acceptability of the hazard (see Appendix B for example safety criteria). The necessity for this step is explained in the following discussion.

Discussion on safety criteria in safety cases

Consider a system that has undergone numerous upgrades and modifications during its operational life. The owner/operator is supposed to be responsible for the safety case and demands safety assessments from contractors/suppliers/system integrators. However, there are few examples in industry of how the various safety assessments conducted by the different contractors are integrated into the operator's safety case, or how in-service monitoring of all these safety assessments is efficiently accomplished.

I suspect that the main contributory factor is that the operator's safety case (and especially its safety criteria) seldom drives the approach taken by externally supplied safety assessments. If a safety assessment has different safety criteria and, even more so, if a different approach (see Chapter 1 Section 1.4) is taken to justifying an adequate level of safety, then managing the safety case is bound to be complicated.

JSP430 advises that:

> The Safety Case is to be prepared in outline at presentation of the Staff Requirement and is to be updated at each major procurement milestone up to and including hand-over from the procurement to the maintenance authority…ideally there should be a seamless development of the Safety Case from one phase to the next.

This should perhaps be extended to also say: ‘Furthermore, the safety case should provide safety requirements/input/criteria for any future modification to the platform. This should not be limited to the usual criteria for risk assessment, but should also provide safety targets for specific failures/events based upon known accident sequences.’

Bear in mind that the goal-based safety criteria used to satisfy JAR25.1309 and JSP553 para 1.38 is not directly compatible with the risk-based approach required by the safety case. In this case, the former should rather be used to identify contributing factors within a sequence of events which may lead to an accident. The goal-based approach is thus a useful source of failure/event inputs, along with their probability of occurrence.

9.4.4 Safety case strategy/approach/argument

The purpose of a safety case can be defined in the following terms (Kelly and Weaver, 1994): ‘A safety case should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context.’ The following are important aspects of this definition:

- **‘argument’** – above all, the safety case exists to communicate an argument. It is used to demonstrate how someone can reasonably conclude that a system is acceptably safe from the evidence available.
- ‘**clear**’ – a safety case is a device for communicating ideas and information, usually to a third party (e.g. a regulator). In order to do this convincingly, it must be as clear as possible.
- ‘**system**’ – the system can be anything, see Fig. 8.1 for more information.
- ‘**acceptably**’ – absolute safety is an unobtainable goal (see Chapter 1). Safety cases are there to convince someone that the system is safe enough (when compared against some definition or notion of tolerable risk).
- ‘**context**’ – context-free safety is impossible to argue. Almost any system can be unsafe if used in an inappropriate or unexpected manner. A robust safety case needs to define/identify the context within which safety is to be argued.

The Safety Case should therefore clearly describe the approach, arguments and reference the evidence used to justify the safety of the system, so that agreement can be reached on the validity of the conclusions. The safety argument should be structured hierarchically, so that this safety justification can be summarised in a safety case report. The safety argument should be developed from the safety objectives defined in Section 9.4.2. It should present the case supporting the use of the system in the defined roles and environments, giving the outstanding risks. For more on the safety argument, see Appendix C.

9.4.5 Risk analysis

The hazard log (see Section 9.3.2) is to include a description of all identified hazards and potential accidents, the relevant mitigation, their safety risk and acceptability, any actions to be taken to reduce the risk, and reference the supporting safety analyses. Ideally all hazards would have been designed out of the system and there would be no risk to consider. In practice this is rarely the case.

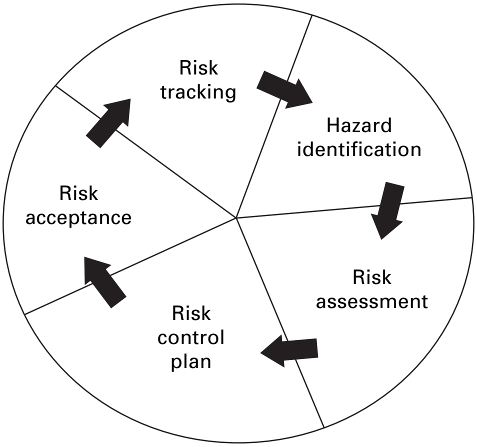
The hazard log needs to be coupled to logical decision process and the following steps are essential in the development of a hazard log (see Fig. 9.3).

- identify conditions and situations that may result in an accident
- provide a measure of the risk by determining the severity and the probability of the accident occurring (see Chapter 6)
- control the implementation of risk reduction measures so as to ensure that the risk of an accident remains ALARP
- accept the level of risk
- track the risk to make sure it does not change.

The hazard log is therefore used to determine the risk of each hazard turning into an accident (see Fig. 6.2). There is an important decision that senior management must make as to the level of risk the company will accept in order to manage the hazards identified. The ALARP principle demands that if a control is technically possible, is reasonable to do and can be achieved without causing financial distress to the company, then those controls should be set in place.

9.4.6 Recommendations and limitations

The safety case report should provide a list of recommendations and limitations needed to ensure that the required level of safety is retained. Particular issues that should be provided include:



9.3 Hazard management process.

- emergency/contingency arrangements to cater for certain foreseeable accidents.[17]
- any operational or other limitations that may be necessary for risk mitigation
- minimum check and maintenance intervals for all system elements (including personnel training) considered in the safety analysis, particularly where exposure time to latent failure conditions is critical
- action, if any, relevant to outstanding risks
- procedures for safety case maintenance in the light of changes to the system, its operational role or environment.

9.5 Discussion

The safety case is thus a documented description of the hazards that the operator of a system/facility faces and the means employed to control those hazards. It is the systematic and structured demonstration by a company to provide assurance, through comprehensive evidence and argument, that the company has an adequately safe operation. The company will have identified and assessed the hazards and safety risks and will be able to demonstrate that they can manage them to levels which are as low as reasonably practicable.

Safety cases can be considered the tangible products of an effective safety management system. The intangible product is a safer system. Note that the safety case was never intended to replace the OEM's safety assessment, which is intended to support the certification of airworthiness of the platform. However, the safety case does need the safety assessment to mitigate the probability of operational hazards turning into accidents. In an ideal world, there should be:

- a live safety assessment (Level 4) maintained by the OEM reflecting the current build standard of the aircraft. This will contain much proprietary data and would require a specific contract with the OEM, and all third-party modification agencies, to ensure it reflects the current build standard.
- a live safety case (Level 5/6) generated by the operator, which proves that the intended level of safety (i.e. as designed) is actually accomplished in service and that all operator-related hazards (e.g. CFIT, maintenance error, etc.) are being identified and managed.

Safety cases tend to be very large documents, containing complex internal interdependencies, which include the results of a wide range of related analyses. They often rest upon a number of implicit assumptions and have a long lifespan, going through many revisions in the course of their production. Both product and process issues need to be addressed in the safety case. It must be shown both that:

- the system meets its safety requirements and
- that the processes for deriving the requirements, constructing the system and assessing the system are of appropriate integrity.

The safety analyses which appear in the safety case depend crucially upon the

[17] A bow-tie analysis (see Appedix A) may be useful to identify these arrangements.

formulation of suitable models of the system, at various levels of abstraction, produced during the development process. Given these characteristics, it is not surprising that safety cases are difficult and expensive to produce and maintain.

Not all safety cases are acceptable. The HSE has reviewed many safety cases in its role as regulator and some of the problems it has found with poor examples include (David, 2002):

- They contain assertions rather than reasoned argument.
- There are unjustified and implicit assumptions.
- Some major hazards have not been identified and are therefore never studied.
- There is a poor treatment of uncertainty of data and sensitivity of the assessments to this.
- They do not deal well with human factors.
- They do not deal well with software.
- There is inadequate involvement of senior management.
- Ownership of the safety case is not always clear.

Furthermore, many safety cases contain a great deal of evidence from the various safety analysis techniques employed, but they do not always draw this evidence together in a clear and understandable manner. Dr Tim Kelly (University of York) is known to have said 'An assertion (or argument) without evidence is unsubstantiated, and evidence without an argument is unexplained'. There should be a clearly discernible thread of argument that flows through the whole safety case. A properly structured safety case argument (see Section 9.3.1) will go a long way to improving the quality and completeness of the safety case.

The user must be involved in safety throughout the life cycle, from setting appropriate safety requirements through to managing residual risk and feeding back information on shortfalls in service use. It is the operator who will be exposed to most safety risks in service, so it seems logical that they must have a major role in accepting the level of risk they will be prepared to tolerate for the benefits the new equipment will bring (Rhys, 2002). Any safety margins should also be made explicit.

The end users need not be given the full safety case, since they do not need to know all the information contained in it. However, the parts dealing with emergency arrangements and with limitations for safe use must be available to them (e.g. through updated operational/maintenance manuals).

10
Numerical probabilistic approach

Do not expect to arrive at certainty in every subject which you pursue. There are a hundred things wherein we mortals must be content with probability, where our best light and reasoning will reach no farther.

Isaac Watts

10.1 Introduction

Amongst various requirements, the certification of an aircraft requires proof that any single failure, or reasonable sequence of failures, likely to lead to a catastrophe has a sufficiently low probability of occurrence. This has led (refer Chapter 4) to the general principle that an inverse relationship should exist between the probability of loss of function(s) or malfunction(s) (leading to a serious failure condition) and the degree of hazard to the aeroplane and its occupants arising therefrom.

It should go without saying that a low probability of occurrence equates with a high level of safety:

- The designer who first decided to duplicate essential bracing wires in combat aircraft during the First World War to reduce the risk of the wires breaking (or being shot away) applied an intuitive probability judgement (Lloyd and Tye 1995, p. 41).
- As later-generation aeroplanes developed, more safety-critical functions were required to be performed, which generally resulted in an increase in the complexity of the systems designed to perform these functions. The potential hazards to the aeroplane and its occupants that could arise in the event of loss of one or more functions provided by a system (or that system's malfunction) had to be considered, as did also the interaction between systems performing different functions.

The difference between then and now is that, due to the increase in system complexity, an instinctive 'feel' of probability has been replaced by quantitative probability assessment. The use of probability evaluations is particularly appropriate in the following instances (refer, Lloyd and Tye, 1995 (p. 105) and Cherry (1995));

- defining the system architecture required for safety (i.e. acceptable reliability levels for systems and sub-systems)
- checking whether the redundancy provided is adequate
- assessing a system's fault tolerance
- determining the requisite check periods necessary to limit the presence of undetected (dormant) failures
- determining whether the effects of performance variations under normal and failure conditions are acceptable
- determining (e.g. for an MEL) what deficiencies of equipment are allowed before take-off and what restrictions should be applied if they are.

10.2 The fundamental concepts

10.2.1 Symbols commonly used

The following symbols are commonly used in probability assessments for the purposes of assessing safety:

F – frequency (i.e. the average rate at which an event will occur)
R – reliability (i.e. the probability of success) (see Section 10.2.5)
Q – probability of event not occurring (e.g. probability of no failure)
P – probability of event occurring (e.g. probability of failure, $P = 1 - Q$)
p – probability per unit time (usually per hour)
λ – constant failure rate = 1/MTBF (so, $\lambda = p$ if the rate is constant)
T – fixed period of time
t – elapsed time

10.2.2 The probability scale

The word 'probability' derives from the Latin word *probare* (to prove, or to test). 'Probable' is one of several words applied to uncertain events or knowledge, being more or less interchangeable with likely, risky, hazardous, uncertain, doubtful, chance, odds, and bet depending on the context. When conducting safety assessments, the term 'probability' is used to give us an indication of the likelihood of a random event occurring. It is a relative frequency of the ratio of n successes in N trials so:

$$P = n/N$$

and $0 \le n \le N$.

Probability is always expressed as a value between 0 (= never) and 1 (= certain). This can be calculated as follows:

$P = n/N$ and $0 \le n \le N$

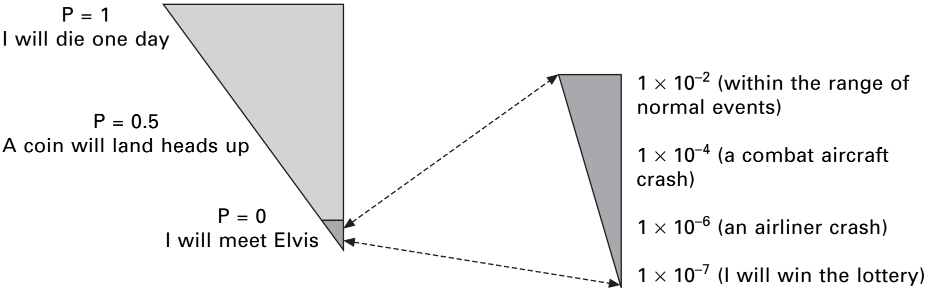
so $0/N \le n/N \le N/N$

which results in $0 \le P \le 1$

Figure 10.1 is intended to put the probability scale into perspective. Note that 'P' is used to indicate the probability of occurrence of the event[1]. P is dimensionless, failure rates are not.

[1] A probability indicates that a failure, error, or accident is possible even though it may occur rarely over a period of time or during a considerable number of operations. A probability cannot indicate exactly when, during which operation, or to which person an accident will occur. It may occur during the first, last, or any intermediate operation in a series without altering the probability of its occurrence.

Consider an example of when the likelihood of an aircraft engine failing is accurately predicted to be one in 100,000. The first time the first engine is tried it fails. One might expect the probability of the second one failing to be less. But, because these are independent events, the probability of the second one is still one in 100,000. The classic example demonstrating this principle is that of flipping a coin. The probability of it landing heads-up is 1 chance in 2 or 0.5. This is true every time the coin is flipped even if the last 10 trials produced a heads-up result.


P = 1
I will die one day
P = 0.5
A coin will land heads up
P = 0
I will meet Elvis
1 × 10–2 (within the range of normal events)
1 × 10–4 (a combat aircraft crash)
1 × 10–6 (an airliner crash)
1 × 10–7 (I will win the lottery)

10.1 The probability scale.

In the aviation industry we are interested in the failure probability per flight hour (see Chapter 4).

> Example
>
> Most items used in aircraft systems have a probability of failure of once in around 1000 hours (see Chapter 7). On certain assumptions, this means a probability of failing per hour of use of 1/1000, which is written as $p = 1 \times 10^{-3}$ per hour.

So, if the failure probability of a sub-system is p per hour, then the probability of failure in a flight duration of T hours is considered to be $P = pT$.

> Example
>
> Civil aviation catastrophic accidents occur on average once every 1 million flying hours. The probability of these catastrophic accidents is $p = 10^{-6}$ per hour. So, for a flight duration of four hours, it can be assumed that the probability of an aircraft crash is: $P = pT = 4 \times 10^{-6}$

Care should be exercised when claiming failure probabilities because (a) they are used to justify the safety of a product, and should therefore be properly substantiated and validated, and (b) very low values are extremely difficult/expensive to achieve.

> Example
>
> Assume a qualitative assessment shows that a probability of an undesired event (e.g. a failure combination) is in the order of 1×10^{-9} per flight hour in occurrence. For a single aircraft, this can be interpreted that it would take 1000,000,000 flying hours to occur. That means, in 114,155 years of continuous flying we are expecting one such an undesired event.

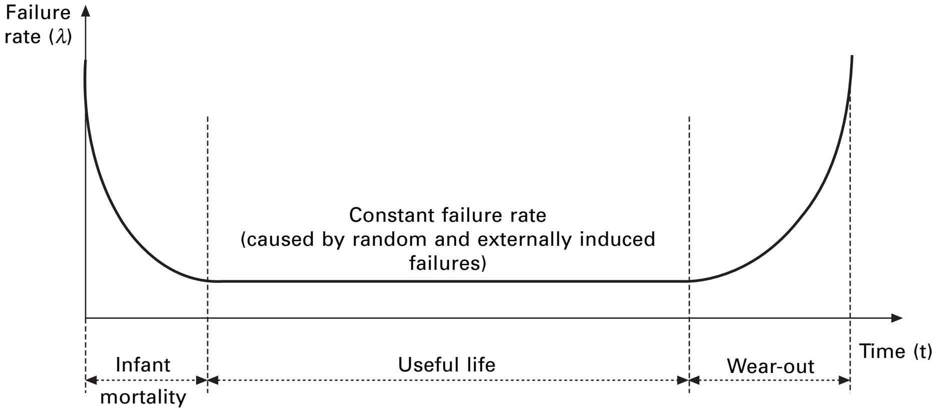
10.2.3 The Bathtub curve

No definition of reliability is complete without an understanding of the bathtub curve. It is generally accepted that a component's (or part or sub-system) failure rate is not constant, but generally goes through three phases over its lifetime. In the first phase the failure rate is relatively high, but decreases over time. Early failures may be due to manufacturing defects slipping through the quality control system, and the failures from only this mechanism are at a reducing rate which reaches zero when all the defective items have failed.[2] This is referred to as ‘infant mortality’ or ‘burn-in’.

In the second phase the failure rate is low and essentially constant. A constant failure rate is characteristic of failures which are unrelated to the age of the equipment, due either to ‘internal’ causes (i.e. design-induced such as software errors and operator malfunctions), or ‘external’ (i.e. stress-related) causes such as maintenance-induced on mechanical systems and overload failures on electrical or mechanical systems.

In the third phase the failure rate begins increasing again, often quite rapidly, due to age or usage. Deterioration can occur (often depending on atmospheric or other environmental conditions) that is unrelated to utilisation; rubber perishes, steel rusts, aluminium alloys exfoliate, magnetic storage devices degrade, etc. Total and degradation failures linked to usage are typically the results of a wearing-out process (e.g. tyre wear, bearing failure) or metal fatigue due to cyclic (electrical or mechanical) loading. All these failure rates are at a rate that increases with age or utilisation (whichever is more appropriate).

Together these produce the line on Fig. 10.2 that looks like a longitudinal section through a bathtub. Infant mortality failures are usually attributable to inadequacies in manufacture, maintenance, or design. The inadequacies result in a reduction in the ability of a component, equipment, or system to survive the environment to which it is subjected. Infant mortality failures exhibit relatively high failure rates during early



10.2 The bathtub curve[1].
1. Hardware usually follows a bathtub shaped curve with a constant reliability for most of its operational life. With software the situation is different, as the reliability does not alter with time. Assuming the stated conditions remain unaltered, then software is not subject to rusting, corrosion, or whatever and that usually simplifies calculations considerably. Software reliability may fluctuate as it is modified and during testing and debugging.

[2] As part of the quality assurance system, overload tests may be performed specifically with the intent of weeding out defective items, and most electrical components are subjected to an initial ‘burn-in’ time before delivery.

life. Random failures are usually attributable to external occurrences. As such, they are not related to the age of a component. However, in some instances it might be that a complex piece of equipment has many different failure modes and they combine to produce an overall failure pattern that appears in a random manner. Random failures exhibit failure rates that are independent of component age and hence are constant with time. Wear-out failures are usually attributable to a progressive deterioration of a component and exhibit progressively higher failure rates with component age. Typical of wear-out failures are fatigue, corrosion, wear, etc.

The actual (practical) useful life ends when the increased failure rate during wear-out becomes unacceptable in terms of economic or functional considerations. By eliminating the infant mortality failures and replacing them before or soon after the wear-out failures start occurring, the useful life is subject only to the constant failure rate. This is often referred to as preventative maintenance and may fall under the category of Certification Maintenance Requirements (see 'definitions' on page 325).

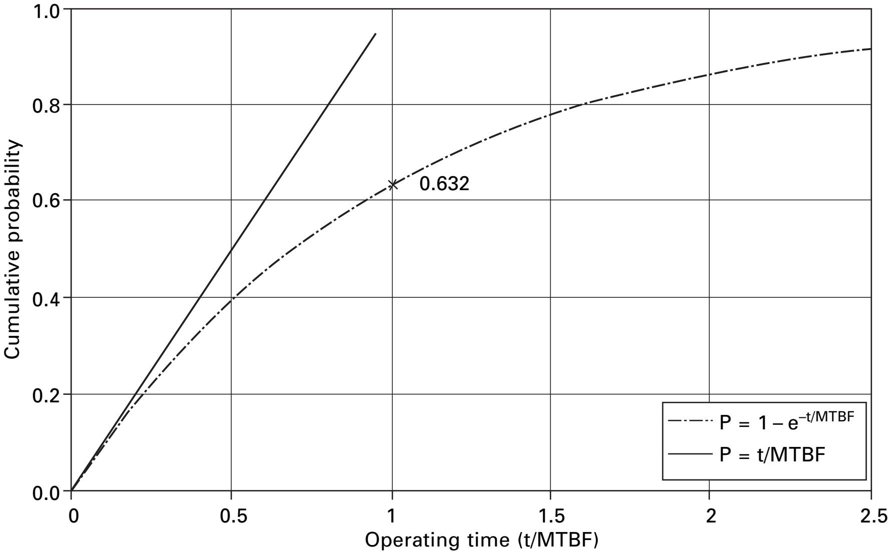
10.2.4 Relationship between failure rate, probability and MTBF

If failure rates for a component had to be plotted over time, the trend (excluding infant mortality and wear-out) would usually be reasonably constant and we will see that the failure rate (λ) is simply the reciprocal of the mean time between failures[3] (MTBF). So $\lambda = 1/\text{MTBF}$ in the constant failure rate phase. The MTBF is the average time a system will operate without a failure. One important characteristic of MTBF is that it is an ensemble characteristic which applies to populations (i.e. 'lots') of things, not a sample characteristic that applies to one specific thing (Daly, 1995). Daly explains this as follows:

> For many systems of interest today the required failure rates are so low that the MTBF substantially exceeds the lifetime. In these cases MTBFs are not only 'not necessarily' sample characteristics, but are 'necessarily not' sample characteristics. In the terms of the reliability *cognoscenti*, failure processes are not ergodic (i.e. you can't blithely trade population statistics for time statistics). The key implication of this essential characteristic of MTBF is that it can only be determined from populations and it should only be applied to populations.

MTBF is, therefore an excellent characteristic for determining how many spare flight displays are needed to support 20 aircraft, but a poor characteristic for guiding you on when you should change your flight display to avoid an unscheduled repair. However, information on the reliability of components is often available in the form of an MTBF. For the purpose of a safety assessment, we need to convert this MTBF

[3] MTBF can be calculated in one of several ways. An expected MTBF can be calculated on a statistical basis from the known failure rates of various components of the system. Specifically, it is the reciprocal of the sum of the failure rates of the components of the system (with the failure rates being expressed in failures per hour). Through empirical testing of a single part, the length of a performance measurement period can be divided by the number of failures that have occurred during that period. Through empirical testing of a group of items, the total functioning life of the population of items can be divided by the total number of failures within the population during the measurement period.



10.3 The exponential curve.

to find the corresponding probability of failure. But first we need to understand the relationship between MTBF and the probability of failure.

Suppose 1000 identical items (each with a failure rate of 1 every 1000 hours) start to run simultaneously (Lloyd and Tye, 1995, p. 48). After 100 hours, the accumulated operating time will be 100,000 h. In this period it is predicted that 100 items will fail. The surviving 900 items then run for another 100 h and 90 will fail, and so on. In short, as the number of surviving items diminishes, so also will the number of failures. If this is plotted against total hours, we obtain a curve similar to the one in Fig. 10.3. This is the 'exponential failure curve' $P = 1 - e^{-\lambda t}$, with e being the exponential number 2.718. On exactly the same reasoning, it can be shown than an individual item has a probability of failing at time t equal to $1 - e^{-\lambda t}$.

So, $P = 1 - e^{-\lambda t}$ and $\lambda = 1/MTBF$

$= 1 - e^{-t/MTBF}$.

Question: Will all similar equipment have failed by the time the MTBF has expired?

Answer: Now, by the time that t = MTBF, the failure probability is

$$\begin{aligned} P &= 1 - e^{-MTBF/MTBF} \\ &= 1 - 0.37 \\ &= 0.632 \end{aligned}$$

Hence it is commonly assumed that 63.2% of all equipment will have failed or needed repair by the time that it reached the MTBF.

Note: This is a total population statement from the manufacturer point of view not from the customer point of view. MTBF is a cumulative statistic. A customer can receive a brand new product and have it fail the day of installation and still meet the MTBF criteria because that failure simply adds to the count on the way to the 63.2% marker

If we are considering the active failure of a component in a flight, then the order of numbers that we will typically use in our assessments are a flight time of less than ten hours and failure probabilities in the order of $10^{-3} < p < 10^{-9}$ per flight hour. Therefore λt is unlikely to exceed 0.01 for typical aircraft systems and for such a small value we can comfortably assume that $1 - e^{-\lambda t} \approx \lambda t$ (see Fig. 10.3)[4]

So, if $P = 1 - e^{-\lambda t}$ and $\lambda t < 0.01$, then
$\approx \lambda t$.
We also know that the failure rate (λ) is equal to the reciprocal of the MTBF, so
$\approx$ t/MTBF
$\approx$ 1/MTBF for one flight hour.

It should be noted[5] by anyone comparing product reliability on the basis of MTBF that:

- there is no standard measure of MTBF. It is often calculated and inferred rather than tested. Extreme care should be taken in its application, as hopelessly optimistic data will be corrupted into the notion of an 'acceptable' failure probability
- the MTBF applies only statistically (and cannot be taken as an expected lifetime). The service life of a product is often shorter than its MTBF and failures do occur during that period
- the MTBF applies only within the service life of a product (that is, after burn-in and before the end of its service life, see bathtub curve). After this time failure rates are not inferred or guaranteed in any way.

10.2.5 Probability vs. reliability

In general, reliability is the consistency of a set of data or pattern of behaviour. More specifically, it may refer to one of several concepts:

- in engineering, the reliability of a device or system
- in statistics, the reliability of a set of data
- in experimentation, the reliability of an experiment.

For system safety we are interested in the first concept. Engineering reliability may be defined[6] in several ways:

- the capacity of a device or system to perform as designed
- the resistance to failure of a device or system

[4] The value of $1 - e^{\lambda t}$ can be written as an expansion as follows: $1 - e^{\lambda t} = \lambda t - \lambda^2 t^2/2 + \lambda^3 t^3/6 - \lambda^4 t^4/24...$, thus if there is any doubt whether pt is sufficiently small to justify the above approximation, this series provides an easy way of checking. However, be careful when applying this approximation to dormant faults (see section 10.5.3) where T can be sufficiently large so that $\lambda t > 0.01$.

[5] Refer http://en.wikipedia.org/wiki/Mean_time_between_failure (downloaded on 7/7/05).

[6] Downloaded from http://en.wikipedia.org/wiki/Reliability_%28engineering%29 on 7/7/05.

- the ability of a device or system to perform a required function under stated conditions for a specified period of time
- the probability that a functional unit will perform its required function for a specified interval under stated conditions.

System reliability requirements are specified using reliability parameters. The most common reliability parameter is the mean-time-between-failure (MTBF), which can also be specified as the failure rate or the number of failures during a given period. Reliability increases as the MTBF increases.

If the probability of failure = P, and the probability of not failing (i.e. the reliability) = R, then it is intuitive that P + R = 1, and so R = 1 – P. We also know that $P = 1 - e^{-\lambda t}$, so, $R = e^{-\lambda t}$.

Example

If a manufacturer says that his product has a reliability of, say, 0.9 for 10,000 hours, what he means is that the probability that a brand new unit (excluding infant mortality), if used properly, will survive beyond 10,000 hours is 0.9. The result: if R = 0.9, and $R = e^{-\lambda t}$ then $\lambda = -\ln(0.9)/10{,}000 = 1.05 \times 10^{-5}$ per hour.

It should be noted that sometimes logisticians refer to the 'unreliability' of the unit, Q = 1 – R. Note that this Q is not the same as the Q used in probability of not failing.

10.3 Applied quantitative assessment

Before we delve into the combined probabilities of various failure combinations in component parts of aircraft systems, it may be worthwhile to briefly remind ourselves of the basic logic.

10.3.1 Dependent events

Consider the probabilities involved in the toss of a coin, where the result will be either heads or tails.

Heads	Tails
✓	×
×	✓

The combined probability of all possible events is: $P_H + P_T = 1$. By definition, the probability of landing on both heads and tails is: $P_H + P_T = 0$, so it will never occur. This is known as a dependent event. Dependent events are those that cannot occur at the same time, and normally describe the probability of a system being in a particular state (e.g. a light can be either 'on' or 'off').

10.3.2 Independent events

In contrast, independent events can occur simultaneously (e.g. the probability of a dual redundant system failing). If two independent events (A and B) can occur, all possible combinations of those events can be described by the following:

Event A	Event B
✓	✓
✓	×
×	×
×	✓

Therefore, all possible combinations of events are:

$$P_A{\cdot}P_B + P_A{\cdot}Q_B + Q_A{\cdot}P_B + Q_A{\cdot}Q_B = 1$$

Subsets of the above state can be used to define combinations of the two events.

$$P_{(\text{A AND B})} = P_A{\cdot}P_B$$

and

$$P_{(\text{A OR B})} = P_A{\cdot}P_B + P_A{\cdot}Q_B + Q_A{\cdot}P_B$$

and we know that Q = 1 – P, so

$$\begin{aligned} P_{(\text{A OR B})} &= P_A{\cdot}P_B + P_A{\cdot}(1 - P_B) + (1 - P_A){\cdot}P_B \\ &= P_A{\cdot}P_B + P_A - P_A{\cdot}P_B + P_B - P_A{\cdot}P_B \\ &= P_A + P_B - P_A\, P_B \end{aligned}$$

However, when we are dealing with small probabilities (typically of the order 10^{-3} or less probable), then the solution approximates the dependent combination, i.e.,

$$P_{(\text{A OR B})} \approx P_A + P_B$$

10.3.3 Mutually exclusive events

Two events can be mutually exclusive. This means that one or the other can occur, but not both at the same time:

Event A	Event B
✓	×
×	✓

$$\begin{aligned} P_{(\text{A XOR B})} &= P_A{\cdot}Q_B + Q_A{\cdot}P_B \\ &= P_A{\cdot}(1 - P_B) + (1 - P_A){\cdot}P_B \\ &= P_A - P_A\, P_B + P_B - P_A\, P_B \end{aligned}$$

$$= P_A + P_B - 2(P_A\ P_B)$$

$$\approx P_A + P_B$$

when dealing with small probabilities (typically of the order 10^{-3} or less probable).

It is important not to confuse mutually exclusive events with dependent events, as the following example shows.

Example

Consider the case of two components, A and B, with failure probabilities respectively of P_A and P_B.

The four possible failure combinations	The probabilities of each of these combinations occurring
A and B fail	$P_A \times P_B$
A fails, B does not fail	$P_A \times (1 - P_B)$
A does not fail, B fails	$(1 - P_A) \times P_B$
Neither A nor B fails	$(1 - P_A) \times (1 - P_B)$

If A and B are independent events (i.e. they can occur simultaneously), then the probability that either can occur is:

$$P_{A+B} = P_A\ P_B + P_A(1 - P_B) + P_B\ (1 - P_A)$$

$$= P_A + P_B - P_A\ P_B$$

$$\approx P_A + P_B$$

If A and B are dependent events (i.e. they cannot occur simultaneously), then the probability that either can occur is:

$$P_{A+B} = P_A(1 - P_B) + P_B\ (1 - P_A)$$

$$= P_A + P_B - 2P_A\ P_B$$

$$\approx P_A + P_B$$

If A and B are mutually exclusive events (i.e. they cannot occur simultaneously), then the probability that either can occur is:

$$P_{A+B} = P_A(1 - P_B) + P_B(1 - P_A)$$

$$= P_A + P_B - 2P_A\ P_B$$

$$\approx P_A + P_B$$

If A and B are dependent events that are mutually exclusive, then the probability of $P_A\ P_B$ must be equal to zero and $P_A + P_B$ must equal unity. Therefore the probability that either can occur is:

$$P_{A+B} = P_A + P_B$$

10.3.4 Combined occurrences

Lloyd and Tye (1995, p. 42) advise us therefore to be very careful in calculating probabilities of combined occurrences to be sure we have properly counted the various possible permutations and combinations.

Example

Consider the probabilities involved in tossing a coin. If it is tossed twice there are basically three results: two heads, or two tails or one of each.

It is tempting to think that the chance of two heads is 1 in 3 (i.e. P = 0.33). But this is wrong, as there are four different possible outcomes:

1st throw	2nd throw
H	H
H	T
T	H
T	T

So the true probability of tossing two heads is 1 in 4 (i.e. P = 0.25), and the probability of tossing one head and one tail is 2 in 4 (i.e. P = 0.5).

Example

Consider the probabilities of failure for two simple units, A and B, with identical failure probabilities. So:

- A and B fail, P^2
- A fails, B does not fail, PQ
- A does not fail, B fails, QP
- neither A nor B fails, Q^2.

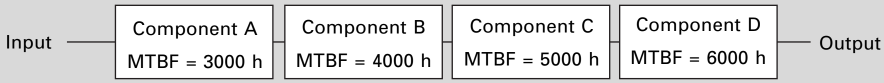
Extending this to larger numbers of units leads to the following:

No. of units	Number of failures			
	1	2	3	4
1	P			
2	2PQ	P^2		
3	$3PQ^2$	$3P^2Q$	P^3	
4	$4PQ^3$	$6P^2Q^2$	$4P^3Q$	P^4

10.3.5 Components connected in series

The following example illustrates how we calculate probabilities for a system consisting of a set of components arranged in a series architecture.

Example of components in series



What is the probability of a failure in system output?
Answer: failure will occur if either A or B or C or D fails, so

$$P_s = P_A + P_B + P_C + P_D \text{ (and we know that } P = \lambda t \text{ and } \lambda = 1/\text{MTBF)}$$
$$= (1/3000 + 1/4000 + 1/5000 + 1/6000)t$$
$$= (9.5 \times 10^{-4})t$$

So, for an average flight of four hours, the probability of:

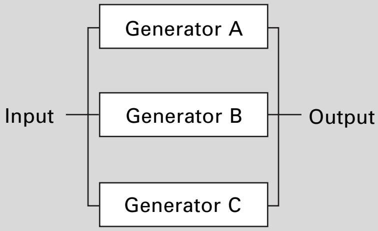
- system failure is 3.8×10^{-3}, and
- the average probability of system failure per flight hour is $p = 9.5 \times 10^{-4}$ per flight hour.

10.3.6 Components connected in parallel

The following example illustrates how we calculate probabilities for a system consisting of a set of components arranged in a parallel architecture.

Example of components in parallel

Consider the following triplicated fully active redundant system of three identical generators:



The possible failure combinations within this system are:

- Triple failure: A and B and C Probability = $P \times P \times P = P^3$
- Double failures: A and B: P^2, A and C: P^2, B and C: P^2 Probability = $3\,P^2$

  (For example, double failure may allow system to operate, but possibly at a reduced capacity).
- Single failures: A or B or C Probability = $3P$

As can be seen, when the number of channels is increased, the probability of total system failure is reduced. However, note also that the probability of single and multiple failures is increased thus reducing serviceability.

10.3.7 Probability of a particular failure mode

One final comment on the use of MTBFs: each system or piece of equipment may have various failure modes, each with their own effect (e.g. one failure mode may cause loss of functionality, while another may cause unwanted action). In the case of systems it may be necessary to calculate the MTBF for each separate failure mode. However, a singularly declared MTBF for a unit is usually all-encompassing of its individual failure modes and thus presents the worst-case failure probability.

10.4 Assessment process

There are a variety of qualitative and quantitative tools to calculate the probability of an undesired event (see Appendix A). The following is tailored from Lloyd and Tye (1995, Appendix 5-1).

- Step 1: describe how the system behaves.

> Example
>
> Consider a system comprising:
>
> - a main system (M),
> - a warning system (W) for when the main system fails, and
> - a standby system (S).
>
> M is in continuous operation in flight. If inoperable at pre-flight inspection, this is evident to the pilot and the instruction is to cancel the flight.
>
> If M fails in flight, this is evident to the pilot only if the warning system operates.
>
> On seeing the warning, the instructions are to check the functioning of M and to switch to the S if M has indeed failed.
>
> S and W can only be checked on the ground, such checks being prescribed at specified intervals.

Note how the above example raises a point about fail-safe design and dormant failures.

- Step 2: state the undesired event (e.g. hazardous condition) for which a probability has to be established. If applicable, include a reference to where the severity for this event was assessed and the safety objective allocated.

> Example (continued)
>
> Total system failure will cause a hazardous event and shall not occur more frequently than 10^{-7} per flight hour (if available, refer to applicable FHA line item or the regulatory requirement).

- Step 3: assemble the numerical values needed for the assessment. Include/reference all substantiating data.

Example (continued)

Average flight duration:	$T = 2$ h (assumption) (see section 10.5.4)
Check period of standby:	$T_s = 100$ h (refer to source)
Check period of warning:	$T_w = 50$ h (refer to source)
Probability of failure of M when active:	$p_m = 10^{-4}$ per h (refer to source)
Probability of failure of S when active:	$p_s = 10^{-3}$ per h (refer to source)
Probability of dormant failure of S:	$p_{si} = 10^{-5}$ per h (refer to source)
Probability of dormant failure of W:	$p_w = 10^{-4}$ per h (refer to source)

Within the scope of this assessment, the probability of human errors (e.g. failure to notice or act on warning, failure to make ground check, etc.) will not be considered.

- Step 4: define all circumstances (states of the system) for the hazardous condition to be present.

Example (continued)

For total system failure, the first event that must occur is a failure of the main system during flight. There are then two ways this can lead to a loss of system function:

A. If the pilot fails to switch over to standby
B. If the pilot does switch over, but there is an existing or subsequent loss of the standby.

- Step 5: define the precise failure sequences that can lead to the undesired event.

Example (continued)

A. Since it is assumed that the pilot will always see the warning, the only reason for not switching over when the system fails is if W failed.
Probability of M failing is: $P_m = p_m T$
Probability of W failing depends on the elapsed time since it was checked (i.e. it is ostensibly zero immediately after the check and $p_w T_w$ immediately before the next check. So, assume $P_w = p_w T_w/2$
Hence, $P_s = p_m T \times p_w T_w/2 = 5 \times 10^{-7}$ per flight.
B. For case B we have two fault sequences:
B1: S in already inoperative when the pilot switches over to it. This case is exactly equivalent to the dormant failure of the warning.
So: $P_s = p_m T \times p_{si} T_s/2 = 1 \times 10^{-7}$ per flight.
B2: S fails after the pilot switches over to it. For this sequence, we have: $P_s = p_m p_{sa} T^2/2 = 2 \times 10^{-7}$ per flight.

- Step 6: summarise the probability of the hazardous event occurring

Example (continued)

The probability of this hazard occurring is thus A + B1 + B2 = 8×10^{-7} per flight. Since the average flight time is two hours, the probability that this will occur during this flight is 4×10^{-7}, i.e. $p_{system} = 4 \times 10^{-7}$ per flight hour.

- Step 7: consider the acceptability of the assessed probability. If it is too high in relation to the consequence then it is necessary to consider what action should be taken.

Example (continued)

Option 1: clearly, P_m contributes directly to the average probability through all three failure sequences. Thus any improvement in its reliability would be reflected proportionately in the total.

Option 2: the greatest contribution to the probability arises from fault sequence A, and this contribution could be reduced if there were a pre-flight test of the warning system. It would become $p_m p_w T^2/2 = 2 \times 10^{-8}$ per flight.

Option 3: similarly, the contribution of the dormant S failure through sequence B1 could be reduced by preflight check: it would become $p_m p_{si} T^2/2 = 2 \times 10^{-9}$ per flight.

Option 4: any improvement to the reliability of the standby system would be proportionality reflected through the contribution of B2 to the total probability.

10.5 Specific issues of concern

10.5.1 Common mode failures

Often when we calculate the probability of multiple failures we are inclined to assume that the failures are totally independent from one another (i.e. one failure has no influence on the likelihood of other failures). This is a risky assumption because, in practice, there are variations on this ideal.

Examples

Scenario 1: in the generator example in section 10.3.6, failure of one or two generators could lead to increased loads on the remaining generator(s), which could increase its probability of failure (i.e. cascading failure).

Scenario 2: a dual redundant system may be compromised by a single failure, such as when the power supply cabling is routed via the same bus or circuit breaker (i.e. common part failure could cause total loss of system functionality).

Scenario 3: contamination of hydraulic fluid could result in failures of all channels in that hydraulic system (i.e. common cause failure).

Even though the probability of a common-mode failure is often very low, it can totally dominate the overall probability of system failure.

Examples

In the generator example in section 10.3.6, if $P_{gen} = 10^{-3}$ for each generator, then total generator failure probability is $(10^{-3})^3 = 10^{-9}$. However, assume there is a common-mode failure (e.g. a common bus-bar) with a failure probability of 10^{-7}, then the total failure probability of the system may be reduced to $10^{-7} + 10^{-9} = 1.01 \times 10^{-7}$, which might be unsatisfactory.

When considering systems failures, we need to remain aware of any common mode failures and/or cascading failures and ensure that we include them in our qualitative/quantitative assessments. See Chapter 6 for more information on these types of failure.

10.5.2 Failure sequences

Up to now we have assumed that the sequence of failures in the flight makes no difference to the end result. This is not always the case.

Example

Consider again the example in section 10.4 (Step 5). Activation of the standby system depends on a warning that the main system has failed. If the warning was already inoperative, by virtue of a dormant fault, the operability of the standby would be of no consequence as the pilot would be unaware of the need to activate it.

So, in some instances, the failure sequence is important to calculate the probability of system failure. The following example from Lloyd and Tye (1995) explains the logic.

Example

Consider systems A and B: If the sequence of failures is immaterial, the probability of double failure is $P = p_A\, p_B\, T^2$. If A had to fail before B:

- the probability of A failing before a time t is: $P_A = 1 - e^{-p(A)t}$
- the probability of B not failing before time t is: $R_B = e^{-p(B)t}$
- the probability of B failing in the period between t and t + dt is $P_B = p_B dt$.

Over the flight of duration T, the probability that A will fail before B is therefore:

$$P_{AB} = \int_0^T (1 - e^{-p(A)t}) \cdot e^{-p(B)t} \cdot p_B dt \text{ (see section 10.5.4).}$$

To a first approximation, this works out to be:

$$P_{AB} = p_A\, p_B\, T^2/2\, (1 - (p_A + 2p_B)T/3)$$

$$\approx p_A\, p_B\, T^2/2 \text{ for small values of } p_A T \text{ and } p_B T.$$

So logically, for two systems, the probability of one failing before another is approximately half the probability of both failing. The same argument can be applied to, say, three items. The order of failure can be ABC, ACB, BAC, BCA, CAB or CBA. Thus one-sixth of the failures are in a specified order with a probability of $p_A\ p_B\ p_C\ T^3/6$.

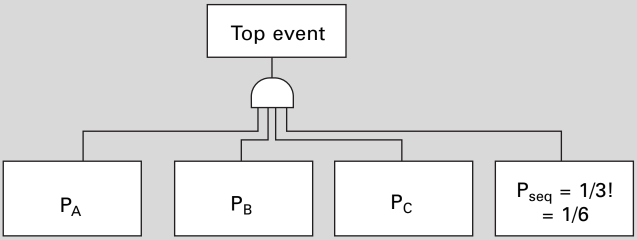
SAE ARP4761 advises that 'failure order dependent events' (i.e. sequential events) can be drawn via a fault tree analysis as follows:

- Use events as inputs into an AND-gate.
- Add events from left to right in order of occurrence.
- Add another 'undeveloped event' which represents the probability that the number of events (n) will fail in that order, with $P_{seq} = k/n!$, with k = number of events in the sequence, n = number of sequences and $n! = n(n - 1) \times (n - 2) \ldots (n - n)$.

Example

Consider three systems A, B and C. If the sequence of failures is immaterial, the probability of total failure is $P = p_A\ p_B\ p_c T^3$
However, if the sequence of failure is important, then

$$P = p_A T \times p_B T \times p_C T \times 1/6$$
$$= (1/6) p_A\ p_B\ p_c T^3$$



10.5.3 Unrevealed/dormant failures

See Chapter 6 section 6.3.1. A dormant fault is one that remains undetected until another failure occurs, or until the use of the system is suddenly required (e.g. the landing gear which is operated infrequently). Designers should try to prevent any dormant failures in their designs. However, if still possible, the probability of its occurrence can be mitigated by making specific checks (e.g. before each flight, or at specified maintenance or flight check intervals).

The desired intervals can be calculated via probabilistic assessment methods as follows: if p = the probability of a dormant fault per flight hour and T_c = the duration between checks then the probability of the fault being present is: $P = pT_c$ (or, more precisely $P = 1 - e^{-pTc}$, especially if T_c is large). So, the probability of a dormant fault depends on the elapsed time since it was last checked (i.e. it is ostensibly zero immediately after the check and pT_c immediately before the next check, leading to 0 at T_c = MTBF. Thus, the average probability of a dormant fault will be: $P = {}^1\!/_2 pT_c$, or for very long check periods, $P = {}^1\!/_2(1 - e^{-pTc})$.

10.5.4 The time of exposure

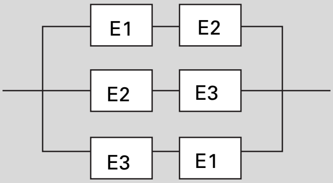
While many risks are dependent on the number of hours of exposure, others depend on:

- the phase of flight (e.g. an automatic landing system which operates only for a few minutes and which should have the capability of being checked prior to commencing the critical part of the approach), or
- the number of times an item operates (e.g. a landing-gear mechanism which normally operates only twice per flight).

These risks have nothing to do with the duration of the flight. The fact that the system is used only for a short period, particularly towards the end of a flight (e.g. brakes, flaps, etc.) does make the system's integrity vulnerable to dormant failures which become apparent only when the system is needed. In these cases, if the probability 'per use' = p, then the probability of failure in a flight = np, where n is the number of uses per flight.

Example

Consider the probability of a double engine failure on the Tristar aircraft (which has three engines). The dependence diagram (see Chapter 6) for this double failure condition could be any of the following:



So, $P_{double} = P_1 \times P_2 + P_2 \times P_3 + P_1 \times P_3$.

If we assume that the average probability of an engine failure is 1×10^{-4}, then:

$$P_{double} = 3P^2$$

We know P = pT, so p = P/T, thus the probability per flight hour is:

$$p_{double} = 3(P)^2/T$$
$$= 3(1 \times 10^{-4})^2/T$$

The most severe time for this to occur would be during take-off, which we assume takes 60 seconds.

So, the probability of a double engine failure during take-off is:

$$p_{double} = 1.08 \times 10^{-4} \text{ per flight hour.}$$

Note that this assumes that the probability of an engine failure during the high take-off loads is not significantly different from the average engine failure rate.

Thus, when estimating total probabilities, including probabilities of combined failures, it is important to remember whether the individual probabilities are of the 'per hour' kind or the 'per use' kind. In the aircraft industry, these then need to be converted back into an 'average probability per flight hour' so that it can be compared with the safety criteria in Table B.4. The average probability per flight hour is normally calculated as the probability of a failure condition occurring during a typical flight of mean duration divided by that mean duration. The process of calculating the 'average probability per flight hour' for a failure condition is described by ACJ25.1309 (Amendment 16, Section 2, Appendix 3) as a four-step process and is based on the assumption that the life of an aeroplane is a sequence of 'average flights'.

Step 1: determination of the 'Average flight'

The average flight duration should be estimated based on the actual/predicted cumulative flight hours divided by the cumulative aeroplane flights for the service life of the aeroplane. The duration of each flight phase (e.g. take-off, climb, cruise, descent, approach and landing) in the 'average flight' should be based on the average flight profile.

Step 2: calculation of the probability of a failure condition for a certain 'average flight'

$P_{\text{Flight (Failure)}}$ can be obtained using structured methods (e.g. FTA, ETA) to consider the probability of occurrence (P) of all significant elements (i.e. combinations of failures and events) that contribute to the failure condition. ACJ25.1309 advises us to consider the following:

- If the failure is relevant only during certain flight phases, the calculation should be based on the probability of failure during the relevant 'at risk' time for the 'average flight'.
- If there is an effect only when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce the failure condition (see section 10.5.2).
- If one or more failed elements in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation should consider the relevant exposure times (e.g. time intervals between maintenance and operational checks/inspections). In such cases the probability of the failure condition increases with the number of flights during the latency period.
- If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the failure condition occurring on an 'average flight'.

It is assumed that the 'average flight' can be divided into n phases (phase 1, ... , phase n), so:

$$T_F = \sum_{j=1}^{n} T_J \quad \text{With: } T_F = \text{'average flight' duration,}$$

$T_j = t_j - t_{j-1}$ = duration of phase j and t_j the transition point between T_j and T_{j+1}

$j = 1, 2, 3, \ldots, n$

Now, if $P_{\text{Flight (Failure)}}$ = the probability that the element fails during one certain flight (including non-flying time), and $P_{\text{Phase j (Failure)}}$ = the probability that the element fails in phase j, then two cases are possible:

- The element is checked by the operative at the beginning of the certain flight. Then:

$$P_{\text{Flight(Failure)}} = \sum_{j=1}^{n} P_{\text{Phase j(Failure)}} \quad \text{and we know that } P = 1 - e^{-\lambda t}$$

$$\text{so:} \quad P_{\text{Flight(Failure)}} = 1 - \prod_{i=1}^{n} \exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)\,dx \right)$$

- The state of the item is unknown at the beginning of the certain flight. Then:

$$P_{\text{Fight(Failure)}} = P_{\text{Prior (Failure)}} + (1 - P_{\text{Prior(Failure)}}) \cdot \left(1 - \prod_{i=1}^{n} \exp\left(-\int_{t_{i-1}}^{t_i} \lambda_i(x)\,dx \right) \right)$$

where $P_{\text{Prior (Failure)}}$ = the probability that the failure of the element has occurred prior to the certain flight.

Step 3 calculation of the 'average probability per flight' of a failure condition

Calculate the probability of the failure condition by summing up the average probabilities per flight (during the relevant time) and divide it by the number of flights during that period.[7]

$$P_{\text{average per flight}}(\text{failure condition}) = \frac{\sum_{k=1}^{N} P_{\text{flight k}}(\text{failure condition})}{N}$$

Where N = the quantity of all flights during the relevant time,

and $P_{\text{flight k}}$ = the probability that the failure occurs in flight k.

[7] The principles of calculating are described in more detail in Documents such as:

- RTCA, Inc., Document No. DO-160D/EUROCAE ED-14D, Environmental Conditions and Test Procedures for Airborne Equipment.
- RTCA, Inc., Document No. DO-178B/EUROCAE ED-12B, Software Considerations in Airborne Systems and Equipment Certification.
- Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754/ EUROCAE ED-79, Certification Considerations for Highly Integrated or Complex Aircraft Systems.
- Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

Step 4: calculation of the 'average probability per flight hour' of a failure condition

Once the 'average probability per flight' has been calculated it should be normalised by dividing it by the 'average flight' duration T_F in flight hours to obtain the average probability per flight hour'.

$$P_{\text{Average per FH}}\,(\text{failure condition}) = \frac{P_{\text{Average per flight}}\,(\text{failure condition})}{T_F}$$

This process may be very complicated and, with reference to Fig. 5.1, unnecessarily accurate. A rough estimate of average flight time (e.g. 10 hours for long haul 747 aircraft, or 3 hours for military C-130 aircraft) may prove of be sufficiently accurate.

10.5.5 Where flight procedures are important

In some instances, the probability of multiple failures will depend on the strategy of the flight.

Example

Assume a flight of T duration in a twin-engine aircraft and each engine has a probability of p per hour of failing. The probability of a double failure is thus: $P = p^2T^2$. After a first engine failure, the pilots may have to decide between the following options:

(a) If we decide to return to base after the first failure, then the probability of one item failing in a short time interval is p.dt. If this occurs at time t, the return flight will take t hours, so the probability of a second failure is pt. The probability of a double failure is therefore:

$$P = \int_0^T p^2 t \cdot dt = p^2T^2/2$$

as the sequence can be either AB or BA, the total probability for this double failure condition is therefore $p^2\,T^2$.

(b) A more beneficial strategy would be to return to base if the first failure occurred before T/2 and to continue if the first failure occurred after T/2. We can regard the flight as being in two halves, each of duration T/2. From (a) above, the probability of double failure in each half is $P = p^2(T/2)^2$. This halves the total risk as compared to (a).

(c) On long flights the risk can be reduced by diverting to an alternative base H hours flight time away. The probability of a first failure in an interval of time dt is as before p.dt and the probability of a second failure in the remaining time H is pH. The double failure probability is therefore:

$$P = \int_0^T p^2\,H \cdot dt = p^2HT$$

again, as the sequence can be either AB or BA, the total probability is $2p^2$ HT.

Recommendations from this assessment will therefore need to be incorporated in the aircraft flight manual, emergency reference cards, as well as the minimum equipment list. These recommendations will tend to ensure that the safety objectives of the system are not compromised for the remainder of the flight.

Example

Suppose we have a duplicated system with a single system failure probability of failure of 3.16×10^{-4} per hour. Suppose further that system failure could have hazardous consequences, so the safety objective is 10^{-7} per hour. If the procedure is to fly on to the destination after a first failure, what flight time is allowed?

The probability of a double failure is: $P_{double} = p^2 T^2$

and we need to ensure that $p \leq 10^{-7}$, so $P_{double} \leq 10^{-7}T$ (because $P = pT$)

so: $p^2 T^2 \leq 10^{-7}T$

$$(3.16 \times 10^{-4})^2 T^2 \leq 10^{-7}T$$

$$T \leq 1$$

so, the strategy allows short flights of up to one hour only.

If the procedure were to return to base following a first failure up to the mid-way point, and to proceed to destination if first failure occurred after the mid-point:

now: $P_{double} = p^2T^2/2 \leq 10^{-7}T$

so: $T \leq 2$ hours

This means that the aircraft may fly on routes up to two hours duration.

For longer flights, suppose it would be possible to divert to an alternative landing point no more than half an hour away from the flight track. After the first failure, the procedure would then be to return to base in the first half hour of flight, to continue to destination in the last half-hour, and in the central segment (duration T – 1) to divert to the nearest alternative.

Then: $P_{double} = P_{Fail\ 1}$ in first 1/2hr + P_{double} in time H + $P_{Fail\ 2}$ in last 1/2hr

$$= p^2 (1/2)^2 + 2\,p^2 \cdot (1/2)(T - 1) + p^2 (1/2)^2$$

$$= p^2 (T - 1/2) \leq 10^{-7}T$$

This means that there is no limit on flight duration, assuming that the furthest alternative airfield is no further than an half a flight hour from the flight route.

10.5.6 Applying failure probabilities to digital systems

A large proportion of the complexity of a modern system is implemented by software. Murphy (1991) notes that, because software malfunction characteristics do not follow any recognised law, it means that the implications of software on safety are very difficult to assess. The occurrence of software errors is probabilistic but not in the same sense as hardware failures. Unlike hardware failures, these probabilities cannot be quantified. Software does not normally 'fail' in the traditional sense of the word, i.e., it does not normally malfunction. If it does not perform its intended function, then a design error exists which has probably been present since the software was first created.

It is almost impossible to test complex software fully – even if it is run many times – as there are an almost infinite number of possible loops, variables and subroutines that may or may not be run in any single program. Program operation is by its very nature non-linear or non-determined and therefore can never be fully tested at box level. For these reasons, reliability calculations are not applied to software, as it has no MTBF. Instead, we make use of development assurance levels (DAL) or safety integrity levels (SIL) (see Table B.6). The main aim or purpose of DALs and SILs is to introduce a number of repeatable 'life-cycle processes' which (if used by the developer) will produce a final product that is capable of meeting not only the original specification requirements, but also producing the correct level of safety both for the developed equipment and the overall aircraft.

Depending on a number of factors (such as system architecture, software segregation and software partitioning) proof of the level of development assurance may lead to a qualitative occurrence claim level as shown in Table 10.1 (see also Table B.6) Due to the fact that digital systems are becoming so prevalent in modern aircraft, this step is essential in determining the probability of various system level functional failure modes. The assurance of integrity depends heavily upon a considerable amount of design effort and engineering judgement. As with analogue and mechanical systems, the overall functional integrity of the system is dependent both on the integrity of the individual components, as well as the architecture of the system (e.g. though the use of dissimilar redundancy).

Numerical probabilities should not be indicated for software errors in fault trees. Any software analysis in an FTA should be expressed in terms of DALs to protect against software errors. The analysis should be evaluated for compliance on a purely qualitative basis. When the probability of an undesired event needs to be calculated, SAE ARP4761 (para 4.1.2) advises as follows:

> Embedded software may be qualitatively included in the FTA/DD/MA for certain systems and items. In particular, FTA/DD/MA may be necessary to provide adequate analytic visibility of software safety issues for complex systems, especially when credit is taken for the following safety attributes:

Table 10.1 Software development assurance levels

	No safety effect	Minor	Major	Critical	Catastrophic
Required DAL	No requirement	Level D	Level C	Level B	Level A
Occurrence claim level	Frequent	Reasonably probable	Remote	Extremely remote	Extremely improbable

a. Systems and items which provide fail-safe protection against software errors (The protection may be provided either via other software or via hardware alone.)
b. Systems and items in which software provides fail-safe protection against hardware errors or hardware faults.
c. Systems and items in which software provides protection against latent hardware faults.

When software is included in fault trees, the relationship between the top level hazards and specific software anomalous behaviours should be clearly established. It is important to explicitly identify the affected functions and to identify how the specified intended functions are affected.

Specific protective strategies can be determined from the various potential cause factors associated with the specific software anomalous behaviours. These protective strategies can include architectural mechanisms in hardware or software and/or specific verification activities as part of a safety directed development (see ARP4754).

This of course makes calculating the probability of the top-level event complicated without an assumption that gives a numerical value to the qualitative term[8]. If such an assumption is used, it should be explicitly stated, in which case the probability of the top-level undesired event should be reconverted into a qualitative expression of probability of occurrence.

10.6 Determining failure rates of basic events

10.6.1 Probability estimation

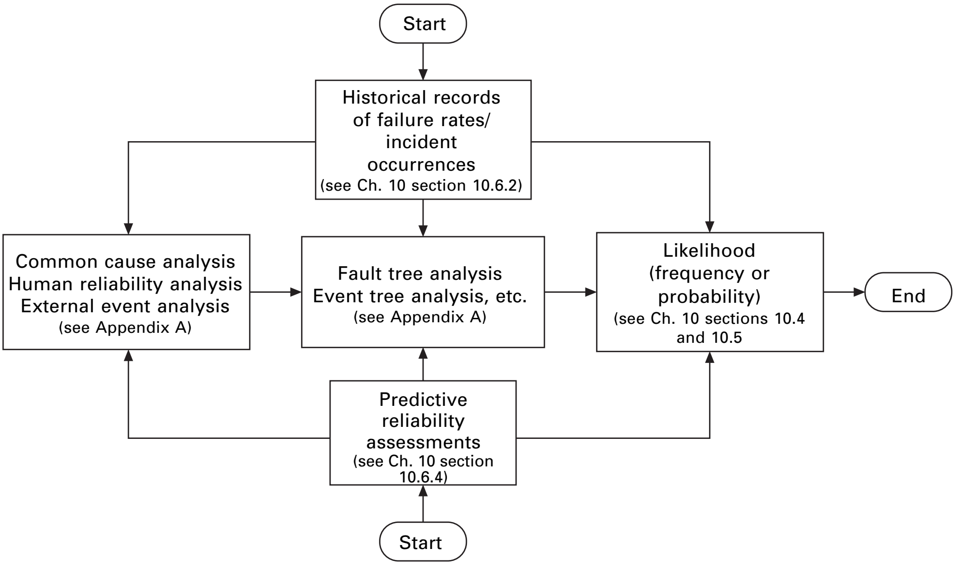
The starting point for all quantitative reliability assessments lies with the determination of values allocated to the primary events. The probability of a certain event occurring is usually derived from either predictive analysis, or relevant experience-based data, combined with assessment techniques such as fault tree analyses. This is illustrated in Fig. 10.4.

10.6.2 Historic data

Strictly speaking, the true MTBF of an item cannot be known exactly until the very end of its service life, and at that point it is therefore of no practical use. However, as time goes by, it is possible to make an increasingly accurate prediction of the true MTBF based on historical data accrued so far. Historic data comes in two forms:

1. Data collected from exposure to certain occurrences, examples of which can be found in Table 10.2.
2. Service experience of a specific component, where the in-service MTBF is used as a foundation for the probability estimation (see section 10.2). However, care

[8] In this case, think of the qualitative value as an indication of probability of occurrence, not failure probability.


Start
Historical records of failure rates/ incident occurrences (see Ch. 10 section 10.6.2)
Common cause analysis
Human reliability analysis
External event analysis
(see Appendix A)
Fault tree analysis
Event tree analysis, etc.
(see Appendix A)
Likelihood (frequency or probability)
(see Ch. 10 sections 10.4 and 10.5
End
Predictive reliability assessments
(see Ch. 10 section 10.6.4)
Start

10.4 Frequency-estimating methods.

must be taken if the environment of the component is different from that for which it is designed. The declaration of a MTBF must therefore be related to specific operating conditions and confidence levels (see below), or else the value is meaningless.[9]

Example

A qualified (e.g. TSO'd) component may have 15 year service use in a commercial turbojet aircraft. During this time it may have proven to have a constant MTBF. However, if this component is installed in a military turboprop aircraft, the MTBF assumption may no longer be valid due to, amongst other things, the following environmental factors:

- Vibration, especially the critical frequency generated by the blade passing frequency (i.e. propeller rpm × number of blades)
- Altitude: civil aircraft rarely operate unpressurised above FL150, whilst some military aircraft do go above FL300 for tactical missions.

When, due to service experience, there are large amounts of failure data available, we can divide the total number of failures by the total running time to obtain a failure rate with which we can feel confident. However, if the sample size is small (or for

[9] There are several points to remember about the nature of MTBF including: The true MTBF never changes, but the value of the observed MTBF will, and as time goes on will approach the value of the true MTBF. The occurrence of failures will be random in time, but governed by the MTBF. The MTBF will be different for different operating conditions.

Table 10.2 Useful aircraft related event probabilities[1]

Event	Probability of occurrence	Source	Comments
Air temperature <–70 °C	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Any rejected take-off	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Busbar failure	$P = 1 \times 10^{-6}$	Lloyd and Tye, 1995 p. 76	'A recognised assumption'
Cabin high altitude requiring passenger oxygen	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Electrical control system interconnections	$P = 1 \times 10^{-6}$	Lloyd and Tye, 1995, p. 76	'A recognised assumption'
Fire in lavatory, cargo compartment, APU compartment, engine.	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Flight conditions ≤ 0 g	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Flight conditions ≥ 1.5 g	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Flight conditions requiring stall warning	10^{-2} per flight	ACJ25.1309 Amendment 16 Appendix 4	Assumption
Flight conditions resulting in a stall	10^{-5} per flight	ACJ25.1309 Amendment 16 Appendix 4	Assumption
General omissions error	$P = 3 \times 10^{-3}$ per crew member per flight hour	Assumption	Errors of omissions embedded in a well-rehearsed procedure may be given the probability $p = 3 \times 10^{-3}$ per crew member per flight hour
Go-around	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Gust and turbulence at limit design	10^{-5} per flight hour	ACJ25.1309 Amendment 16 Appendix 4	See also JAR25.341 (under review by Structures Harmonisation Working Group)
High energy rejected take-off	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	

[1] For suggested additions, or an up-to-date version of this table, please contact the author at www.aircraftsystemsafety.com

Table 10.2 Contd

Event	Probability of occurrence	Source	Comments
HIRF conditions	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Icing normal (trace, light, moderate icing)	1	ACJ25.1309 Amendment 16 Appendix 4	
Icing severe	10^{-2} per flight	ACJ25.1309 Amendment 16 Appendix 4	
Lightning strike	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Lightning strike to large aircraft	1 every 6000 h world wide 1 every 2400 h in EU	Lloyd and Tye, 1995, p 84	Main strikes occur between the extremities of the aircraft but they can sweep along the fuselage or across the wing behind projections such as the engines. Principal concerns: • ignition of fuel vapour at vents • disruption of non-metallic unbonded parts • voltage injection into system (particularly if earthed) from a charged aircraft skin. • localised heating of non-metallic panels • lightning dwell (e.g. where paint is too thick) causing localised heating and even penetration
Need to jettison fuel	No accepted standard data	ACJ25.1309 Amendment 16 Appendix 4	
Wind: cross wind >20 kts during take-off and landing	10^{-2} per flight	ACJ25.1309 Amendment 16 Appendix 4	See also AC120-28, JAR-AWO
Wind: head wind >25 kts during take-off and landing	10^{-2} per flight	ACJ25.1309 Amendment 16 Appendix 4	See also AC120-28, JAR-AWO

Notes: if 'no accepted standard data' appears in this table, then the designers must provide a justified value if the probability used is less than 1. Sometimes data are valid only in special circumstances. For instance, a statistical source may indicate that a specific number of aircraft accidents due to birdstrikes take place every 100,000 or million hours. One may conclude from this data that the probability of a birdstrike is comparatively low. Hidden by the data analysis approach is the fact that at certain airfields, such as Boston, the Midway Islands, and other coastal and insular areas where birds abound, the probability of a birdstrike accident is much higher than the average. This example demonstrates that generalised probabilities will not serve well for specific, localised areas. This applies to other environmental hazards such as lightning, fog, rain, snow, and hurricanes.

Table 10.3 The Poisson distribution[1]

Distribution	Functional form	Mean	Standard deviation
Poisson	$f_p = \frac{e^{-a}a^x}{x!}$	a	$a^{1/2}$

[1] See http://hyperphysics.phy-astr.gsu.edu/hbase/math/poifcn.html#c2.

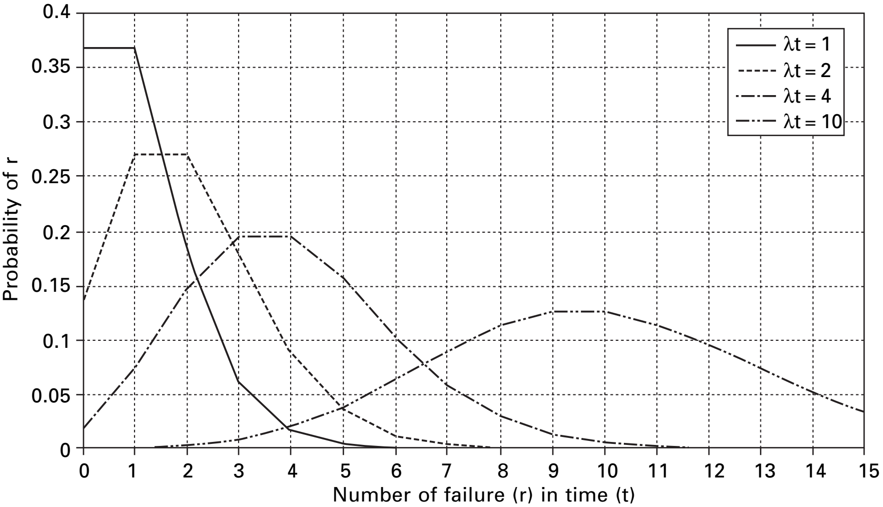
new products where the test runs are short) we need to find a way to make best use of the data available to establish the predicted MTBF. It is possible to quantify this effect statistically, and thereby attach confidence values to the MTBF declared. The Poisson distribution (which is not dependent on sample size)[10] provides a useful way to assess the percentage of time when a given range of results will be expected (Table 10.3).

The Poisson equation for predicting the probability of a specific number of failures (r) in time (t) is:

$$P(r) = \frac{(\lambda t)^r e^{-\lambda t}}{r!}$$

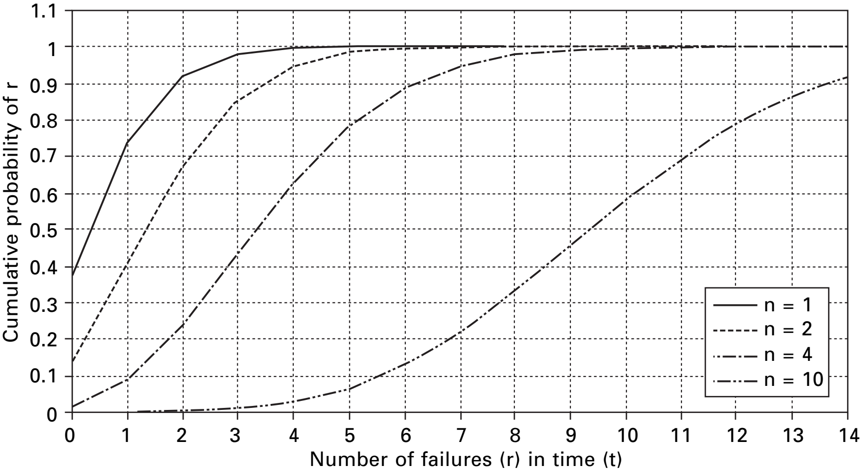
where: r = number of failures in time (t)
λ = failure rate per hour
t = time expressed in hours
P(r) = probability of getting exactly r failures in time *t*

See Fig. 10.5 for the developing trend of the Poisson curve for ever increasing values of λt.

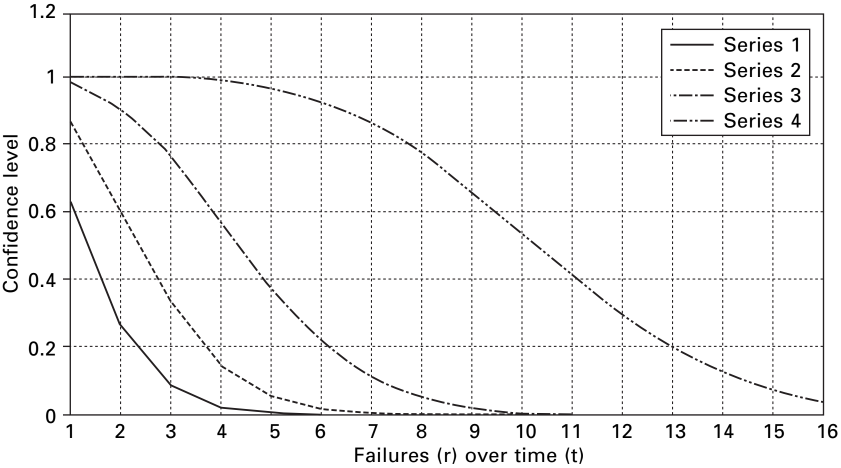


10.5 Example of Poisson distributions.

[10] See Papoulis (1984), pp. 101 and 554; Pfeiffer and Schum (1973), p. 200, http://mathworld.wolfram.com/PoissonProcess.html, and http://mathworld.wolfram.com/PoissonDistribution.html



10.6 Example of cumulative Poisson distributions.



10.7 Example of Poisson confidence levels.

To calculate the probability of k or fewer failures occurring in time (t), the probability of each failure occurring must be summed (Sherwin, undated, Vol. 9 No. 1):

$$P(r \leq k) = \sum_{0}^{k} P(r)$$

Figure 10.6 shows the developing trend for ever increasing λt.

The confidence level (CL) that the population has a failure rate (λ) based on r ≤ k failures occurring in time (t) is:

$$CL = 1 - \sum_{0}^{k} P(r)$$

Figure 10.7 shows the developing trend for ever increasing values of λt.

Example

Assume that the population of a component has a failure rate of 121.7 failures per one million hours. The component is expected to operate for 43,800 hours and only two failures are expected to occur.

Question 1: What is the probability of two or fewer failures over 43,800 hrs?

Answer 1: $P(r) = \dfrac{(\lambda t)^r e^{-\lambda t}}{r!}$, so

$$P(0) = \frac{(121.7 \times 10^{-6} \times 43800)^0 e^{-121.7\times10^{-6}\times43800}}{0!} = 0.0048$$

and

$$P(1) = \frac{(121.7 \times 10^{6} \times 43800)^1 e^{-121.7\times10^{-6}\times43800}}{1!} = 0.0256$$

and

$$P(2) = \frac{(121.7 \times 10^{-6} \times 43800)^2 e^{-121.7\times10^{-6}\times43800}}{2!} = 0.0682$$

So, $P(r \leq k) = \sum_0^k P(r) = 0.0048 + 0.0256 + 0.0682 = 0.0986$

Question 2: How confident are we of the failure rate of the population?

Answer 2: $CL = 1 - \sum_0^k P(r) = 1 - 0.0986 = 0.9014$, so 90.14% confident.

We need also to keep a clear distinction between the terms ‘probability’ and ‘probability density’ when using service records to establish the patterns of failures over time. Probability density refers to the frequency of occurrence of failures at a particular time t. As time proceeds and failures occur, the number of surviving items diminishes (see the exponential curve in Fig. 10.3). With fewer survivors there are fewer failures. Lloyd and Tye (1995, p. 50) advise that the simplest approach is to count failures occurring between time intervals (e.g. 0 to 500 hours, 500 to 1000 hours) and to divide each by the corresponding total number of item-hours in each interval. If this gives more or less a constant figure then this means that the failure rate is constant and any confusion with the varying probability density is avoided.

Historic data is most desirable for the following reasons:

- credibility: the use of real data from previous incidents avoids the need for further justification of the likelihood, provided appropriate and accurate data is used.
- speed: it is much quicker than using other techniques, which often require considerable expertise.

Unfortunately historic data is not always available and then we need to make use of predictive methods.

10.6.3 Reliability predictions

Reliability predictions are commonly used in the development of products and systems to compare alternative design approaches and to assess progress toward achieving reliability design goals. They are often criticised as not being accurate forecasts of field reliability performance because they do not usually account for all the factors that cause field failures.

Nevertheless, predictions are a valuable form of analysis that also provide insight into safety, maintenance and warranty costs and other product considerations. US Department of Defence Handbook (MIL-HDBK-217F, dd Dec 1991) can be used for reliability prediction of electronic components (e.g. microcircuits, semi-conductors, lasers, resistors, capacitors, etc.).[11] The purpose of MIL-HDBK-217 is

> to establish and maintain consistent and uniform methods for estimating the inherent reliability (i.e., the reliability of a mature design) of military electronic equipment and systems. It provides a common basis for reliability predictions during acquisition programs for military electronic systems and equipment. It also establishes a common basis for comparing and evaluating reliability predictions of related or competitive designs. The handbook is intended to be used as a tool to increase the reliability of the equipment being designed.

This handbook contains two methods of reliability prediction – 'Part Stress Analysis' (in Sections 5 through 23) and 'Parts Count' (in Appendix A). These methods vary in the degree of information needed to apply them:

- The part stress analysis method requires a greater amount of detailed information regarding the components and is applicable during the later design phase when actual hardware and circuits are being designed. It therefore offers a more accurate estimate of failure rate.
- The parts count method requires less information, generally part quantities, quality level, and the application environment. This method provides a simpler reliability math[12] and is applicable during the early design phase (e.g. during proposal formulation) when detailed information is not available, or a rough estimate of reliability is all that is required.

[11] MIL-HDBK-217 was the original standard for reliability. It was designed to provide reliability math models for nearly every conceivable type of electronic device. It is used both by commercial companies and the defence industry, and is accepted and known worldwide. It is sometimes referred to as MIL 217, MIL Handbook 217, MIL-217, MIL-217F, MIL-STD-217, or MIL-HDBK-217E, a previous revision. The most recent revision of MIL-HDBK-217 is Revision F Notice 2, which was released in February of 1995.

[12] The parts count method is a technique for developing an estimate or prediction of the average life, the mean time between failures (MTBF), of an assembly. It is a prediction process whereby a numerical estimate is made of the ability, with respect to failure, of a design to perform its intended function. Once the failure rate is determined, MTBF is easily calculated as the inverse of the failure rate, as follows: $\text{MTBF} = 1/(\text{FR}_1 + \text{FR}_2 + \text{FR}_3 + \dots \text{FR}_n)$, where FR is the failure rate of each component of the system up to n, all components.

In general, the parts count method will usually result in a more conservative estimate (i.e. higher failure rate) of system reliability than the parts stress method.

Even though this handbook is no longer being kept up to date by the US military, it remains the most widely used approach by both commercial and military analysts. Other commonly used electronic reliability prediction approaches include Bellcore, RDF 2000, PRISM, Physics of Failure and the IEEE Gold Book (see Appendix A for more information).

10.6.4 Applying probabilities to mechanical failures

The prediction of failure probabilities for structural (e.g. wing spars) and mechanical elements (e.g. hydraulic pipes) cannot be based on MTBF. When predicting the integrity of mechanical parts, the following main factors need to be considered:

- Static strength: static integrity is ensured through the application of safety factors (e.g. proof and ultimate load factors), which ensure that the systems are designed to withstand higher forces than ever anticipated during operational service. Acceptable safety factors are usually based on service experience and are often stipulated in the regulations.
- Fatigue strength: the fatigue life of a component is dependent (Lloyd and Tye, 1995 p. 128) on:
  - the spectrum of applied loads
  - the internal stresses resulting from those applied loads
  - the S-N (stress vs. cycles) curve for the particular material
  - the scatter of fatigue life about the mean
  - the condition (i.e. manufactured or maintained) of the component and the crack growth rate.
- Corrosion prevention: this is extremely hard to predict and reliance is generally placed on good design principles (e.g. keeping dissimilar metals apart, 'wet assembly', surface protection, etc.), service experience and frequent inspections.
- Redundancy: experience has shown that no structure is immune to failure. Hence the increasing use of redundancy in the form of duplicated systems and multiple load paths. For more information, see the fail-safe principles discussed in Chapter 7.
- Quality: the unique characteristics of each component and their variety and assemblies can cause large deviations in reliability.

It can be seen that the basis for establishing failure probability of mechanical systems presents special challenges in terms of reliability prediction. However, we still need to be able to demonstrate that failure probabilities have been reduced to acceptable levels, and the definitions of these levels need to be consistent with our safety criteria. So, systematically:

- assess by the above factors. There are three basic approaches for predicting the reliability of mechanical systems (see also Appendix A).
  - NPRD-95 – *The Non-electronic Parts Reliability Data* (NPRD-95) databook is a widely used databook published by the Reliability Analysis Center that provides a compendium of historical field failure rate data on a wide array of mechanical assemblies.

  - NSWC-94/L07 – *Handbook of Reliability Prediction Procedures for Mechanical Equipment.* This handbook presents a unique approach for prediction of mechanical component reliability by presenting failure rate models for fundamental classes of mechanical components.
  - Weibull analysis: if field failure data has been collected for a mechanical component, Weibull analysis can be used to determine the best-fit distribution for these failure data points. This information can then be used to estimate the parameters of the failure distribution and determine component reliability.
- assess the application of preventive maintenance techniques (e.g. inspections and replacement of vulnerable parts at specifically prescribed intervals),

only then the designer will be able to substantiate that, for instance, the probability of failure is anticipated as '*unlikely to occur to each aeroplane during its entire life but which may occur several times when considering the total operational life of a number of aeroplanes of this type*', which fall within the 'remote' category (see Table B.3).

10.7 Discussion

The International Civil Aviation Organisation's (ICAO) *Airworthiness Manual* (Appendix H to Chapter 4, page IIA-4h-I) states the following:

> Critical combinations of failures should be investigated and may be accepted on the basis of assessed numerical probability values where these values can be substantiated, and a suitable analysis technique[13] has been employed. When the failure of a device can remain undetected in normal operation, the frequency with which the device is checked will directly influence the probability that such a failure is present on any particular occasion.[14]

For purposes of aircraft design and safety assessment, no extensive knowledge of statistics is needed. Properly used, simple probability methods provide a useful tool to aid the processes of design. But though the rules are simple, they should be well understood if pitfalls are to be avoided. It does not help that many regulations (and often within the same document) contain numerous probability terms which are undefined and/or used in dissimilar ways.

Quantitative analytical approaches may be used to prove compliance against regulatory standards (e.g. such as FAR/JAR25.1309). However, in accordance with AMJ25.1309 para 4(b) these analytical tools are intended to supplement, not replace, engineering and operational judgement.

Throughout the product life cycle, MTBF data will require validation and possible re-baselining, particularly if predictive methods were used. This is necessary because predicted MTBF data would have been used to determine initial design redundancies, verify requirements and architecture, and justify the accomplishment of safety objectives. Should the observed in-service MTBF be less than the predicted MTBF, the aircraft

[13] See Annex A for a range of suitable techniques.

[14] See section 10.5.3 for more on checking for passive failure conditions.

system may not possess the inherent safety levels expressed in the safety assessment/ safety case and will therefore either require re-design or acceptance of residual risk. Typically, validation of predicted MTBF data can occur only when the original design has stabilised and is sufficiently robust. For aircraft this is normally 4–7 years after introduction into service.

To use quantitative reliability prediction methods wisely, one should be aware of their limitations. Like all engineering models, the failure rate models are approximations to reality. The failure rate models are based on the best field data that could be obtained for a wide variety of parts and systems; this data is then analysed and massaged, with many simplifying assumptions thrown in, to create usable models. Then, when the model is used, more assumptions are made for the design parameters entered, such as stress and temperature.

It is generally agreed that these predictions can be very good when used for relative comparisons, such as comparing design alternatives, or comparing products. However, a reliability prediction number for a product should not be treated as an absolute prediction of its field failure rate. Do not make erroneous assumptions on the robustness of a system rather than on dependable engineering data and rigorous testing. Do not confuse luck with reliability. Note also that reliability predictions do not account for substandard quality control for purchased parts, bad workmanship, poor product level quality control, overstressed field operation, etc.

10.8 Further reading

http://en.wikipedia.org/wiki/Probability

Tye, W. *Probability Methods for Aircraft System Safety Assessment,* Oct. 2001.

Lloyd, E. and Tye, W., *Systematic Safety – Safety Assessment of Aircraft Systems,* Errington Print, 1995.

AMC25.1309 and AC25.1309.

11 Minimum equipment lists

Do not make erroneous assumptions on the robustness of a system rather than on dependable engineering data and rigorous testing. Do not confuse luck with reliability.

Al DeCastro (2004 Hercules Operators' Conference)

11.1 Introduction

For economic and/or operational requirements an operator may require some leeway to enable flights to proceed with certain items of equipment or functions inoperative because:

- systems and associated equipment suffer faults/failures, which will require maintenance time and effort to rectify
- some faults will be difficult to rectify before a scheduled flight. Others can only be rectified pending the incorporation of modifications
- sometimes the aircraft needs to be recovered to its main base where repairs can more readily be made.

However, at certification, the aircraft was designed to achieve a certain level of safety. When any one system, instrument or equipment becomes inoperative, the designed level of safety is reduced. The question is, how can we be sure that under such conditions the aircraft will continue to be operated safely? The solution lies in using the system safety assessment to define 'minimum equipment lists' which will guide the operator as to allowable deficiencies, exposure times and appropriate limitations of use.

11.2 The concept of minimum equipment lists

The concept behind a minimum equipment list (MEL) is not new – aviation regulatory authorities have used it for many years (e.g. under the terminology 'Allowable Deficiencies, Go/No-go list, Dispatch Deviation Manual', etc.). Initially the concept was applied to allow operators to operate their aircraft with certain items of equipment or components inactive, provided that the Authority concerned was satisfied that an equivalent level of safety could be maintained either by (Christy, 1994):

- introducing appropriate operating limitations
- transferring the function to another operating component or
- referring to other instruments or components providing the required information.

On early-generation aircraft the systems employed were far less complex. Without recourse to extensive analysis, sound operational judgement was acceptable to decide which items of equipment or functions could be allowed to be inoperative at the time of dispatch. However, increased system complexity[1] requires a more auditable approach to evaluate the remaining integrity in the aircraft system. If aircraft are to be allowed to operate with equipment or functions inoperative, it would seem logical for such allowable deviations to take account of the safety assessment. AMC25.1309 (to CS25) advises that:

> A list may be developed of equipment and functions which need not be operative for flight, based on stated compensating precautions that should be taken, e.g., operational or time limitations, flight crew procedures, or ground crew checks. The documents used to show compliance with CS 25.1309, together with any other relevant information, should be considered in the development of this list, which then becomes the basis for a Master Minimum Equipment List (MMEL). Experienced engineering and operational judgement should be applied during the development of the MMEL.

The MMEL and MEL are alleviating documents:

- The MMEL is a master list appropriate to an aircraft type which determines those instruments, items of equipment or functions that, while maintaining the level of safety intended by the regulations, may temporarily be inoperative (refer to JAR-MMEL/MEL, 2000). The level of safety may be maintained due to:
  – the inherent redundancy of the design and/or
  – specified operational and maintenance procedures
  – specified conditions and limitations.[2]
- Depending on in-service experience, operational conditions[3] and maintenance procedures the aircraft operator may wish to amend the MMEL by producing a minimum equipment list (MEL). This is allowed by the authorities on the condition that the MEL remains within the limitations of the MMEL (i.e. the MEL must not be less restrictive than the MMEL for the particular aircraft type.[4]

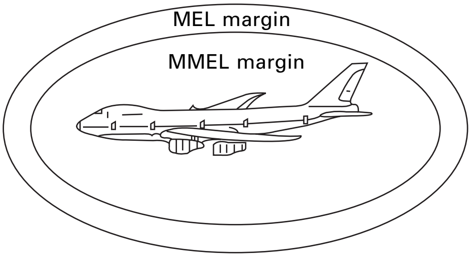
  The MEL is (TGL 26, 2004) a joint operations and maintenance document prepared by an operator to:
  – identify the minimum equipment and conditions for an aircraft to maintain the Certificate of Airworthiness in force and to meet the operating rules for the type of operation
  – define operational procedures necessary to maintain an acceptable level of safety and to deal with inoperative equipment
  – define maintenance procedures necessary to maintain an acceptable level of safety and procedures necessary to secure any inoperative equipment.

[1] A system is complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods (AMC to CS25.1309).

[2] For example, limitations on weather conditions, length of flight, speed, altitude, etc.

[3] Kinds of operation which may require specific MEL dispensation include crew training, positioning flights, demonstration flights, etc. (JAR-MMEL/MEL.055).

[4] Refer, *inter alia*, CAP 549 para. 4.1, JAR-OPS1.030 and JAR-OPS3.030.



11.1 Aircraft margins of safety (adapted from UK CAA Presentation on Continued Airworthiness (2003)).

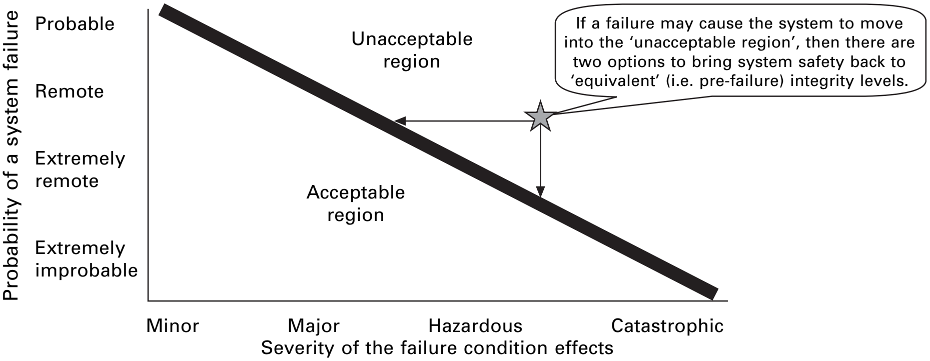
This relationship between the MEL and the MMEL is illustrated in Fig. 11.1 All items related to airworthiness of the aircraft and not included in the list are automatically required for flight. Non-safety-related equipment (such as galley equipment, passenger and convenience systems) need not be listed in the MEL and MMEL.

11.3 Generic approach

The implications of the MEL requirements are that:

- The safety assessment should highlight the level of criticality of the system and its function in respect of hazards which might arise in the event of a failure.
- Items may be permitted to be inoperative providing an equivalent level of safety is maintained by other reliable means (tailored from Christie (1994)):
  - There may be elements of redundancy which – although required for a safety measure – could be permitted to be inoperative for a short period (i.e. restricted flight time) without significantly affecting the required safety objectives.
  - In some instances it may be possible to substitute redundancy with a maintenance check.
  - In some instances it may be possible to reduce the severity of an adverse effect by restricting the aircraft's capability (e.g. limit despatch to VMC conditions).

So, if we consider Fig. 11.2 (refer Ch. 5), we need to ensure that the safety targets remain accomplished.



11.2 Inverse relationship between the consequence and the frequency of a system failure.

Example 1

Suppose we have a duplicated system with a single system failure probability of failure of 3.16×10^{-4} per hour. Suppose further that system failure could have hazardous consequences, so the safety objective is 10^{-7} per hour. How long may the flight continue after the first system fails?
Answer: The probability of a double failure is: $P_{double} = P \times P = p^2 T^2$. Now, we need to ensure that $p \leq 10^{-7}$, so $P_{double} \leq 10^{-7}$ T (because P = pT).

Hence:

$$p^2 T^2 \leq 10^{-7}T$$

$$(3.16 \times 10^{-4})^2 T^2 \leq 10^{-7}T$$

$$T \leq 1$$

So the aircraft would need to be diverted to an airfield less than one flying hour away after the first system fails.

In practice, circumstances are not as clear-cut as have been described above. Nevertheless, the general principles apply and, somehow, the manufacturer and authority must be reasonably confident that these principles have been conscientiously applied when allowing an item of equipment or a function to be temporarily inoperative.

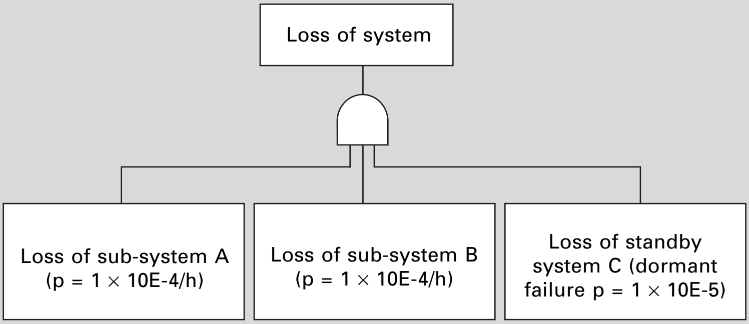
11.4 Process

The following guidelines (tailored from Christie (1994)) are offered when considering the MEL/MMEL:

- Establish the function or functions which make a system and its associated equipment ‘safety critical’ or ‘safety significant’ (i.e. those which lead to catastrophic and hazardous failure conditions).[5] If the modification does not influence any of these functions, then no MEL/MMEL changes may be required.
- Consider the effects of the occurrence of other probable events, not necessarily systems initiated (e.g. environmental conditions, and time of day, daylight, darkness, etc.).
- Take account of national operating regulations which may require certain equipment or functions to be available at all times.
- Check whether, in redundant systems, the non-availability of an equipment or function will appreciably increase the likelihood of a hazardous event, or whether there is sufficient built-in redundancy for such non-availability to have little or no adverse affect.
- Consider whether increased maintenance inspections or pre-flight checks would provide adequate compensation (see Example 2).
- Consider the practicality of temporary additions or changes to the flight crew procedures and assess the increase in workload thereof.

[5] Refer JAR25.1309(b)(1)&(2).

Example 2


Loss of system
Loss of sub-system A (p = 1 × 10E-4/h)
Loss of sub-system B (p = 1 × 10E-4/h)
Loss of standby system C (dormant failure p = 1 × 10E-5)

Probability of total loss of function per flight hour:

$$p = p_A \times p_B \times p_c$$
$$= (1 \times 10E\text{-}4) \times (1 \times 10E\text{-}4) \times (1 \times 10E\text{-}5)T$$

If the maintenance check is every 10,000 h, then: p = 1 × 10E-9.

Question 1: assuming our safety target is p = 1 × 10E-9. Can we dispatch with either A or B inoperative?

Answer 1: if flight is one hour long, and C was checked to be operable prior to each flight, the probability of C failing during the next hour of flight is $p_c = (1 \times 10E\text{-}5) \times 1$

then: p = 1 × 10E-9, so equivalent level of safety.

Question 2: is it acceptable to dispatch with C inoperative?

Answer 2: p = (1 × 10E-4) × (1 × 10E-4) = 1 × 10E-8, which does not meet the safety target.

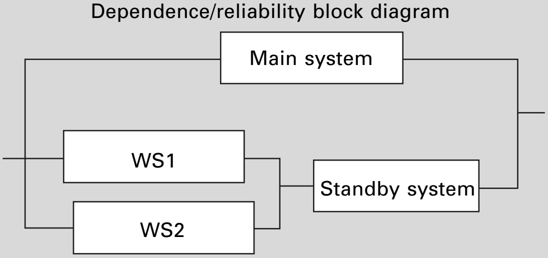
Example 3
(tailored from Lloyd and Tye (1995) and Christie (1994))

Consider again the simple system that we assessed in section 10.4 which comprises a main system (main), a standby system (standby) and a duplicated warning system (WS).

The main system is in continuous operation in flight. If it fails in flight, this is not sufficiently evident to the pilot unless the warning system operates.

On seeing the warning, the instructions are to check the functioning of the main system and if it has failed, to select the standby system.

Example 3 continued



Let us assume the following:

- that all the systems are capable of being checked for operability before each flight. Hence dormant failures are confined to those which occur during the particular flight.
- t = 2 h (average flight)
- $\lambda_M = 1 \times 10^{-4}$ per hour (10^{-4})
- $\lambda_{SA} = 1 \times 10^{-3}$ per hour (active)
- $\lambda_{SI} = 1 \ \times 10^{-5}$ per hour (inactive)
- $\lambda_W = 1 \times 10^{-4}$ per hour.
- No defects at start of flight

Remember: $P = 1 - R$

$= 1 - e^{pt}$

$\approx pt$ (if $pt \leq 0.01$)

The following observations can be made:

- If main system operates throughout there is no risk. Only necessary to consider main system failures in combination with other failures.
- Two conditions need to be considered:

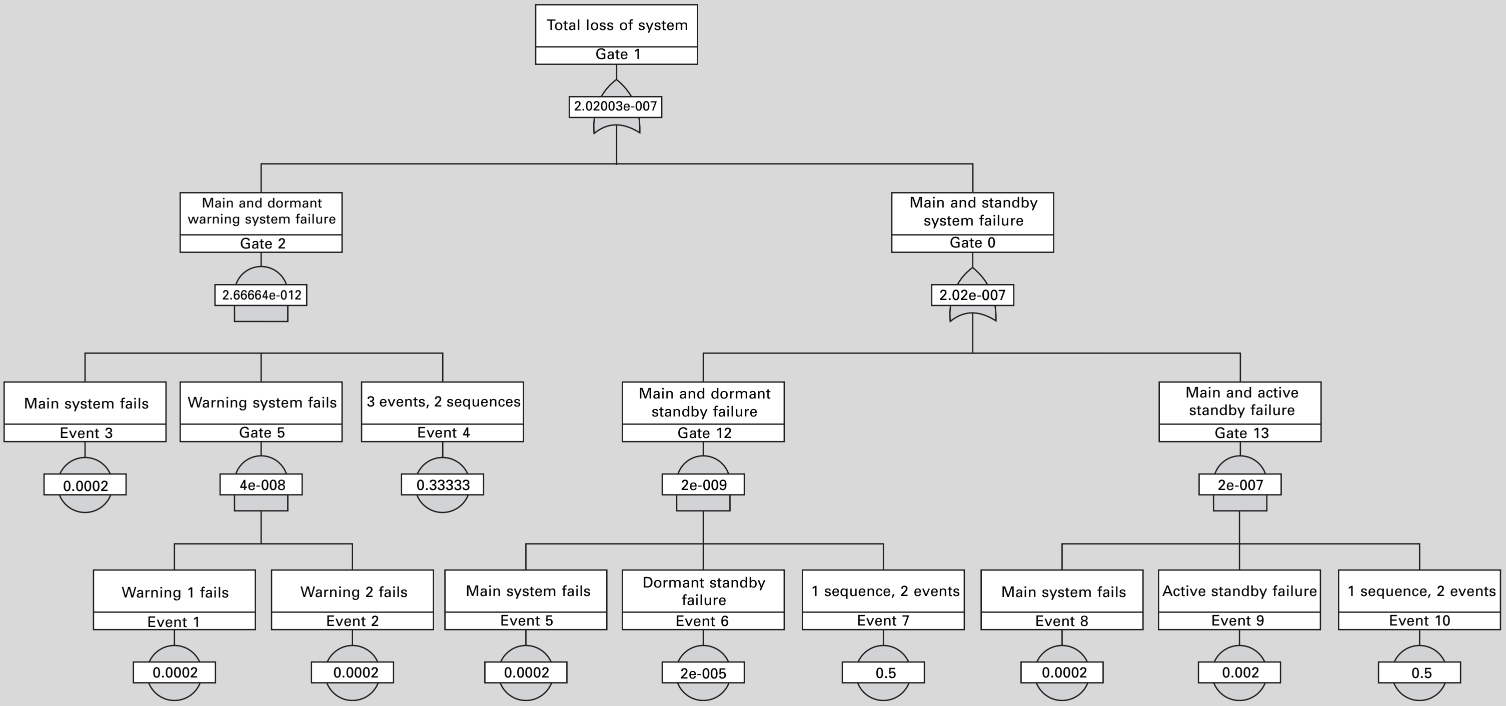
  Case A: loss of main with dormant failure of warning.

  1. Failure of WS1, followed by failure of WS2, followed by failure of the main system.
  2. Failure of WS2, followed by failure of WS1, followed by failure of the main system.

  Case B: loss of main with loss of standby.

  1. Dormant failure of S/B before main system failure.
  2. Active failure of S/B after main system failure.

Example 3 continued



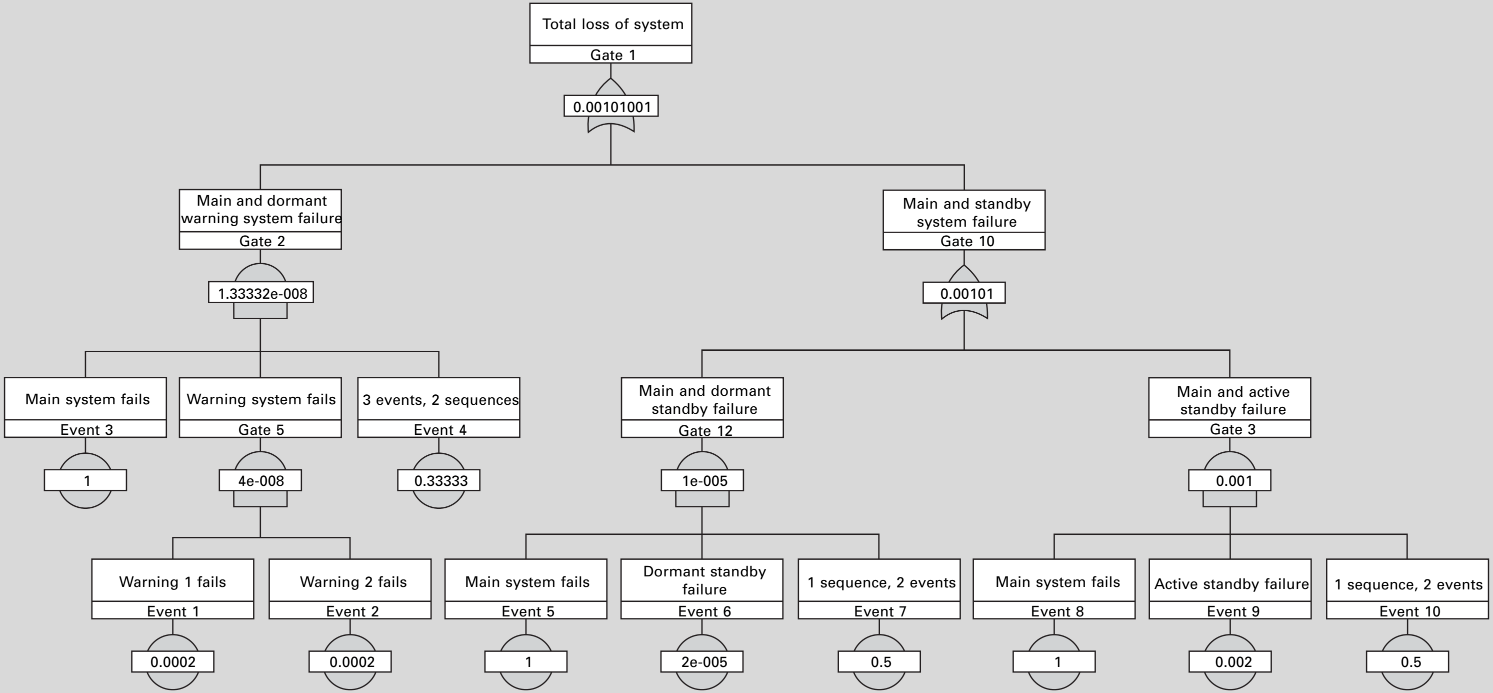
Example 3 continued

Discussion:

Above we saw that the total risk of failure during a 2 h flight = 2.02×10^{-7}.

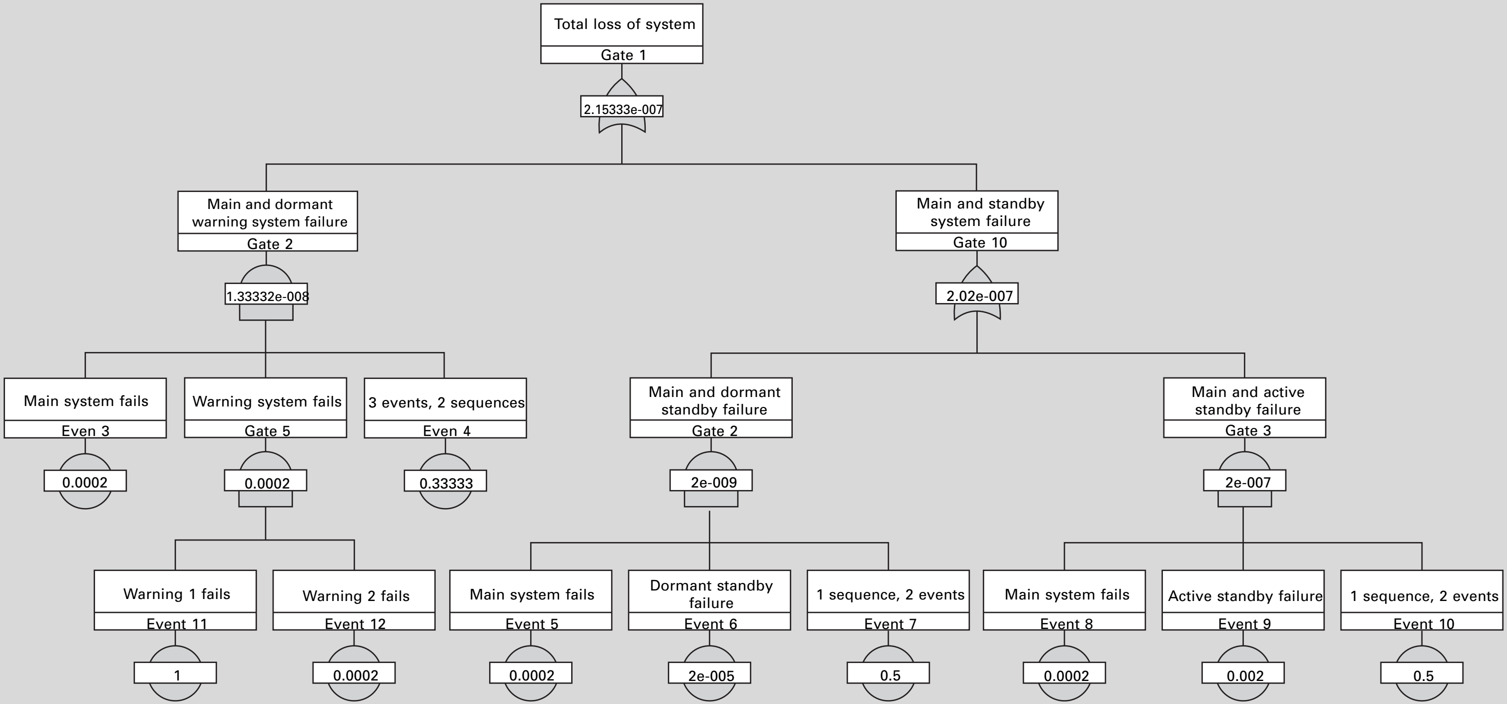
If one element of the system is deficient, would it be safe to dispatch the flight?

- Consider main inoperative and using standby only:



Example 3 continued

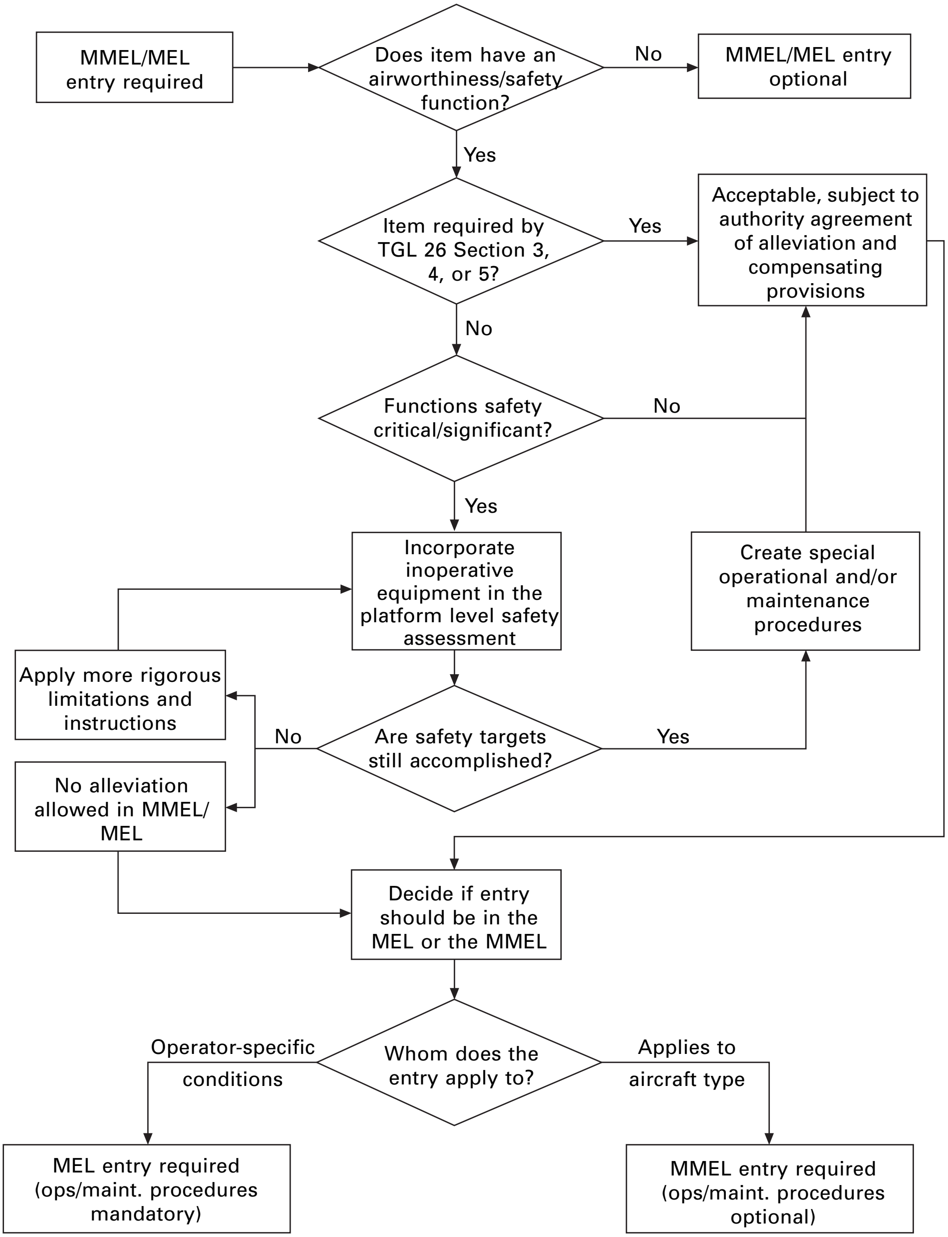
- Consider WS1 inoperative:



So, main failure would not be an allowable deficiency, but starting a flight with only one WS operative would only increase the risk by 10%.

11.5 Equipment included in an MMEL/MEL

Most aircraft are designed and certified with a significant amount of equipment redundancy, such that the airworthiness requirements are satisfied by a substantial margin. In addition, aircraft are generally fitted with equipment that is not required for safe operation under all operating conditions, e.g., instrument lighting in day


MMEL/MEL entry required
Does item have an airworthiness/safety function?
No
MMEL/MEL entry optional
Yes
Item required by TGL 26 Section 3, 4, or 5?
Yes
Acceptable, subject to authority agreement of alleviation and compensating provisions
No
Functions safety critical/significant?
No
Yes
Incorporate inoperative equipment in the platform level safety assessment
Create special operational and/or maintenance procedures
Apply more rigorous limitations and instructions
No
Are safety targets still accomplished?
Yes
No alleviation allowed in MMEL/MEL
Decide if entry should be in the MEL or the MMEL
Operator-specific conditions
Whom does the entry apply to?
Applies to aircraft type
MEL entry required (ops/maint. procedures mandatory)
MMEL entry required (ops/maint. procedures optional)

11.3 MEL/MMEL decision tree (based on JAR-MMEL/MEL and JAA TGM 26).

VMC. Other equipment, such as entertainment systems or galley equipment, may be installed for passenger convenience. If this non-safety related equipment does not affect the airworthiness or operation of the aircraft when inoperative, it need not be listed in the MMEL/MEL or be given a rectification interval. However, if the non-safety-related equipment has another function related to safety (such as use of the entertainment system for passenger briefings) then this item must be included in the MMEL/MEL with an appropriate rectification interval. Put more simply, the MMEL/MEL lists required systems.

The JAA decision process for inclusion of items in the MEL or MMEL is specified in JAR-MMEL/MEL and JAA TGM26, which was used to compile the process flowchart in Fig. 11.3.

11.6 Discussion

The MMEL and associated MEL are alleviating documents. Their purpose is not to encourage the operation of aircraft with inoperative equipment. It is undesirable for aircraft to be dispatched with inoperative equipment and such operations are permitted only as a result of careful analysis of each item to ensure that the acceptable level of safety is maintained. Fundamental considerations include:

- All items related to the airworthiness of the aircraft and not included in the MMEL are automatically required to be operative prior to flight.
- An operator or pilot retains the option to refuse any alleviation, and may choose not to dispatch with any particular MEL item inoperative.
- The continued operation of an aircraft under MEL/MMEL conditions should be minimised.
- When considering redundancy techniques, system designers should provide for ‘extra redundancy’ in some systems to enable the aircraft to continue safe flight and landing with adequate safety margins (Lloyd and Tye, 1995 p. 147).
- Where items are included in an existing MMEL or MEL, account should be taken of them in the safety assessment (Lloyd and Tye, 1995, p. 147).

12

The safety management system

Captain Lavendar of the Hussars, a balloon observer, unfortunately allowed the spike of his full-dress helmet to impinge against the envelope of his balloon. There was a violent explosion and the balloon carried out a series of fantastic and uncontrollable manoeuvres, whilst rapidly emptying itself of gas. The pilot was thrown clear and escaped injury as he was lucky enough to land on his helmet.

Remarks: This pilot was flying in full-dress uniform because he was the Officer of the Day. In consequence it has been recommended that pilots will not fly during periods of duty as Officer of the Day. Captain Lavendar has subsequently requested an exchange posting to the Patroville Alps, a well known mule unit of the Basques.

No. 2 Brief from Daedalian Foundation Newsletter (Dec. 1917)

12.1 Introduction

12.1.1 Background

A number of factors and inherent dangers exist that may influence the achievement of an acceptable level of system safety.

- Aircraft are very complex and highly integrated with a multitude of critical systems involving interfaces between hardware, software and operators. These configurations and interfaces are not stagnant and continue to evolve, introducing new situations and conditions.
- Aircraft, especially military, are required to operate in very demanding environments. Actual testing under realistic environmental conditions is not possible in all cases.
- Weight restrictions require aircraft designs to be optimised with minimum margins of safety.
- Redundancy is often considered an unaffordable luxury, especially for military aircraft types.
- Design restrictions often place limitations on safety measures.
- During service life, the operational usage might change beyond that assumed in the original design and definition of the maintenance schedule.
- Despite testing, unexpected hazardous conditions (such as flutter and stores separation problems) may occur.
- Cost-cutting measures may be implemented, e.g., extended maintenance intervals, less training, etc.
- Other imperatives, such as mission accomplishment, available financial resources

and schedule constraints may at times conflict with the technical airworthiness rules and standards.

As a result personnel associated with the design, manufacture, maintenance and material support of aeronautical products may be exposed to an evolving, ever-changing, level of risk.

Until quite recently only the people directly involved would have been held to blame for an accident. Now it is recognised that safety is everybody's concern. However, whilst individuals are responsible for their own actions, only managers have the authority and resources to correct the attitude and organisational deficiencies which commonly cause accidents. An accident is an indication of a failure on the part of management (David, 2002). What is required is an ordered approach to manage safety throughout the system's life cycle. This ordered approach is facilitated by the safety management system (SMS). This chapter provides some guidance on the philosophy and approach to a safety management system.

12.1.2 Regulatory requirements

Various regulators require a safety management system, for instance:

- JAR OPS 1 (commercial air transport operation) and JAR OPS 3 (rotorcraft operation) require that 'an operator shall establish an accident prevention and flight safety programme to achieve and maintain risk awareness by all personnel involved with operations'.
- The JAR OPS statement is derived from the ICAO recommended practice (Annex 5 part 1) for operators to have such a programme in place. ICAO document 9422 (*Accident Prevention Manual*) gives appropriate guidance material and describes safety management systems.
- The FAA's core approach to safety management is the air transport oversight system (ATOS). A key goal of ATOS is for the operator to implement its own system safety culture, including its own safety audits and self-correction programmes.
- The UK Health and Safety Executive requires all organisations to outline the overall philosophy, chain of command, systems and procedures in relation to health and safety management.

12.2 What is a safety management system?

A company's safety management system (SMS) defines how the company intends to manage safety as an integral part of its business management activities. Profit (1999, p. 1) states that an SMS is no more than a systematic and explicit approach to managing the risk of an accident (just as a quality management system is a systematic and explicit approach to improving a product or service). The prime purpose of a SMS is to improve the level of safety by enabling: the effective identification of hazards; the systematic introduction of control measures; an audit trail for all of the safety related decisions. This involves planning, organising, monitoring, evaluating and recording the arrangements for the management of safety.

The actual content of an SMS will be dependent upon each company's management system but, fundamentally, an SMS has three basic characteristics:

1. A comprehensive corporate approach to managing safety, for instance:
   - leadership and commitment to safety
   - active involvement of top management
   - clarity of policy objectives and safety improvement
   - enhanced safety standards (relative to regulatory minima)
   - development and maintenance of a learning safety culture.
2. An effective organisation for delivering safety, for instance:
   - committee structure for overseeing safety management
   - management review mechanisms
   - clarity of line management responsibilities
   - coherent cascade of accountabilities for safety
   - role of accountable manager (CEO) and SMS custodians
   - change management process in place
   - effective competency and training requirements.
3. Robust systems for assuring safety, for instance:
   - ensuring a pro-active approach to safety (e.g. through system safety assessments, safety cases, change assessments, etc.)
   - maximising use of available information and a strong corporate knowledgebase for safety data exchange, training and awareness
   - structured monitoring of SMS compliance (e.g. safety/quality audits, process and practice monitoring, incident investigation and follow-up to maintain or improve safety).

12.3 Safety culture

A safety culture is (Kuo, 1995) 'The belief or philosophy on safety matters held by organisations and individuals, which is demonstrated in practice through their attitudes, actions and behaviour. An organisation's safety culture becomes evident in 'the way we do things around here when no-one is looking' (Matthew S., head of the Flight Safety Foundation). A safety culture is the attitude that exists when: everyone recognises and accepts their responsibilities for safety; the organisation 'thinks safety' as a matter of course; and management realises that the safety achievement of a system is not static and it may tend to degrade over time (e.g. as people become complacent or less vigilant, or when systems start to age).

Example: Challenger Shuttle

'Shuttle program management made erroneous assumptions about the robustness of a system based on prior success rather than on dependable engineering data and rigorous testing'.

CAIB Report, Aug 2003

A safety culture is significantly influenced by the following philosophical extremes (refer, *inter alia*, Kuo (1997a, Ch. 8)):

- Blaming philosophy. When a failure/hazard occurs, someone must be at fault and should be punished. Although the guilty are punished and the immediate cause is found, this approach leads to:
  - a defensive attitude (due to a culture of blame and defensiveness)
  - the systematic causes behind the incident (e.g. management failures, commercial pressures, insufficient training, unsafe systems/processes, etc.) being often ignored.

  Reports of equipment failures, design faults or procedures which might cause a hazard, must be encouraged without threat of disciplinary action wherever possible. An effective safety culture requires an atmosphere in which individuals are not unduly punished or blamed for their mistakes – a 'blame-free' environment. This is an ideal which is difficult to achieve in practice; when things really do go wrong, people's reaction is often to protect themselves by pointing the finger of blame at others.
- Collaborative philosophy. Best solutions are usually derived via close collaboration between the prescribing authorities, users, suppliers, and other stakeholders. This approach encourages a shared responsibility and a willingness to improve safety. A collaborative safety culture is the most desired foundation for an effective SMS. It recognises that there is no panacea for safety; that safety requires time to develop, and that factors keep changing (e.g. systems age, competence levels fluctuate, etc.).

Even an organisation that strives to achieve a blame-free environment is still subject to rules and legal regulation. A 'just' culture is one in which individuals are not free of blame if they are culpably negligent and where the organisation gives due regard to honesty (David, 2002).

Culture is the sense of values, beliefs, and norms which is being practised in the business. Management creates culture and it is their responsibility to influence it. Management has great leverage in affecting safety within an organisation; through its attitudes and actions, management influences the attitudes and actions of line managers, who in turn repeat it to their employees (be they inspectors, quality control personnel, designers, operational personnel, etc.).

A safety assessment must not be viewed as a one-off exercise; people should be continuously trying to make things safer. Errors and mistakes are inevitable and safety can only be improved if the organisation can learn from its mistakes. The SMS thus needs to enforce a culture of communication and continuous improvement. There are several ways achieving this, for example:

- incident reporting, investigation and feedback
- safety reviews and audits
- safety working groups and safety panels
- suggestion schemes which cover safety
- incident reporting (including some sort of anonymous reporting scheme).

12.4 Developing a safety management system

12.4.1 Introduction

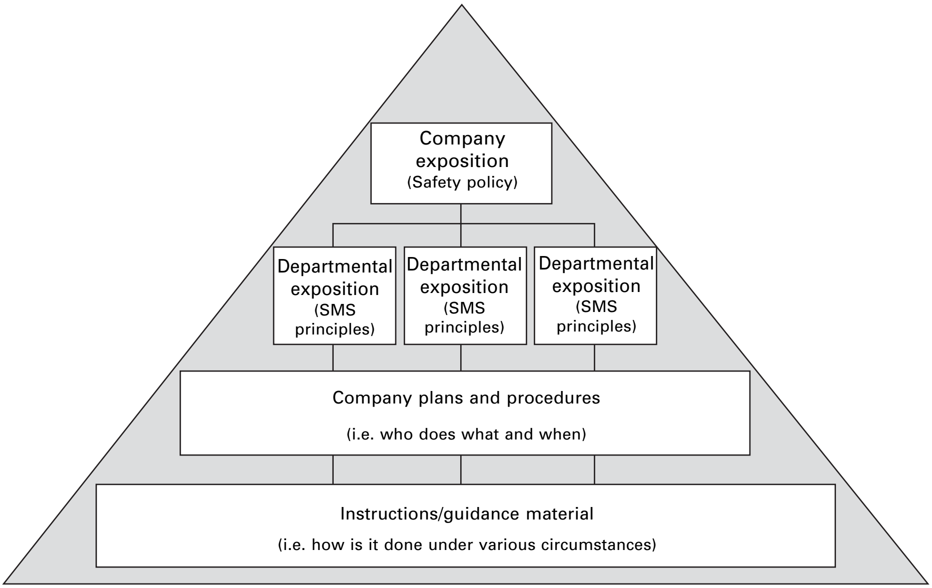
Safety management is that part of the overall management function which determines and implements an organisation's safety policy. It is the means by which the management principle is translated into front-line safety performance improvement activities. The implementation of a safety management system should thus follow a top-down programme which ensures that:

- safety policies are defined. These statements should define the organisation's fundamental approach to the management of safety and should commit the organisation at the highest level to the fulfilment of its stated safety policy.
- from the policy statements, the organisation should define its safety management principles, which specify the safety objectives with which the organisation intends to comply.
- having defined the policy statement and principles, the organisation should produce plans and procedures and define responsibilities which will ensure that the safety objectives are accomplished. Note that there is an ever-present danger of creating formal 'policies' or procedures to respond to each regulator or to each new hazard (Jenkins (1999), p4). At a strategic level, the safety aspiration and principles (policies) are common to all processes and hazards, whilst at the detailed level the implementation is specific and tailored to the process and hazard.[1] Organisation should take a pragmatic approach, building on existing procedures and practices (particularly quality management).
- procedures should be supported by advisory/ guidance material, working instructions, checklists, templates, etc. The advantage of keeping these separate from the procedures is that they should be easily tailored and improved upon as
  - part of the development of corporate memory
  - encouraging a safety culture
  - striving for a 'best-practice' approach.

A fully-fledged SMS is a formalised, company-wide system. It should be traceable from the aim of the policies statements through to the principles, individual responsibilities and the detailed procedures and instructions. This process is illustrated in Fig. 12.1. Where safety sensitive functions are outsourced (e.g. maintenance), contractual arrangements should identify the need for an equivalent SMS in the supplier's organisation.[2]

[1] This argument may seem obvious, or even trivial, but it is critically important when an organisation has many types of operation. If a manager has a good grasp of what the fundamental principles are, then it is no longer necessary to develop too many different processes for delivering that principle in order to achieve good safety performance in different activities.

[2] This raises an important point: British Airways found (Passmore 1999) that incidents would occur which clearly highlighted the lack of auditing of the supplier and/or no risk assessment of the change from in-house to sub-contract supply. On these occasions when a risk assessment was done then it was often informal and not properly recorded'. The same principle holds true when suppliers are changed (often because of a lower price) or when work is moved from one department to another.


Company exposition (Safety policy)
Departmental exposition (SMS principles)
Departmental exposition (SMS principles)
Departmental exposition (SMS principles)
Company plans and procedures
(i.e. who does what and when)
Instructions/guidance material
(i.e. how is it done under various circumstances)

12.1 SMS documentation pyramid.

12.4.2 Safety management policy statements

The policy statements should define the fundamental approach to be adopted for managing safety and the organisation's commitment to safety. The following bulleted items (tailored from SRG (1999)) provide typical safety policy topics:

- **Safety objective.** Declare a top-level commitment to a business objective for safety that minimises its contribution to accident risk as low as reasonably practicable.

  Rationale. This should be the key policy statement defining what the organisation is striving to achieve through its safety management system.
- **Safety management.** Make a commitment to the adoption of an explicit, proactive approach to systematic safety management.

  Rationale. An intuitive or *ad hoc* approach to safety is not acceptable.
- **Safety responsibility.** Make a policy statement that confirms that everyone has an individual responsibility for the safety of their own actions and that managers are accountable for the safety performance of the activities, products, services, etc., in their charge. Flow down to departmental expositions who is ultimately accountable for safety and how that accountability is delegated.

  Rationale The safety management system depends upon individuals understanding and accepting their delegated responsibility within the organisation. Accountability for safety belongs to all levels of management and the attainment of satisfactory safety performance requires the commitment and participation of all members of the organisation. Everybody within an organisation should be aware of the consequences of mistakes and strive to avoid them. Management should foster this basic motivation within members of an organisation so that everybody accepts their responsibility for safety.

- **Safety priority.** Commit the organisation to ensuring that safety is given the highest priority when considering commercial, operational, environmental or social pressures.

  Rationale: The safety management system should clearly address and resist misguided business pressures. Conversely, the safety management system should ensure that safety is not used to support commercial, financial, environmental, etc., decisions inappropriately, which have little real safety significance. If the term 'safety' is abused in this way the safety management system cannot be focused on controlling the real risks.
- **Safety standards and compliance.** Commit the organisation to complying with all appropriate safety standards and requirements (see Chapter 3 for more information).

  Rationale. Compliance with safety standards and requirements can form part of a robust safety argument and facilitate the safety assessment process.
- **Externally supplied products and services.** Commit the organisation to ensuring that the safety assurance processes used by its external suppliers satisfy its own safety management standards and safety requirements.

  Rationale. A safety assessment requires input from all phases of a product or service development. For externally supplied products or services the external supplier must understand and comply with the organisation's safety and safety management system requirements.

12.4.3 Safety management principles

The following safety management principles (tailored from SRG (1999)) define the scope of a safety management system, provide a framework for the establishment of processes to identify safety shortcomings, and provide assurance that safety levels are being met or improved. These principles must be supported by referring to the applicable procedures that ensure their execution.

- **Safety criteria.** Whenever practicable, safety targets should be derived, maintained, and improved for all products and services (see Chapter 4, Chapter 5 and Appendix B for more information).

  Rationale. If the safety performance of a service or product is to be assessed and monitored it is necessary to define the safety objectives that need to be met.
- **System safety assessments.** All new/modified systems should be subjected to some sort of safety assessment (see Chapter 8 for more information).

  Rationale. The analysis process is conducted during development of the system to establish safety requirements. The safety assessment process is used to demonstrate that these requirements are met.
- **Safety case.** An organisation should assess all existing operations, and proposed changes/additions/replacements for their safety significance (see Chapter 9 for more information). For those areas where the probability of the accident occurring may be impacted, formal safety assessments should be conducted.

  Rationale. Engineering alone cannot guarantee safety. Systems evolve, as do their operational applications. Procedures and maintenance do affect safety. Frequent training can improve effectiveness.

- **Safety records.** An organisation should identify and record the safety requirements for a service or product, the results of the safely assessment process and evidence that the safety requirements have been met. These records need to be maintained throughout the life of the service or product.

  Rationale. The safety assessment documentation should provide the evidence to the organisation upon which it will base its decision whether it is safe to use the service, or product. Maintenance of these records throughout the life of the service or product provides ongoing assurance that it continues to meet its original safety requirements and that any remaining risks are adequately controlled.
- **Competency.** Each department in the organisation should ensure that staff remain adequately trained, competent and qualified for the job they are required to do.

  Rationale. Staff competence is fundamental to safety.

12.4.4 Safety management plans and procedures

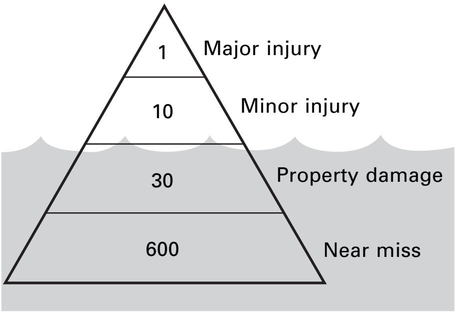
Safety management plans and procedures should specify the activities that need to be conducted in order to execute the SMS policy and principles. Typical latent failures in management include inadequate procedures, poor scheduling and allocation of resources, and neglect of recognised problems. Plans and procedures are needed which clearly stipulate life-cycle milestones as well as responsibility allocation. The following topics should typically be addressed by safety procedures and plans:

- **Life-cycle safety activities.** The procedures should stipulate the safety activities that typically need to be conducted during the various phases of the system's life. These procedures could be formulated around either (or both) the safety case approach (see Chapter 10) or the SSA approach (see Chapter 9).

  Rationale. Clearly defined activities and milestones (both during the development lifecycle as well as operational application) are essential requirements for a proactive approach to safety management.
- **Safety monitoring.** An organisation should have in place suitable monitoring arrangements so that unacceptable trends in service or product performance can be recognised and be subject to remedial action (SRG, 1999).

  Rationale. Service and product performance can deteriorate, or the environment within which they operate can change. Such changes need to be detected, assessed and managed.
- **Safety significant events.** Studies from a range of industries have shown that there is consistently a much greater number of less serious incidents than those which led to an injury (David, 2002). Often it was only a matter of chance that these near misses or non-injury accidents did not harm people. Incidents and accidents should be investigated immediately and any necessary corrective action taken.

  Rationale. Information on real accidents and incidents, whether or not they actually caused damage, provides the opportunity to learn about actual problems and to improve safety. Figure 12.2 illustrates the 'iceberg' of incident statistics,



12.2 The safety iceberg (David, 2002).

where the large bulk of learning opportunities lie below the surface of obvious accidents.

- **Safety audits.** Organisations should routinely carry out safety audits to identify opportunities for improvement, to provide management with assurance of the safety of activities and to confirm conformance with the safety management system (SRG 1999).

  Rationale. This should be a routine part of business activity. This is the proactive safety management mechanism by which any potential risks associated with an existing service or product can be identified and controlled.
- **Incident planning.** Procedures should be defined to deal with the unfortunate occurrence of incidents and accidents (see bow-tie analysis in Appendix A).

  Rationale. Recovery procedures will limit loss of life and resources. It will also ensure that the organisation knows what to do in the event of an accident investigation/board of inquiry.

12.4.5 Safety instructions/guidance

Safety instructions, templates, checklists, guidance material, databases, etc., must evolve within the organisation to facilitate business efficiency. These instructions and guidance should empower (not restrict) individuals to accomplish the following:

- **Safety improvement.** An organisation should have in place arrangements that actively encourage staff to identify system and process inefficiencies, and propose solutions.

  Rationale. This requires an effective means of communicating safety issues and the development of an internal safety culture that encourages every member of staff to focus on the achievement of safety, and to report errors and deficiencies without fear of punitive actions against them.
- **Lesson dissemination.** An organisation should ensure that lessons learnt from its safety assessments, hazard logs,[3] safety occurrence investigations, case histories,

[3] Effective lesson dissemination can be achieved through a variety of means. For example, establishing a risk register and keeping it active and updated with operational data provides a means for ensuring that everyone within the organisation is aware of the current risk situation and work that is ongoing to resolve specific risks.

experience from other organisations, etc., are distributed widely and actioned to minimise the probability of recurrence and to design more error-tolerant and effective systems.

Rationale. Few would argue that an effective and widespread learning process is essential to ensure that error management within safety-critical systems is continually informed and improved. Including the results of such lessons in training programmes, safety review bulletin, etc., will raise staff awareness levels.

These tools should provide a means to eliminate unnecessary work by establishing corporate memory, reducing programme risks and avoid repeating errors/risks. By ensuring salient lessons are learned throughout the company, the error-management process can be better informed throughout the product lifecycle.

12.5 Discussion

Safety management is concerned with having a consistent approach to potential causes of harm and targeting effort where it will have most benefit. The SMS provides the following:

- a comprehensive corporate approach to safety
- an effective organisation for delivering safety
- robust systems for assuring systematic safety.

To develop a SMS a company must:

- gain top management commitment and involvement
- ensure that safety policy makes the priority safety explicit
- initiate steps to build a learning safety culture in the company
- build the company's hazard register
- define the criteria to be used for risk assessment and hazard management
- document the safety case/assessments
- train the staff and management.

SMS has a significant part to play in improving safety performance in an organisation – especially if it involves everyone in the company from totally honest top management dedicated to its success, to the most diligent hangar sweepers. Moreover, the adoption of a formal SMS by operators and service providers makes the safety regulatory function considerably more effective.[4] It facilitates the safety monitoring and approval roles of the regulator and makes the task of assessing an organisation's corporate safety competence much easier (Profit, 1999, p. 10).

The SMS approach also reflects the general trend in safety regulation to evolve towards a performance-based approach, in other words, specifying what a desired outcome should be and not prescribing in detail how to do it. What a SMS does is to

[4] It is worth noting that the International Maritime Organization (IMO) mandated SMS for passenger shipping in 1998 and Lloyds of London will not insure vessels without SMS.

provide a framework for an organisation to take responsibility for their own activities, rather than rely purely on compliance with ever more detailed, prescriptive safety regulations. By moving beyond mere compliance with regulatory requirements and proactively using best practice, the risk of causing injury to people, damage to property or harm to the environment should be significantly reduced. Not only does this provide a management framework for controlling risks, but it also enables the regulator to focus resources on the areas of highest risk rather than merely inspecting compliance against predictive safety requirements.

12.6 Further reading

For more information on the SMS topic, see:
Profit, R. Keynote Address: *European Safety Regulation and Harmonisation*, Aviation Safety Management Conference, 20 May 1999, London, IBC UK Conferences Ltd, London.

CAP 712, *Safety Management Systems for Commercial Air Transport Operations*, UK CAA Safety Regulation Group, 2001, www.caa.co.uk (publications). http.//www.caa.co.uk/docs/33/CAP712.pdf

ICAO document 9422 (*Accident Prevention Manual*) gives appropriate guidance material and describes safety management systems.
http://www.healthandsafety.co.uk/safpofs.html

13
Concluding observations

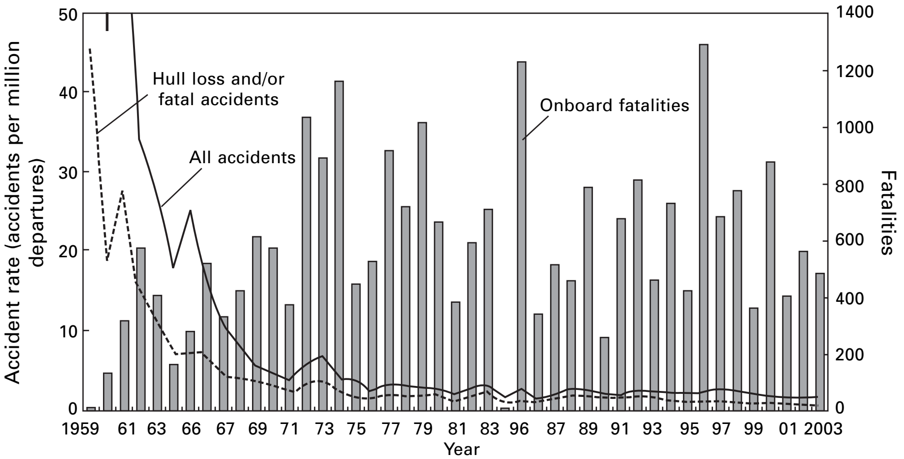
Accidents are not due to lack of knowledge, but failure to use the knowledge we have

Trevor Kletz

13.1 Aviation trends

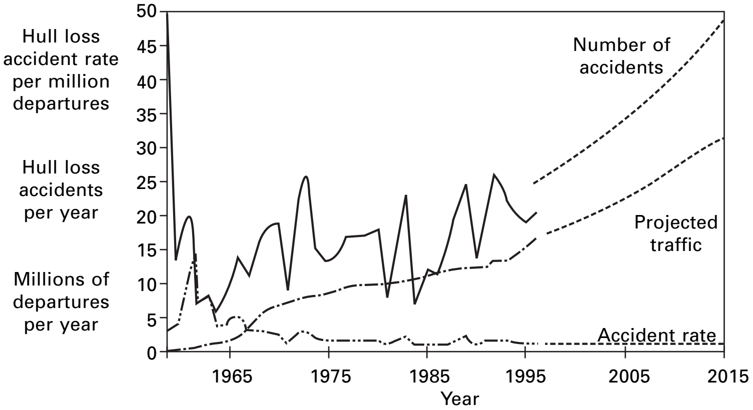
Aircraft flight has been transformed from an adventurous activity enjoyed by a select few to a stable mass-market service industry which is largely taken for granted ... until things go wrong. The industry is then dominated by public perception of risk and the social amplification thereof. Accidents resulting in hull loss[1] often result in fatalities and are almost always treated to extensive coverage in the national, if not world-wide, press.

As can be seen from Fig. 13.1, the accident rate has been essentially constant for at least 20 years. However, if the accident rate remains constant, and airline traffic grows at the projected rate, then the number of hull loss accidents worldwide would reach almost one per week by the year 2015. Figure 13.2 neatly illustrates this probable future trend in commercial aviation accidents.



13.1 Commercial jet accident rate and fatalities per year (*Boeing 2003 statistical summary*, May 2004, www.boeing.com/news/techissues).

[1] 'Hull loss' is used by the industry to describe an accident where the aircraft is damaged beyond economical repair.



13.2 Global commercial airline transport safety trends (with kind permission, Arbuckle *et al.,* 1998).

This is something that the public will not accept,[2] implying a limited growth scenario for airline traffic – unless something is done to reduce the hull loss or fatal accident rate. What is needed is a revised relationship between management and safety. The aircraft industry is set to become more complex, the skies more crowded, and the budgetary pressure will increase. A new impetus must be found in pro-safety activity if the high confidence of the public is to be maintained, let alone improved, through the impending doubling of traffic by 2020 and beyond. It will not be sufficient to increase the reliability of technical systems alone. It is well known that, after controlled flight into terrain (CFIT), fire (and the accompanying toxic fumes) is the most common cause of aircraft fatalities. Furthermore, the accident rate is a function of many factors, which include human performance, weather, design, operation, training, maintenance, and airspace system infrastructure.

Regulatory authorities, operators and maintainers need to enforce a proactive approach to safety, whereby the safety management system not only ensures that the intended level of safety remains intact, but also that trends are monitored and used to make improvements before an accident or incident occurs. Trends can be monitored via internal programmes such as FRACAS/DRACAS (see Appendix A) as well as via data-sharing programmes such as Flight Operations Quality Assurance (FOQA), Aviation Safety Action Partnerships (ASAP) and accident databases.

13.2 Safety assessments/safety cases

Initially there were some misgivings about moving to the more disciplined safety management approach. The need for safety management plans, safety cases, etc. all gave rise to concerns over the resources that would have to be deployed on such

[2] The National Civil Aviation Review Commission concluded in 1997 that it is evident that the frequency of fatal accidents cannot increase in line with the predicted growth in commercial air traffic.

planning, assessment and reporting activities whose value was difficult, initially, to appreciate.

Different projects use a variety of safety tools/techniques in numerous combinations. There is much guidance material and standards available on this subject (e.g. JSP318B, ARP4761, etc.). Often these are not agreed upon before contract closure and are used 'after the fact' to satisfy safety questions, and not as a useful tool to influence and optimise the design.

The real challenge is to recognise that safety management is not a bolt-on extra, but to arrange all activities within the context of a safety management system. For instance:

- The safety management plan needs to be prepared as part of the project's through-life management planning process (Dallimore, 2003). This plan should prevent safety assessment activities from becoming fragmented/disjointed thoughout the system's life cycle, i.e., from the specification stage through implementation, verification, operation, maintenance and decommissioning (Mauri, 2000). The SMP must co-ordinate and facilitate all safety activities 'from the cradle to the grave'.
- The safety assessment/case needs to evolve in a planned and structured manner through life so that it supports all stages of the programme, informs all the key decision makers and provides a clear audit trail to support the safety claims at all stages of the project from concept to disposal (Dallimore, 2003).
- Ensure consistency of results by integrating and relating all aspects of the safety assessment (e.g. hardware analysis with software analysis; low-level probability studies with the high-level functional failure analysis) (Muari, 2000).
- Safety assessment activities should not cease upon system certification. There needs to be a proper interchange of information between the aircraft manufacturer and operators, so that:
  - modes of failure and critical failure rates that occur in service can be checked against the predictions. If either particular failure mode or its effect has not been correctly predicted it is important that the aircraft constructor should know so that he can consider whether the implications are serious.
  - alterations to checks and maintenance periods can be substantiated by the analysis.
  - modification can be assessed against the assumptions and limitations of the original design.
  - a sound MEL can be maintained and amended according to experience.
  - actual MTBF experienced will probably differ from predicted MTBFs used in FTA calculations during initial certification. Direct advantages are possible if the FTA can be updated with actual MTBF data. Action can be taken to improve safety or (if the predicted MTBFs were very conservative) maintenance intervals can be increased.

Benefits of adopting this approach will include (refer, *inter alia*, Dallimore, 2003):

- Early planning helps identify and deal with those safety-related risks that, if not resolved up front, can emerge late in the programme and give rise to cost escalation and delay.

- The ALARP approach can assist in setting priorities for investment by indicating which opportunities for designing out a safety risk or adding a safety feature give most benefit.
- The through-life approach assists judging the value that a proposed investment in safety adds to the provision of the desired operational capability.
- The audit trail provides a sound, and readily available, basis for defending the various investment and safety decisions when called upon to do so.

The point of system safety is to prevent accidents/incidents (the difference between which lies only in the result) before they occur. Safety lessons are there to be learned so as to prevent the next incident becoming an accident.

Problems affecting safety must be identified at the earliest possible stage to allow progression of the most cost-effective and efficient solution. Failure to consider and anticipate possible problems at an early stage can be an expensive omission. These risks can be as much of a hazard to the programme as other technical and commercial risks. It is not the identified hazard that is the problem. If a hazard has been identified it can be measured; it can be fixed and controlled. It is the unidentified hazard that is the problem. A hazard not identified is a hazard not managed. If it cannot be identified, it cannot be measured. If it cannot be measured it cannot be controlled. A safety assessment/safety case is therefore not just what has been done – it is also about how it has been done, and why no more is needed to be done.

There is no standard, correct and formal way to analyse system safety, there is always the need for human judgement. Engineers have always used judgement for safety issues. Professional judgement continues to be by far the most important part of safety management. Formal safety assessment methods must be used as aids to judgement and not as substitutes for it. Actions and decisions may be challenged by others with hindsight. A decision may have to be defended on the basis of judgement and so the decision process needs to be documented and validated wherever possible. What is required is an ordered approach to consider and document safety.

The safety assessment/case provides a way of showing that safety has been considered properly and that decisions have been well founded. The assessment should be systematic but there is no guarantee that the analysis will be 100% effective and complete. The process is therefore an iterative process within the overall life cycle of the system.

13.3 New technologies

The application of formal safety management has existed for many years. However, the maturity of safety management in different parts of the industry varies greatly, although there has been some convergence in recent years. Angove (1999) summarises some of the complicating factors:

- Regulation is fragmented and the requirements for safety are not always consistently imposed or adopted.
- Systems are made up of a huge diversity of inherited, new and partially mature systems, reflecting a similar diversity of technology.
- The operational installation and use of equipment and associated procedures (the operational environment) varies greatly.

- A wide variety of national cultures and attitudes cloud the picture, and different countries have evolved their own approaches to regulation.
- An increase in the profile of safety, particularly i.t.o. public perception.
- Litigation and legislation trends in the aftermath of accidents

Aviation's history provides evidence that, whatever the benefits of technological advances, the safety graph dips – or at least waivers – while industry learns how to use the new technology.

Example

Software automation has not always improved safety as much as expected, generally because of inadequate training and particularly in the 'need-to-know' (i.e. keeping the pilot in the loop).

Many flight-deck engineering concepts fail to consider the man–machine interface so necessary for safe flight (although this is fast changing under the banner of 'human factors').

For the near-term future, automated systems cannot be expected to be totally reliable because computers have no intuition, no intelligence and no decision-making ability of the kind required to resolve unforeseen situations. When the automatics suddenly start 'misbehaving' the technical knowledge limitations and surprise factor of the crew have frequently led to accidents and serious incidents. However, computers do monitor things far better than humans. They also refine performance (e.g. engine or flight path management) more efficiently.

There is a clear indication that the sheer complexity of modern systems creates problems for notions of management control (Smith, 1999). Weaknesses in the management of complex technological systems permit predictable and unintentional errors and cause catastrophic loss (Keely, 2000). Given the sheer complexity of modern systems, management faces problems of emergence – where elements of a system interact to create properties that had previously been unforeseen.[3] By breaking complex systems down into their component parts (reductionism) to generate solutions, we compound the risk of further failure by neglecting the impact of such interventions on the emergent properties of the system.

The intent is to grapple with the unknown and win: to determine a methodology for predicting, more accurately than before, the kind of problems which new technology or new operational practices may bring.

[3] Increased automation can lead pilots to become complacent and so unstimulated in the quieter phases of flight that it is easy for them to lag behind what the aircraft is doing. Furthermore, the rarity of failures (e.g. modern digital systems are often relatively trouble-free compared to their old mechanical counterparts) may mean that the pilot is slow to diagnose and deal with unaccustomed symptoms.

13.4 Safety engineering competence

As explored in Chapters 8 and 9, there is a clear need to address the 'whole system' when considering safety implications (see Chapter 8). This is due to the inherent complexity of engineering systems today, as well as those of the future, and demands that safety knowledge be distributed throughout the systems' supply chain, from the safety assessor to the designers, operators and maintainers.

The key difference between engineering systems of the past and those of today and the future is that a thorough knowledge of a system held by one individual is unusual because the system will often be an integration of several complex sub-systems. The safety implications of such a system are thus an integrated discipline of computer/mechatronics systems engineering, regulatory requirements and human behaviour. Whilst a profound knowledge in all of these aspects is ambitious, the ability to effect a dialogue between expert parties requires a familiarity with the key potential risks and the interactions between them. This is the philosophy of Safety Engineering.

Safety engineering is an engineering discipline requiring specialised professional knowledge and skills in specific principles, criteria and techniques, to allow the identification and control of hazards to acceptable levels (AAP 7001.054, Section 2 Ch 1 para 16-17). It draws upon professional knowledge and skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis, to specify, predict, and evaluate the safety of the system. To apply successfully, consistently and (most of all) efficiently, safety engineering is a skill acquired only after numerous years of practising in the system safety design and analysis areas.

Designers often only concentrate on (and then test) normal operation of a system. If the safety assessment is to be used as an effective design tool, then the designer should use it to consider the abnormal situations. The safety assessment should ask how a system will fail, not only how it will work, and then predict the probability of the undesired event occurring. It requires the use of imagination to determine possible sequences of events leading to accidents.

In many cases, the safety implications themselves can be as complex as the systems in which they might arise and thus familiarity with the technologies that comprise the modern engineering system is necessary beyond on-the-job, osmotic training. This also means that safety engineers have to work closely with system engineers, operators and maintainers (i.e. the system specialists who know the intricacies of the system) to meet the safety requirements required from the system under consideration.

13.5 Safety culture

Safety ownership is often viewed as being the exclusive responsibility of specific departments, yet a good safety culture results only from top-level sponsorship and support. Corporate actions and policies must demonstrate this, not just to the workforce in general, but especially to the safety management teams. Inaction or inappropriate actions by corporate management gives rise to a lack of commitment and erosion in morale.

A safety culture needs to be in place if safety in aviation is to improve. Research by Helmreich (1999) identifies three intersecting cultures:

1. National. This can be illustrated by the differences between the US (individualistic) and Asia (collectivistic). In the latter, a 'high power distance' culture, the leader is clearly boss. The comparison is strict obedience vs. 'I'll do my own thing'. In terms of adherence to rules Taiwan came out top and the US bottom – with potentially serious safety implications.
2. Professional. Hemreich describes this aspect as the 'dark side', as it is reflected in a sense of personnel invulnerability, which is 'clearly unrealistic. Positive culture, however, is reflected in the pride of work.
3. Organisational. Regards values with respect to errors, openness and adherence (see Chapter 12).

Key problems afflict the relationship between corporate management and the safety specialists (Fairfield, 2003). Some examples are:

- The former view the latter as cost centres, not revenue generators and therefore prime targets during overall expenditure squeezing.
- The former have difficulty understanding technical issues and the latter have difficulty avoiding the use of technical jargon.
- Safety shortfalls considered as significant by the former, are so rare as to be regarded as statistically insignificant. This causes considerations of need (or cost benefit of improvement) to seem academic, and are often unquantifiable.

The best way to overcome this is to implement a policy of 'to measure is to manage'. Safety concerns are categorised in accordance with accepted criteria and target and alert levels are set in such a way to enable all stakeholders to remain focused on achieving the safety targets. However, safety objectives can be achieved by a diverse range of means and may suffer from inherent subjectivity (e.g. human factors) and engineering judgement (e.g. service experience). It requires the safety professionals to stand up for themselves and ensure that all statements are made in a manner that will withstand the scrutiny of a legal inquiry after the unfortunate occurrence of a mitigated or unforeseen event occurring.

13.6 Impact on projects

Increasingly the procurement of aircraft, equipment and systems for the aeronautical industry is by means of collaborative projects. The arrangements for such projects are negotiated both between the Governments of the participating nations (via a Memorandum of Understanding), and the contractors of the participating countries.

Any variations in airworthiness procedure and standards are to be clearly documented. The safety engineer should agree these arrangements to ensure safety responsibilities can be accomplished. Specific issues to consider are listed below.

- Experience has shown that specifying regulations and standards can help to minimise risk and it can be a very powerful influence on safety provided it is applied intelligently. However, Murphy (1991) advises that it is counterproductive for the contract to simply list a large number of conflicting, sometimes out-of-date and unrealistic documents. This is because of the considerable effort necessary to reconcile these into a common set of practical requirements and deliverables.[4]

- The safety targets and risk levels need to be clearly defined. Murphy (1991) also correctly emphasises that this is a very important (and arguably most neglected) topic as it is the 'safety acceptance criteria' the system is expected to achieve, and hence the standard the safety assessment/safety case will be evaluated against. To successfully conduct the assessment the output should be measurable and achievable in the light of any other contractual constraints.
- All organisations involved need a common understanding of the applicable terms (for example, see the definition of a hazard in Chapter 5. Many terms have more than one meaning. Be certain that the whole supply chain is working with common definitions.
- For collaborative projects, safety activities need to be co-ordinated and managed from a top-down total system point of view.
  - Each organisation involved must understand the system level (see Chapter 6) of their part of the assessment, and how it interfaces with the other levels. Any safety integrity claims of a part of a system (e.g. COTS parts, assemblies or subsystems) without considering the whole (e.g. the aircraft) should be viewed with scepticism.
  - Someone must be appointed with overall responsibility for all aspects of safety, and he/she must (Murphy, 1991) have full visibility of all contractors and subsystems and the authority to initiate and technically control any lower-level analysis from them.

13.7 Final remarks

We will continue to see a continuation of the constant quests to protect crew, passengers, maintenance personnel, third parties and the environment from the ever-present risks associated with operating and maintaining complex (and especially high kinetic energy) machinery such as aircraft. Although an accident-free society is an unrealistic dream, it can be tempered by technical excellence in design, maintenance and operation to continually improve on the safety record.

Major challenges facing the European aeronautics industry include the following:

- continuing to reduce cost in every way – cost of design, cost of certification, cost of construction, cost of fuel consumed, cost of in-service support
- continuing to improve environmental performance – both noise and emissions – despite the major advances already made
- continuing to increase system capacity and performance
- continuing to improve safety.

[4] In order to do a satisfactory estimate to support a 'Fixed price competitive' contract, this task needs to be carried out during the contract negotiation phase, but the contractor generally cannot afford to fund this. If the contractor attempts this task during the development phase, it is probably without a budget and he again has a dilemma.

Technology will continue to be a major determinant of what the industry can deliver. Not all of the solutions to these issues are likely to be technology related. Technology alone cannot solve all problems caused by technology and when it comes to safety, we need to address the way in which hazards are managed and communicated. All stakeholders (from the decision makers, though to the users and maintainers of the system) need to have better information on the magnitude of the risk, the factors affecting that magnitude, and the consequences of each of the possible mitigating actions.

It is essential therefore to make safety assessments/cases, even of the most complex systems, comprehensible to all concerned and not just to the analyst. They must assist the designer and the operator in making decisions. They must make clear what the critical features are and on what special manufacturing techniques, inspection, crew drills and maintenance procedures they are critically dependent. The purpose of the analysis is not only to convince airworthiness authorities that a system is safe, but also to state clearly those aspects on which safety depends. Safety cases/assessments could therefore be especially useful to operators it they can be used in anger, instead of lying in a dust-gathering tomb.

Safety and performance, although important, are not the only aspects to be considered. One has to ensure that the design is practical and economical and likely to be reliable in service. It is relatively easy just to multiply the systems to achieve the required level of safety but this in itself may lead to problems of reliability and spares provisioning. In addition, practical operation of the aircraft may demand that it should be able to take off and fly safely, with various defects present. These factors have to be integrated into the overall design of the system and the aircraft.

Appendix A

Safety assessment tools and techniques

Note: This table has been compiled from a variety of sources (ranging from textbooks, publications, and the internet to the personal experiences of friends, colleagues and acquaintances).

Each of these tools has its own advantages and disadvantages and the extent to which these can be used during various phases of the product life cycle, and the degree to which it can be applied to safety assessments, vary. Listed in alphabetical order, the tools/techniques most frequently used by the author have been shaded.

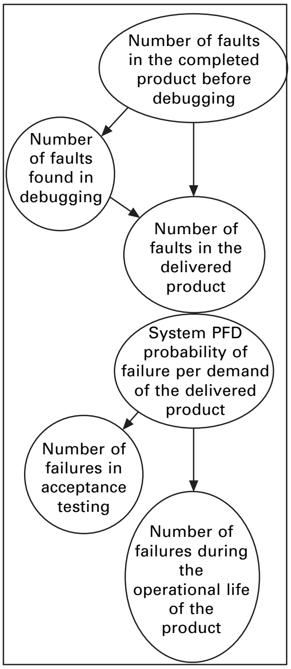
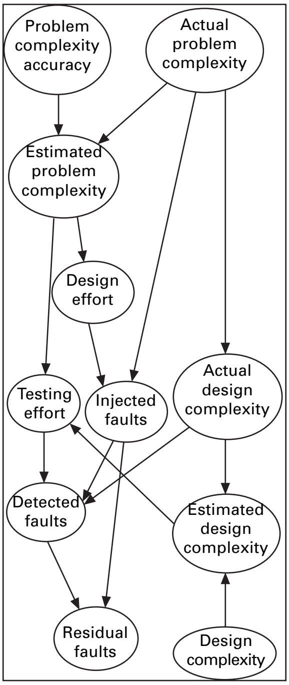
It is extremely important to note that as the complexity of the tool increases so does the degree of training required for the user and/or the need for an experienced evaluation team to conduct the evaluation. On the plus side, the data derived from the more complex methodologies may be more supportable. Unfortunately, the primary disadvantage of such tools is that 'trained subject matter experts' may have limited experience in the actual operational environment and, therefore, their evaluations may not be entirely applicable to the certification.

This table is intended to be thought provoking but has all the limitations of generic data. In no circumstances should it be considered complete, applicable to all systems or wholly objective. Many entries have no advantages/limitations listed, and space is provided for the reader to add data if desired.

The author will gladly receive any comments/suggestions/recommendations, which can be sent to systemsafety@hotmail.co.uk. For the latest update on this table (including links to relevant websites), see www.aircraftsystemsafety.com

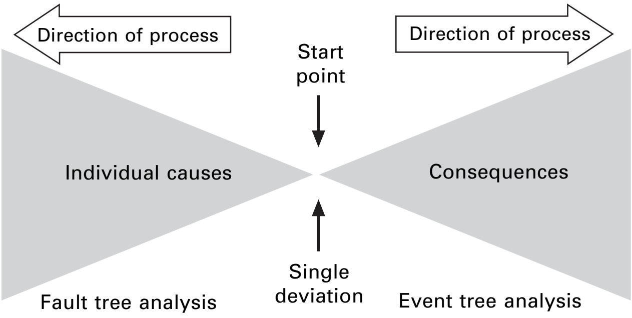
Technique	Description
Accident analysis	The purpose of the accident analysis is to evaluate the effect of scenarios that develop into credible and incredible accidents. Any accident or incident should be formally investigated to determine the contributors of the unplanned event. Many methods and techniques are applied.
Accident sequence evaluation programme (ASEP)	This tool is based on the Technique for Human Error Rate Prediction. ASEP comprises pre-accident screening with nominal human reliability analysis, and post-accident screening and nominal human reliability analysis facilities (Kirwan, and Ainsworth, 1992)
Action error analysis	Action error analysis analyses interactions between machine and humans. It is used to study the consequences of potential human errors in task execution related to directing automated functions. Any automated interface between a human and automated process can be evaluated, such as pilot/cockpit controls, or controller/ display, maintainer/equipment interactions.
ATLAS	ATLAS is a software package for use in support of systems design and analysis work. It combines the elements of graphically based task analysis with the advantages of a database. ATLAS supports a variety of conventional task analysis methods and incorporates more than 60 human performance, workload and human reliability algorithms. (Hamilton and Bierbaum, 1990)
Barrier analysis	Any system is comprised of energy, should this energy become uncontrolled accidents can result. The barrier analysis method is implemented by identifying energy flow(s) that may be hazardous and then identifying or developing the barriers that must be in place to prevent the unwanted energy flow from damaging equipment, and/or causing system damage. Barrier analysis is an appropriate qualitative tool for systems analysis, safety reviews, and accident analysis. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Bayesian belief networks	A BBN is a graphical network that represents probabilistic relationships among events in a network structure. With BBNs, it is possible to articulate expert beliefs about the dependencies between different variables and to propagate consistently the impact of evidence on the probabilities of uncertain outcomes, such as ‘future system reliability’ (Falla, 1997, Ch 4). The BBN on the left uses comparatively little evidence, depending only on the observed reliabilities and defect counts of previous products of the same process, and on the defects discovered in the current product during debugging. The topology of the graph is used to indicate probabilistic relationships among the variables described in the nodes. The BBN on the right includes subjective indicators, like problem complexity and design effort. Thus, this network is meant to be populated with probabilities that are not all derived from statistical inference, but at least in part from expert opinion. BBNs are also sometimes called causal probabilistic networks, probabilistic cause-effect models or probabilistic influence diagrams.

Advantages	Limitations
•	•
• ASEP provides a shorter route to human reliability analysis than THERP by requiring less training to use the tool, less expertise for screening estimates, and less time to complete the analysis.	•
•	•
•	•
•	•
• Provides decision-support for a wide range of problems involving uncertainty and probabilistic reasoning. • BBNs enable reasoning under uncertainty and combine the advantages of an intuitive visual representation with a sound mathematical basis in Bayesian probability. • BBNs allow an injection of scientific rigour when the probability distributions associated with individual nodes are simply 'expert opinions'. • A BBN will derive all the implications of the beliefs that are input to it, and some of these implications are statements of fact that can be checked against the observed reality of a software project, or simply against the experience of the experts and decision makers themselves.	• Because BBNs have a rigorous, mathematical meaning, software tools (i.e. efficient algorithms) are needed that can interpret them and perform the complex calculations needed in their use. •

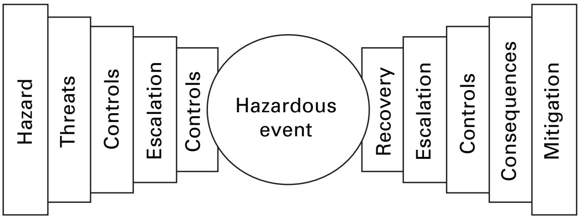
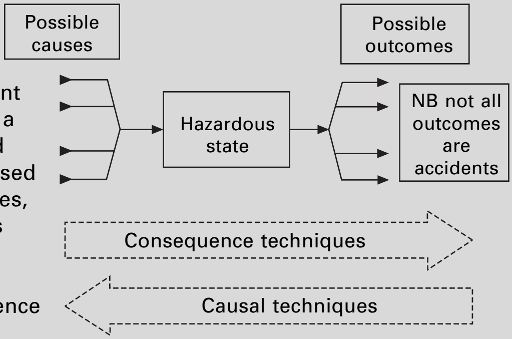
Technique	Description
	 
Bedford scale	Human factors evaluative tool.
Bellcore TR332 (now Telcordia)	The Bellcore approach is widely used in the telecommunications industry and has been updated to SR-332 (in May 2001). Bellcore's approach is very similar to that of MIL-HDBK-217 but it's based primarily on telecommunications data and covers five separate use environments. The approach also assumes an exponential failure distribution and calculates reliability in terms of failures per billion part operating hours, or FITs. Its empirically based models are in three categories: the Method I parts count approach that applies when there is no field failure data available, the Method II modification to Method I to include lab test data and the Method III variation that includes field failure tracking. Method I includes a first year modifier to account for infant mortality. Method II includes a Bayes weighting procedure that covers three approaches depending on the level of previous burn-in the part or unit has undergone. Method III includes a Bayes weighting procedure as well but it is based on three different cases depending on how similar the equipment is to that from which the data was collected. For the most widely used Method I case where the burn-in varies, the steady-state failure rate depends on the basic part steady-state failure rate and the quality, electrical stress and temperature factors as follows: $\lambda_{SSi} = \lambda_{Gi} \pi_{Qi} \pi_{Si} \pi_{Ti}$
Benefits analysis	An assessment (either qualitative and/or quantitative) used to determine the potential benefits to be derived from following (or not following) a particular course of action (see cost benefits analysis).

Number of faults in the completed product before debugging
Number of faults found in debugging
Number of faults in the delivered product
System PFD probability of failure per demand of the delivered product
Number of failures in acceptance testing
Number of failures during the operational life of the product

Advantages	Limitations
• Subjective in terms of safety implications.	• Subjective.
• TR-332 is widely used in the telecommunications industry and is generally believed to more accurately predict the reliability of telecommunications equipment than MIL-HDBK-217F.	•
• Effective to compare/contrast different options.	• Can be very subjective.

Technique	Description
Bent pin analysis	Connector shorts can cause system malfunctions, anomalous operations, and other risks. Bent pin analysis evaluates the effects should connectors short as a result of bent pins and mating or demating of connectors. Any connector has the potential for bent pins to occur. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Bottom-up analysis approach	Also known as the 'hardware' method, this starts with the hardware failure modes which can occur, and analyses the effects of these on the sub-system and the system. An example bottom-up approach is the FMEA.
Bow tie analysis	Uses a methodology known as the hazards and effects management process, which requires hazards to be identified, assessed, controlled and if subsequently they are released, recovery measures to be in place to return the situation to normal if possible.  Direction of process Start point Direction of process Individual causes Consequences Single deviation Fault tree analysis Event tree analysis The stages worked through in the bow tie are: • Proactive measures: – identification of the hazard. – identification of the threats that could release the hazard. – assessment of the threat controls already in place and the identification of additional controls that may be necessary to manage the threat effectively. – identification of the escalation factors that are conditions that prevent a threat control being effective. – assessment of the escalation controls, which are further measures needed to maintain control of the escalation factor. – identification of the hazardous event, which is the initial release of the hazard that can lead to an accident.

Advantages	Limitations
•	•
• Useful to identify the various failure modes of a specific module – especially if that module is safety critical. • Smaller parts are more manageable and lend themselves to controlled testing and evaluation (Garland, *et al.* 1999].	• A bottom-up approach for a complex system (with many combinations of failures together with the effects of crew and maintenance errors) may result in an impossible number of combinations. This may drive you to a top-down approach. • May lose sight of the 'big picture' • Can be expensive and time consuming. • The whole is often more that the sum of its parts.
• Has both proactive and reactive elements that systematically work through the hazard and its management. • The output of the bow tie analysis is tested against the risk assessment matrix, where judgements can be made as to the probability of a hazardous event occurring and the severity of its consequences. • Useful aid to any safety management system.	• Very time consuming and expensive to generate if not adequately prioritised. • Needs continuous management to reflect the current reliability.

Technique	Description
	 Hazard Threats Controls Escalation Controls Hazardous event Recovery Escalation Controls Consequences Mitigation • Reactive measures: – assessment of the recovery measures that would be appropriate to return the situation to as near to normal as possible. – identification of the escalation factors that are conditions that prevent a recovery measure being effective. – assessment of the escalation controls, which are further measures needed to maintain control of the escalation factor.
Brainstorming	Uses a team of knowledgeable people to work in an imaginative and non-critical atmosphere to solve problems.
Cable failure matrix analysis	Less then adequate design of cables can result in faults, failures, and anomalies, which can result in contributory hazards and accidents. Should cables become damaged system malfunctions can occur. Cable failure matrix analysis identifies the risks associated with any failure condition related to cable design, routeing, protection, and securing. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Causal analysis	Deductive analysis, which investigates the possible outcome of an undesired event. Uses techniques such as FTA, Software FTA, FMECA.
Cause consequence analysis	Integration of deductive (e.g. fault tree) and inductive (e.g. event tree) analysis into a single method and notation. Mainly used in nuclear industries, no good examples found in other industries yet. See also consequence analysis.  Possible causes Possible outcomes Hazardous state NB not all outcomes are accidents Consequence techniques Causal techniques

Advantages	Limitations
• This can be applied to hazard identification, where ‘thinking the unthinkable’ can suggest possible accidents and problems which the designer may never have considered. •	• There is little framework to ensure that the exercise is systematic and all hazards have been identified. • •
• Determines all credible combinations or sequences of causal factors that can lead to a hazard occurring. • Enables the calculation of the probability of a hazard occurring, which in turn can be used to determine the risk of an accident due to that hazard. •	• Hard to use, requires skilled analyst(s). • Difficulty of modelling increases very rapidly with system complexity.
• Very expressive notation with high information density. • Can express interactions of multiple failures and protective mechanisms. • Works through consequences-related failures. • Can be used for probability analysis, but becomes very complex. • Particularly suited to analysis of systems which include protective mechanisms.	• Hard to use, requires skilled analyst(s). • Difficulty of modelling increases very rapidly with system complexity. • Not widely adapted yet, but will improve due to new software tools.

Technique	Description
Change analysis	Change analysis examines the effects of modifications from a starting point or baseline.
Checklists	In the past, hazards identification relied on the experience of individual engineers and on previous accidents. Sometimes this knowledge would be embodied in hazard checklists. A checklist is, as its name implies, a list of questions, features or key points against which something is assessed ('checked') to determine its acceptability. Checklists can be constructed for many purposes and can be short or long, simple or complex. In fact, checklists are as varied as the systems being designed or evaluated or the tasks to be performed. Checklists incorporate past experiences in convenient lists of 'do's' and don'ts'. The list is more of a prompt to the imagination of the user than a checklist which can guarantee identifying all possible hazards. Some useful checklists include: • The ATC Electronic Checklist, developed by the Volpe Center and the FAA, provides a checklist of human factors issues that should be considered in the design and evaluation of air traffic control systems and equipment. The checklist points controllers and other operations specialists to questions that they may wish to consider in the evaluation of new systems or subsystems or a new component of an existing system (see http://www.hf.faa.gov/) • The Ergonomics Audit Program (ERNAP) is a computerised checklist to help managers design and/or evaluate procedures for aviation maintenance and inspection. ERNAP is simple to use and evaluates existing and proposed tasks and set-ups by applying ergonomic principles. ERNAP allows the auditor to maintain audits for further reference. ERNAP was developed under the auspices of the FAA, and can be downloaded from the Human Factors in Aviation Maintenance and Inspection (HFAMI) website. See http://www.hfskyway.com/jobaids.htm) • CRT display checklist, which forms Appendix A to NUREG/CR-3557. It provides subjective comparisons of methods for displaying screen information but is also used as a design checklist (refer Kirwan and Ainsworth, 1992) • Ravden & Johnson Checklist, which is a comprehensive checklist of items that evaluate the usability of human-computer interfaces. It is easy to administer but its 156 questions make it somewhat lengthy. It generates much data on interface factors including visual clarity, consistency, compatibility, feedback, explicitness, functionality, control, error management, help facilities, and the usability of help facilities (Ravden and Johnson, 1989). • NUREG-0700: US Nuclear Regulation Commission (NRC) has produced several human factors guidance documents. NUREG-0700 is a detailed checklist for control room design (or more precisely, design review) in the nuclear power industry. The checklist addresses individual instruments, so using this checklist is a time-consuming process because of its detail. The guidelines, first issued in 1981, were recently revised to take into account the introduction of computer-based, human-computer interface technology (Kirwan and Ainsworth, 1992).

Advantages	Limitations
•	▪
• Useful for revealing otherwise overlooked hazards. • Easy to use (if it does exist) evaluation against existing guidelines. • Based on experience. • Requires minimum manpower. • Useful when more precise methods (e.g. FMEA, HAZOPS) are not possible or practical. • Particularly useful if combined with 'What-if' analysis. • Hazard checklists are available from various sources such as DEF STAN 00-56 and BSEN 1050 and they range from the very general to industry specific.	• Satisfactory for known hazards only (i.e. if they have been met before). Cannot foresee new hazards (e.g. for new technology). • Need to be continually supplemented to remain valid. • Not predictive. • Can be box ticking exercise. • Generally better at identifying physical hazards than functional hazards, unless the checklist is system-specific. • Checklists are generally better at suggesting relevant physical hazards than functional hazards.

Technique	Description
Chi-squared method	A method for detecting differences between a binomial and a multinomial population. Observations may fall into one or more categories and compare two or more samples
Cognitive event tree system (COGENT)	Human error reliability assessment.
Cognitive reliability assessment technique (CREATE)	Human error reliability assessment.
Cognitive work analysis (CWA)	Traditional approaches to work analysis tend to emphasise centralised work organisations, whereas turbulent, dynamic environments tend to require more distributed work organisations. The focus of the CWA framework is on identifying the constraints that shape behaviour rather than trying to predict behaviour itself. Rasmussen's (1986) framework for cognitive work analysis (CWA) provides separate descriptions of different classes of constraints: Work Domain (the functional structure of the work domain in which behaviour takes place); Control Tasks (the generic tasks that are to be accomplished); Strategies (the set of strategies that can be used to carry out those tasks); Social-Organisational (the organisation structure); Worker Competencies (the competencies required of operators to deal with these demands). [http://www.mie.utoronto.ca/labs/cel/research/frameworks/cwa.htm, 5/9/05]
Common cause analysis (CCA)	Generic term encompassing ZSA, PRA and CMA (see SAE ARP4761) Although most systems employ redundancy techniques (i.e. fail safe design), it will be found on examination that many of them have a 'single cause' (e.g. EMI/EMC), or 'common point' (e.g. common bus-bar or common controller), that could cause multiple failures. A common mode failure is a failure that has the potential to fail more than one safety function and to possibly cause an initiating event or other event simultaneously. For instance: • Common part failure: three totally independent flying control systems may merge together in a common part – the pilot's control column. A failure of this common part causes total system failure. • Common cause failure: a fire in a compartment might destroy all the channels of a system running through that compartment. Likewise, contaminated hydraulic fluid could cause all the channels of the hydraulic system to fail, or mechanical failures in an electrical loom. • Common mode failure: identical software in a dual redundant system will fail when exposed to the same inputs; jamming of a mechanical system (either due to failure or due to FOD); overheating of avionic equipment, etc. • Cascade failures: a single failure may overload the remaining channels, thereby increasing the probability of their failure. Or, an initial minor failure (e.g. a deflated tyre) causes a cascade of events (e.g. Concorde). The CCA (consisting of the ZHA, PRA and the CMA) provides the tools to verify required independence, or to identify specific

Advantages	Limitations
• Useful in statistical analysis for RAM data.	•
• A complement to traditional task analysis in that it retains the benefits of these methods but also adds the capability for designing for the unanticipated by describing the constraints on behaviour rather than behaviour *per se*.	•
Identifies failure modes or external events which could lead to a hazardous failure condition. • Supports the selection of system architecture through determination that appropriate independence can be achieved. • Most other techniques concentrate on the functionality. CCA ensures that the installed design is free from common causes which can undermine design, qualitative and quantitative predictions. • Analyses system architectures that rely on redundancies. Establishes and validates physical and functional separation and isolation requirements between systems. • Crosses system boundaries, and should identify the fault containment strategies needed. • May identify common development errors (e.g. software design errors, installation error, etc.). • May identify common environmental hazards (e.g. HIRF, moisture, temperature, etc.) • Validates independence. • CCA fault sources include S/W errors,	• Used throughout design process, but more cost-effective if done earlier because of the influence on system architecture. However, confirmation is often only feasible when the implementation is complete. • Difficult to be rigorous. • Requires detailed knowledge of the system. • Difficult to identify hazards in isolation, best suited to brainstorming sessions with multiple input (preferably using checklists as prompts).

Technique	Description
	dependencies. It identifies failures which by-pass or invalidate redundancy/independency assertions.
Common mode analysis (CMA)	Provides evidence that the failures assumed to be independent are truly independent in the actual implementation. Covers the effect of design, manufacturing and maintenance errors and the effects of common component errors (e.g. considers independence of duplicate systems due to design errors (e.g. S/W), lightning, HIRF, cooling, fire, contamination, etc.). A common mode failure has the potential to fail more than one safety function and to possibly cause an initiating event or other abnormal event simultaneously. Rare in technical systems, but typical in human actions (e.g. maintenance).
Comparison-to-criteria	The purpose of comparison-to-criteria is to provide a formal and structured format that identifies safety requirements. Comparison-to-criteria is a listing of safety criteria that could be pertinent to any system. This technique can be considered in a requirements cross-check analysis. Applicable safety-related requirements such as OSHA, NFPA, ANSI, are reviewed against an existing system or facility. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Confined space safety	The purpose of this analysis technique is to provide a systematic examination of confined space risks. Any confined areas where there may be a hazardous atmosphere, toxic fume, or gas, the lack of oxygen could present risks. Confined space safety should be considered at tank farms, fuel storage areas, manholes, transformer vaults, confined electrical spaces, race-ways. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Consequence analysis	Inductive analysis, which takes a given event (usually a failure) as a starting point, and works forward to determine the possible outcome (see also cause consequence analysis). The consequence analysis will determine the relationship between hazards and the accidents to which they lead. The forward looking part of HAZOPS, SWIFT and functional FME(C)A are all consequence analyses. Includes ETA, cause consequence diagrams, etc.

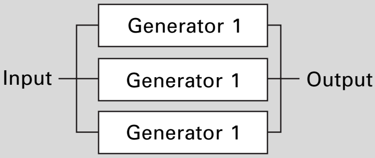
Advantages	Limitations
requirement errors, repair process errors, environmental factors, H/W design errors, production errors, installation errors, operational errors, cascading failures, etc.	
• Verifies that the 'AND'-ed events in the FTA/DD/MA are independent in the actual implementation. • A good second line check on design. • Covers the effects of design errors (e.g. S/W error, requirements error), manufacturing errors (e.g. production process error), maintenance errors, operational errors (e.g. operator failure), the effects of common component failures (e.g. common S/W in redundant systems), cascading faults, common external source faults, etc.	• Relies on acceptance that seemingly unlikely events will occur. • Difficult to be rigorous. •
•	•
•	•
• Determines the relationship between hazards and the accidents to which they lead. • Enables the calculation of risk for each accident. • Enables either: a. The calculation of risk of each accident – carrying probabilities up the accident model. b. The setting of a safety target – moving targets down the accident model to the system(s) presenting the hazard.	• Accident sequence needs to include ability of pilot/technician/maintainer to influence the outcome based on their expected levels of training and experience. This tends to lead to high levels of subjective judgement to compensate for factors such as high workload or stress. • In many situations it is difficult to be certain about the scale of the consequences. There may be little quantitative data available on rare events such as major explosions and releases of toxic gas clouds. • It explores all the consequences, not all of which may result in harm.

Technique	Description
Contingency analysis	Contingency analysis is a method of minimising risk in the event of an emergency. Potential accidents are identified and the adequacies of emergency measures are evaluated. Contingency analysis should be conducted for any system, procedure, task or operation where there is the potential for harm. Contingency analysis lists the potential accident scenario and the steps taken to minimise the situation. It is an excellent formal training and reference tool. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Continuous safety sampling methodology (CSSM)	This is a form of hazard analysis that uses observation (e.g. control charting) and work sampling techniques to • determine and maintain a pre-set level of the operator's physical safety within constraints of cost, time and operational effectiveness. • observe the occurrence of conditions that may become hazardous in a given system. These conditions, known as dendritics, may become hazards and could result in an accident or occupational disease. Continuous safety sampling methodology performs a random sampling for the occurrence of these dendritics. The collected data are then used to generate a control chart. Based on the pattern of the control chart, a system 'under control' is not disturbed whereas a system 'out of control' is investigated for potential conditions becoming hazardous. Appropriate steps are then taken to eliminate or control these conditions to maintain a desired safe system. This tool is used to determine whether activities are within tolerable limits. If outside tolerable limits, corrective action is then derived. (Quintana and Nair, 1997 (DK))
Control rating code	Control rating code is a generally applicable system safety-based procedure used to produce consistent safety effectiveness ratings of candidate actions intended to control hazards found during analysis or accident analysis. Its purpose is to control recommendation quality, apply accepted safety principles, and priorities hazard controls. Control rating code can be applied when here are many hazard control options available. The technique can be applied toward any safe operating procedure, or design hazard control. (FAA System Safety Handbook, Chapter 9: Analysis Techniques December 30, 2000)
Cost benefit analysis	A weighing scale approach to decision making. All the pluses (e.g. cash savings, lives saved) are put on one side of the balance and all the minuses (e.g. costs, disadvantages) are put on the other. Whichever weigh the heavier wins. A frequent mistake is to use non-discounted amounts for calculating costs and benefits. A method like 'net present value (NPV)' and 'economic value added' is strongly recommended, because all these account for the time value of money. Another frequent problem is that typically the costs are tangible, hard and financial, whilst the benefits are hard and tangible, but also soft and intangible. Care should be taken here against claims that 'if you cannot measure it, then it does not exist/it has no value'.

Advantages	Limitations
•	•
• Proactive methodology for accident prevention.	• It may focus more on industrial injuries.
•	•
•	Often not socially (and even legally) acceptable

Technique	Description
Critical incident technique	This is a method of identifying errors and unsafe conditions that contribute to both potential and actual accidents or incidents within a given population by means of a stratified random sample of participant-observers selected from within the population. Operational personnel can collect information on potential or past errors or unsafe conditions. Hazard controls are then developed to minimise the potential error or unsafe condition. This technique can be universally applied in any operational environment (Tarrents, 1980).
Critical path analysis	Critical path analysis identifies critical paths in a program evaluation graphical network. Simply it is a graph consisting of symbolism and nomenclature defining tasks and activities. The critical path in a network is the longest time path between the beginning and end events. This technique is applied in support of large system safety programme, when extensive system safety-related tasks are required.
Damage modes and effects analysis	Evaluates the damage potential as a result of an accident caused by hazards and related failures. Risks can be minimised and their associated hazards eliminated by evaluating damage progression and severity (Tarrents, 1980).
Deactivation safety analysis	This analysis identifies safety concerns associated with facilities that are decommissioned/closed. The deactivation process involves placing a facility into a safe mode and stable condition that can be monitored if needed. Deactivation may include removal of hazardous materials, chemical contamination, spill cleanup.
Decision analysis	Decision analysis is a broad term to describe tools for facilitating, understanding or structuring decision-making processes. The essence of decision analysis is to break down a complicated decision into its component parts or elementary qualities, and in particular to separate clearly the subjective and objective aspects of that decision. Decision analysis originates in the field of operations research but has links to economics, mathematics, psychology and human factors. A wide range of tools have been developed which utilise a variety of methods such as influence diagrams, decision trees, voting methods, multi-attribute utility methods and so on.
Deductive analysis	Analysis which works back from a given event (failure) to identify its causes. It starts from known effects to seek unknown causes. A deductive argument is where the conclusion is implicit in the evidence used to support the argument.
Defect/failure reporting analysis and corrective action system (DRACAS/FRACAS)	Closed loop data reporting system to aid design, identify actions, and evaluate results.

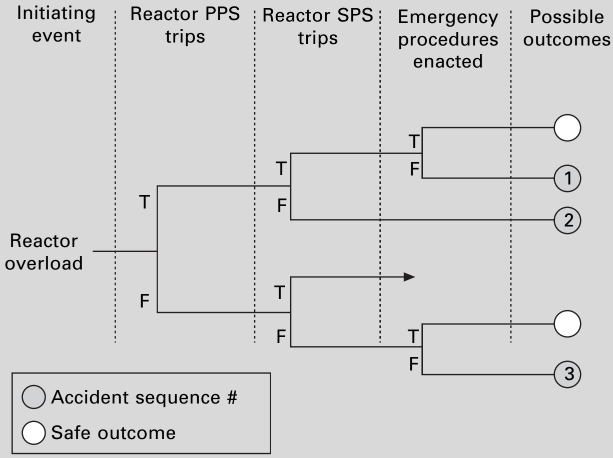
Advantages	Limitations
•	•
•	•
•	•
•	•
•	
• Useful during incident/accident analysis.	
• Useful to identify common mode failures and trends. •	• Historical data technique (relies on past experience). • Primarily a reliability tool. • Depends on accurate data collection. • Depends upon ability to find similar data. • Does not address unknown hazards.

Technique	Description
Dependence diagrams (DD)	Similar to the FTA, but replaces the logic gates by paths to show the relationship of the failures. A dependence diagram analysis is success-oriented, and is conducted from the perspective of which failures must not occur to preclude a defined failure condition.  Input Generator 1 Generator 1 Generator 1 Output Each block defines, for example, a failure of a part of a system and the conditions related to it and, where needed, the estimated frequency of occurrence. The blocks are arranged in series or parallel to represent 'and' or 'or' gates respectively. See SAE ARP4761
Design appraisal	A qualitative appraisal of the integrity and safety of the system design. Can be used to consider a range of issues, such as: • what happens if? • possibility of maintenance induced failures • suitability/compatibility of materials
Dynamic workload scale	Human factors evaluative tool.
Electromagnetic compatibility analysis	The analysis is conducted to minimise/prevent accidental or unauthorised operation of safety-critical functions within a system. Adverse electromagnetic environmental effects can occur when there is any electromagnetic field. Electrical disturbances may also be generated within an electrical system from transients accompanying the sudden operations of solenoids, switches, choppers, and other electrical devices, radar, radio transmission, transformers (Tarrents, 1980).
Energy analysis	The energy analysis is a means of conducting a system safety evaluation of a system that looks at the 'energetics' of the system. The technique can be applied to all systems, which contain, make use of, or which store energy in any form or forms, (e.g. potential, kinetic mechanical energy, electrical energy, ionising or non-ionising radiation, chemical, and thermal) (Tarrents, 1980).
Energy trace analysis	This hazard analysis approach addresses all sources of uncontrolled and controlled energy that have the potential to cause an accident. Examples include utility electrical power and aircraft fuel (FAA System Safety Handbook, Chapter 9). Sources of energy causing accidents can be associated with the product or process (e.g., flammability or electrical shock), the resource if different than the product/process (e.g., smoking near flammable fluids), and the items/conditions surrounding the system

Advantages	Limitations
• Illustrates the failure combination of the system. • Less complicated than FTA (adopted by some European aircraft constructors). • Very useful where numerical assessment of the probabilities is needed. • Like the FTA and MA, it identifies the failure events which could collectively or individually lead to the occurrence of the undesired top event. • Establishes crew and maintenance tasks and intervals needed to meet the safety objectives. • S/W errors can be qualitatively represented. • Rapidly identifies critical failure sequences (i.e. minimum cutsets).	• Assumes failure modes are independent. • Assumes failure rates are small and constant over time. • Not an exhaustive analysis toll.
• Simple and pragmatic. • Quick, hence an effective tool at the early stages to identify potential problem areas. • May be used effectively on all systems.	• Highly subjective, often not systematic. • Not a rigorous method and very dependent on the analyst's experience.
• Subjective in terms of safety implications.	•
•	•
•	•
•	•

Technique	Description
	or resource of concern (e.g., vehicles or taxiing aircraft). A large number of hazardous situations are related to uncontrolled energy associated with the product or the resource being protected (e.g., human error). Some hazards are passive in nature (e.g., sharp edges and corners are a hazard to a maintenance technician working in a confined area). The purpose of energy trace analysis is to ensure that all hazards and their immediate causes are identified. Once the hazards and their causes are identified, they can be used as top events in a fault tree or used to verify the completeness of a fault hazard analysis. Consequently, the energy trace analysis method complements but does not replace other analyses, such as fault trees, sneak circuit analyses, event trees, and FMEAs.
Energy trace and barrier analysis	Similar to energy analysis and barrier analysis. The analysis can produce a consistent, detailed understanding of the sources and nature of energy flows that can or did produce accidental harm. The technique can be applied to all systems, which contain, make use of, or which store energy in any form or forms, (e.g. potential, kinetic mechanical energy, electrical energy, ionising or non-ionising radiation, chemical, and thermal) (Tarrents, 1980).
Energy trace checklist	Similar to energy trace and barrier analysis, energy analysis and barrier analysis. The analysis aids in the identification of hazards associated with energetics within a system, by use of a specifically designed checklist. The analysis could be used when conducting evaluation and surveys for hazard identification associated with all forms of energy. The use of a checklist can provide a systematic way of collecting information on many similar exposures (Tarrents, 1980).
Environment analysis	Human error reliability assessment technique. The environment analysis can be performed concurrently with the user and task analysis. Activities or basic tasks that are identified in the task analysis should be described with respect to the specific environment in which the activities are performed.
Environmental risk analysis	The analysis is conducted to assess the risk of environmental noncompliance that may result in hazards and associated risks. The analysis is conducted for any system that uses or produces toxic hazardous materials that could cause harm to people and the environment (Tarrents, 1980).
Event and causal factor charting	Utilises a block diagram to depict cause and effect. The technique is effective for solving complicated problems because it provides a means to organise the data, provides a summary of what is known and unknown about the event, and results in a detailed sequence of facts and activities (Tarrents, 1980).

Advantages	Limitations
•	•
•	•
•	• In most cases, the user characteristics need to be considered in a particular environment.
	•
•	•
•	•

Technique	Description
Event tree analysis (ETA)	ETA is an inductive technique that considers the consequence of an initiating event and the expected frequency of each occurrence. It is a graphical technique that starts from an initial occurrence (e.g. lightning strike or system condition, such as a rupture of a fuel pipe or loss of power supply) and builds upon this by sequencing the possible events. It is illustrated as a tree of possible true/false outcomes against each mitigating mechanism. Event tree analysis starts with a hazard, but instead of working backwards as in the fault tree, it works forward to describe all the possible subsequent events and so identify the event sequences that could lead to a variety of possible consequences.  Initiating event Reactor PPS trips Reactor SPS trips Emergency procedures enacted Possible outcomes Reactor overload T F T F T F T F T F 1 2 3 Accident sequence # Safe outcome Originally devised to access the protective systems and safety of nuclear reactors, it operates with inductive (i.e. forward) logic by asking the question: ‘What happens if...’
Explosives safety analysis	This method enables the safety professional to identify and evaluate explosive hazards associated with facilities or operations. Explosives safety analysis can be used to identify hazards and risks related to any explosive potential, i.e. fuel storage, compressed gases, transformers, batteries (Tarrents, 1980).
Extended master plan logic diagram (MPLD)	Extended from MPLD to include the additional category of couplings which originate common cause failures (a logic diagram that shows how functional, equipment and component failure combine to cause a system malfunction) These are represented in fault-tree-like structures, except that basic events are not represented as leaf events but are listed in the lower left part of the tree and connected to gates though a sort of matrix (Mauri, 2000).
External events analysis	The purpose of external events analysis is to focus attention on those adverse events that are outside of the system under study. It is to further hypothesise the range of events that may have an effect on the system being examined. The occurrence of an external event such as an earthquake is

Advantages	Limitations
• IDs all possible outcomes (i.e. consequences) of an event (e.g. accident sequences). • Displays at a glance the sequences of events that relate to the proper functioning of a system. • Effectively explores how design copes with different accident scenarios. • Complements FMEA and HAZOP by tracing the chain of events resulting from a component failure. • Useful in accident sequence studies. • Useful to model mitigation (highlights insufficient mitigating mechanisms). • It can be quantified if the probabilities of success and failure at each branching point can be established. • Easy to understand, with time basically running from right to left. • Event tree analysis complements fault tree analysis in much the same way as FMEA complements HAZOP.	• Does not consider equipment/system degradation. • Reliant on experience of human actions. • Very subjective. • Can become very complex. • Only deals with success/failure combinations, cannot deal with delayed recovery. • The event tree shows all possible outcomes from an initiating event, ranging from major accidents to safe results. • Separate ETA diagrams are required for each initiating event being examined, so interaction of various events/outcomes not easily modelled.

Technique	Description
	evaluated and affects on structures, systems, and components in a facility are analysed (Tarrents, 1980).
Facility system safety analysis	System safety analysis techniques are applied to facilities and its operations. Facilities are analysed to identify hazards and potential accidents associated with the facility and systems, components, equipment, or structures (Tarrents, 1980).
Failure logic analysis for system hierarchies (FLASH)	Developed to enable the assessment of a hierarchically described system from the functional level down to the low levels of its hardware and software implementation. Each module of the architecture (i.e. sub-system or basic component) is systematically examined for potential failure modes and how those failure modes relate/propagate to other modules in the system hierarchy (Mauri, 2000).
Failure mode and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA)	A systematic, hardware (i.e. bottom-up) approach of identifying failure modes of a system or item, and determining the effects on a higher level. It answers the question 'if this part fails, what will be the next result?' The FMEA is performed at a certain level (system, subsystem, module, part/item, etc.) by postulating the ways the chosen level's specific implementation may fail. Can be developed to the level of the smallest replaceable item (i.e. piece part FMEA) or functional level (i.e. functional FMEA, which could be the same as an FHA). Piece part FMEA is useful to determine the theoretical failure probability of the part being considered, whilst a function FMEA uses predetermined probabilities as an input. Failure effects leading to the same system condition can be identified and grouped together in a FMES. Does not have to be quantitative. Best suited to mechanical and electrical hardware systems. Although very extensive, the 'devil is in the details'. It is generated to support the safety assessment, so it is important to understand the expectations and requirements of the FMEA before any work on it commences (e.g. its sole purpose may be to support verification of the FTA through a comparison of FMEA failure modes with the basic events of the fault tree). Co-ordinate required scope of FMEA with the user requesting it. If the failure rates from a Functional FMEA allow the PSSA targets to be met, then a piece part FMEA may not be necessary. See MIL-STD-1629 and BS 5760 Part 5 and SAE ARP4761. For useful software tools, see www.byteworx.com
Failure mode and effects summary (FMES)	Summary of lower-level FMEA failure modes with the same effect. The failure rate for each failure mode is the sum of the failure rates coming from the individual FMEAs see SAE ARP4761.

Advantages	Limitations
•	•
• Contributes towards improving consistency, completeness and correctness in safety analysis by integrating well-established safety analysis techniques (Mauri, 2000).	• FLASH has recently resulted from a doctoral study at York University (Mauri, 2000), and is yet to be proven in industry. • It is complex, and may need software automation to reduce workload and repetitive errors.
• Simple, flexible concept that identifies those failures (including dormant/latent failures) that could cause a loss of a specific function. • Very systematic at lower levels (i.e. individual components). Identifies the cause of each failure mode. • Useful for the preparation of diagnostic routines (e.g. flowcharts or fault-finding tables) by conveniently listing all the failure modes. • Good record for future reviews. • Identifies the possible causes of each failure mode and so assists with BIT, failure indications and redundancy. • Complements the FTA when an item has particularly significant potential consequences. • FMECA provides a numerical probability level as well as a criticality classification for each failure. • Provides RAM data to the LSA process. • Provides source data for the FTA/DD/MA. • Functional FMEA suitable for designs not finalised to component level.	• Lists only single failures (assumes rest of system is working perfectly), some of which may be of no safety concern. • Primarily a reliability technique. Good at generating maintainability. • Can be very detailed (critical aspects may be lost in the detail). Level of analysis must be decided (piece-part/LRU/Subsystem/system). • In FMECA severity can only be allocated if it is taken through to system level (e.g. adding a safety severity to a resistor failure is meaningless). • Time consuming and expensive to generate (often iterative). • Needs continuous management to keep it current. • An empirical, rather than a relative measure. • Often too much reliance is placed on the FMEA/FMECA, while ignoring threats which can arise from outside the system (e.g. common cause failures, human error, multiple failures, etc.). • Cannot cope with human induced hazards/errors. • Piece part FMEA is not practically feasible for modern microcircuit based LRU and systems.
• Used as input into the FTA (and others). • Simplifies the FTAs (reduces the number of OR-gates) by combining the effect of item failures (and failures of the installation that have the same effect) as one single event.	•

Technique	Description
Failure propagation and transformation notation (FPTN)	Hierarchical graphical notation that represents system behaviour. It represents a system as a set of interconnected modules; these might represent anything from a complete system to a few lines of program code. The connections between these modules are failure modes, which propagate between them (Mauri, 2000).
Fault hazard analysis	A system safety technique that is an offshoot from FMEA. Similar to FMEA above, however, failures that could present hazards are evaluated. Hazards and failures are not the same. Hazards are the potential for harm, they are unsafe acts or conditions. When a failure results in an unsafe condition it is considered a hazard. Many hazards contribute to a particular risk. Any electrical, electronics, avionics, or hardware system, sub-system can be analysed to identify failures, malfunctions, anomalies, faults, that can result in hazards (Tarrents, 1980).
Fault isolation methodology	The method is used to determine and locate faults in large-scale ground-based systems. Examples of specific methods applied are; half-step search, sequential removal/replacement, mass replacement, and lambda search, and point of maximum signal concentration. Determine faults in any large-scale ground-based system that is computer controlled (Tarrents, 1980).
Fault tree analysis (FTA)	A graphical model (developed in the 1960s) for illustrating: • logical relationships between a particular failure condition and the failures or other causes leading to a particular undesired event. • the pathways within a system that can lead to a foreseeable, undesirable loss event. The pathways interconnect contributory events and conditions, using standard logic symbols. It is a top-down (deductive) analysis proceeding through successively more detailed (i.e. lower) levels of the design until the risk of occurrence of the top event (the feared event) can be predicted. It is the opposite process to the FMECA: the FTA goes down to a primary event (i.e. an event which does not need to be broken down any further). The primary events can be hardware failures, human errors, software faults or external factors like the weather. Developed in the 1960s and has since then been readily adopted by a range of engineering disciplines as one of the primary methods of predicting system reliability and availability parameters. FTA is essentially a systematic qualitative technique to which a quantitative analysis can usually be applied if suitable failure data exists. Even in situations where failure data does not exist, it may still be useful to perform an FTA due to the insight it yields concerning a system's potential failure behaviour. FTA provides valuable information through qualitative analysis but can also be quantified with event probabilities or rates to give an estimate of how often the top event will occur. Computerised FTA provides good graphic output, quick evaluation of changes, more sophisticated algorithm, but can lead to less

Advantages	Limitations
•	•
•	•
•	•
• Gives a visual representation of combinations of failures. • Establishes deeper understanding than just understanding of the correct functioning. • Provides insight into the relationship between the various functional elements. Allows for the identification of common mode/cause failures. • Useful to determine what single failure (i.e. component failure or human error) or combination of failures exist at the lower levels that might lead to a higher level (e.g. functional) failure (i.e. identified hazard causes and cause combinations). • Unlike the FMECA, the FTA analyses only the detail contributing to the top event and hence the costs are significantly reduced by concentrating effort where it has most effect. • Good for fault diagnostics (e.g. during maintenance and operatations) and sensitivity assessments. • Well-defined semantics and clear structure. • Complementary information available from qualitative and quantitative analysis. • Can be used to verify compliance with PSSA objectives.	• FTA is not a technique for hazard identification. • Requires good understanding of the design, its components and how they fail, so design needs to be quite mature. • Complex and tedious to prepare. Substantial experience needed to produce useful, well structured trees in a reasonable time. • There is the potential for failure paths to be missed. • Large trees difficult to understand/follow. • Logically overprecise. • Can be drawn in many ways. • May miss common cause failures at lower levels. • Less valuable for revealing system design deficiencies unless they are directly related to, or within, a component. • Poor at evaluating human errors. • Cannot consider accident sequences (where timing is important) and transient effects. • Prone to error (vulnerable to mistakes at base levels). • Difficulty with common cause or common effect failures. • Where do you stop? (When sufficient

Technique	Description
	understanding by analysts and a temptation to become overly complex.
Fire hazards analysis	Fire hazards analysis is applied to evaluate the risks associated with fire exposures. There are several fire hazard analysis techniques, i.e. load analysis, hazard inventory, fire spread, scenario method. Any fire risk can be evaluated (Tarrents, 1980)
Flow analysis	The analysis evaluates confined or unconfined flow of fluids or energy, intentional or unintentional, from one component/sub-system/system to another. The technique is applicable to all systems which transport or which control the flow of fluids or energy (Tarrents, 1980).
Function and task analysis	Human error reliability assessment technique. Detailed analysis of the functions to be accomplished by the human/machine/ environment system and the tasks performed by the human to achieve those functions. • Function analysis. An analysis of basic functions performed by the 'system' (which may be defined as human-machine, human-software, human-equipment-environment, etc.). The functional description lists the general categories of functions served by the system. Functions represent general transformations of information and system state that help people achieve their goals, but do not specify particular tasks. • Task analysis. Task analysis is one of the most important tools

Advantages	Limitations
• Can include operational, environmental and human models. • Can establish crew and maintenance tasks and intervals needed to meet the safety objectives. • Useful during MEL consideration. • Supports qualitative and quantitative analysis, although not easily in combination. S/W errors can be qualitatively represented. • FTA intrinsically generates the documentation required to support an audit trail. • Particularly useful to model complex systems. • Assist with allocation probability budgets. • Useful for sensitivity analysis (e.g. evaluating sensitivity of failure rates). • Useful for systems with redundancy (two or more ways of achieving a function) and looking at the number of separate events required to cause the undesired top event. • It can also identify potential problems with 'dependent failures' which might affect several apparently separate redundant equipments (e.g. both the duty and standby power supplies). • Allocates budgets to lower level events.	detail to satisfy the top level hazard requirement has been identified.) • Difficult in complex designs (e.g. computer systems). • Illusive quantitative base event data. • Qualitative FTA only identifies the events that contribute to a scenario, it does not provide quantitative results. • If the undesirable top-event is not defined very specifically, the fault tree produced would quickly become large, complex and unmanageable. • Not sufficient for addressing the interaction of components, maintenance actions, repairability and redundancies.
•	•
•	•
•	

In general, the more complex the system, such as air traffic control, the more detailed the function and task analysis. It is not unusual for ergonomists to spend several months performing this analysis for a product or system. The analysis would result in an information base that includes user goals, functions and major tasks to achieve goals, information required, output, and so on.

Technique	Description
	for the user to understand and can vary substantially in its level of detail and completeness. The preliminary task analysis traditionally specifies the jobs, duties, tasks, and actions that a person will be doing.
Functional analysis system technique (FAST)	This tool is used in the early stages of design to investigate system functions in a hierarchical format and to analyse and structure problems (e.g., in allocation of function). The aim of FAST is to understand how systems work and how cost effective modification can be incorporated. It asks 'how' sub-tasks link to tasks higher up the task hierarchy, and 'why' the super-ordinate tasks are dependent on the sub-tasks (Creasy, 1980; Kirwan and Ainsworth, 1992).
Functional failure analysis (FFA)	See functional hazard analysis
Functional failure path analysis	A method of determining the safety critical aspects of an implementation. A structured, top-down, iterative analysis which identifies functional paths and associated failures.
Functional hazard analysis (FHA)	A systematic, comprehensive examination of a system's functions to identify and classify failure conditions (conditions which the system can cause or contribute to, not only if it malfunctions or fails to function, but also in its normal response to unusual or abnormal external factors) of those functions according to their severity. The FHA provides a top-level analysis of the functions performed by the system and the risks presented by these functions following failure or misuse. These hazards produced by the system are categorised according to their level of severity. Potential effects on the aircraft or on crew workload determine each hazard's associated severity.
Gathered fault tree combination (DEK3)	Formalised extension of FMES (developed in France, used on Airbus and Concorde).

Advantages	Limitations
•	•
•	•
• Identifies functions and required design assurance levels for those functions. • Functional divisions may cut across system boundaries (multiple systems may contribute to the performance of more than one safety function). • Considers means of implementing functions. •	•
• Provides a systematic approach to the derivation of critical failure conditions. • Determines the scope and depth of further safety assessments. • Determines the integrity requirements of the function. • Predictive and target setting: determines the system's safety objectives without any architectural limitations. • Systematic and a good record. • Useful as primary mechanism in the identification of safety critical and safety involved failures of a system. • Highlights functional failures that affect another aircraft system (through interfaces/ dependencies/boundaries). • Improves understanding of how the design relates to safety. • Assists in limiting the scope of the safety assessment by determining the safety assessment requirements of the system. • Provides the FTA top events.	• Addresses only functional hazards. • May be disproportionately time consuming. The 'law of diminished returns' applies. Beware of taking the analysis too far by selecting the appropriate system level and assess the worst case conditions only. • The determination of the hazard severity level does not attempt to account for the system failures necessary for occurrence; it only seeks to determine the appropriate limits for probability of occurrence for a given hazard.
•	•

Technique	Description
Generic error modelling system (GEMS)	GEMS is an error classification model that is designed to provide insight as to why an operator may move between skill-based or automatic rule based behaviour and rule or knowledge-based diagnosis. Errors are categorised as slips/lapses (frequently skill-based errors) and mistakes (usually knowledge based errors). The result of GEMS is a taxonomy of error types that can be used to identify cognitive determinants in error sensitive environments. GEMS relies on the analyst either having insight to the tasks under scrutiny or the collaboration of a subject matter expert, and an appreciation of the psychological determinants of error.
Goals, operators, methods and systems (GOMS)	GOMS is a task modelling method to describe how operators interact with their systems. Goals and sub-goals are described in a hierarchy. Operations describe the perceptual, motor and cognitive acts required to complete the tasks. The methods describe the procedures expected to complete the tasks. The selection rules predict which method will be selected by the operator in completing the task in a given environment. GOMS is mainly used in addressing human-computer interaction and considers only sequential tasks.
Goal structured notation (GSN)	GSN is a graphical representation of an argument showing how it is to be accomplished. A convincing argument safety assessment/safety case requires three elements: • safety objective

Advantages	Limitations
•	•
• Assists in definition of human interface requirements at the earliest stages of design, so indirectly influences safety in this manner. • Can be used to model how skilled people will use a system (http://ei.cs.vt.edu/~cs5724/g2/) • Gives designers the ability to make quantitative predictions about skilled behaviour without having to train people (http://ei.cs.vt.edu/~cs5724/g2/) • Parameter-free estimates make the GOMS approach useful in design because it allows comparisons of different design alternatives. (http://ei.cs.vt.edu/~cs5724/g2/)	Not designed to be a safety assessment tool. Card *et al.* (1993) provided the most detailed list of the weaknesses of GOMS. The weaknesses are as follows: • The model applied to skilled users, not to beginners or intermediates. • The model does not account either for learning the system or its recall after a period of disuse. • Even skilled users occasionally make errors; however, the model does not account for errors. • Within skilled behaviour, the model is explicit about elementary perceptual and motor components. The cognitive processes in skilled behaviour are treated in a less distinguished fashion. • Mental workload is not addressed in the model. • The model does not address functionality. That is, the model does not address which tasks should be performed by the system. The model addresses only the usability of a task on a system. • Users experience fatigue while using a system. The model does not address the amount and kind of fatigue. • Individual differences among users is not accounted for in the model. • Guidance in predicting whether users will judge the system to be either useful or satisfying, or whether the system will be globally acceptable is not included in the model. • How computer-supported work fits or misfits office or organisational life is not addressed in the model.
• Improved comprehension of existing arguments. • Useful way to define safety assessment/case strategy. • Easy to read, even to a novice.	• Takes a lot of effort to develop the arguments. • Can easily go into too much complicated detail (e.g. sometimes it is more efficient to make the solution a separate

Technique	Description
	• supporting evidence • a clearly discernible 'thread' or argument that flows through the document. GSN shows show how goals ▭ are broken into sub-goals, and eventually supported by evidence (solutions) ○ whilst making clear the strategies ▱ adopted, the rationale for the approach (assumptions, justifications) ⬭ and the context ▢ in which goals are stated. The goal structuring notation (GSN) – a graphical argumentation notation – explicitly represents the individual elements of any safety argument (requirements, claims, evidence and context) and (perhaps more significantly) the relationships that exist between these elements (i.e. how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument). When the elements of the GSN are linked together in a network they are described as a 'goal structure'. The principal purpose of any goal structure is to show how goals (claims about the system) are successively broken down into sub-goals until a point is reached where claims can be supported by direct reference to available evidence (solutions). As part of this decomposition, using the GSN it is also possible to make clear the argument strategies adopted (e.g. adopting a quantitative or qualitative approach), the rationale for the approach and the context in which goals are stated (e.g. the system scope or the assumed operational role). Developed for use in safety cases by Tim Kelly, John McDermid (Department of Computer Science, University of York)
Hardware/software safety analysis	The analysis evaluates the interface between hardware and software to identify hazards within the interface (Tarrents, 1980).
Hazard analysis	A generic term describing a whole collection of techniques whose combined strengths have a good chance of revealing and evaluating/analysing hazards. A multi-use technique to identify hazards within any system, subsystem, operation, task or procedure (Tarrents, 1980). Also referred to as a system safety analysis (JAR 25.1309). Includes both top-down techniques oriented to tracing back from potential real-world hazards to the sources of failures which could lead to accidents, and bottom-up techniques which follow through hypothetical component failures to determine their hazardous consequences. (Strictly these are 'middle-out' because one also looks at how the component could come to fail.)
Hazard and Operability studies (HAZOPs) IEC 61882 DEF STAN 00-58	A team-based structured brainstorming technique for identification of hazards before they arise. HAZOP starts with a deviation from normal system operation and examines how that deviation might occur and the consequences should such a deviation occur.

Advantages	Limitations
• Presents logical argument to get from a goal to its logical solution (forces a logical argument). • Identifies holes in an argument. • Positively identifies assumptions. • Removes ambiguity (i.e. you have to define measurable goals). • Assists in managing programme risk (i.e. solution planning and prioritising). • Ease to audit. • Prevents duplication of solutions. • Prevents unnecessary work (e.g. if not required by a goal). • Defines scope of work, so assists in planning and budgeting. • Arguments can be re-used in another project.	compliance matrix rather than trying to argue compliance via GSN). • Arguments are always subjective, so every person will compile a GSN differently. • Can spend a lot of time agreeing an argument, so it may be more efficient to restrain GSN to a top-level argument only, i.e. do not repeat each finding which exists in tabular format (e.g. FHA). • Needs experience and skill. • Not as user friendly in hardcopy format, because complex GSN needs hyperlinks. •
•	•
Top-down techniques provide, in effect, a way of supporting lateral thinking about that most error-prone stage of development, the requirement specification.	Bottom-up techniques, like event tree analysis, can be very resource intensive because of the combinatorially explosive growth in consequences. A number of techniques are well established for electrical and electronic systems but there has been much debate as to how relevant these techniques are when applied to software.
• Wide-ranging, comprehensive and methodical. • Most useful if applied to continuous process systems (e.g. fluid and thermal systems). • Allows the members to brainstorm opinions and viewpoints using the experience from within their own fields of expertise.	• 6-8 people required, including the services of an experienced HAZOP team leader and minute taker. • Very lengthy to conduct. • Multi-disciplined team approach is expensive – must be shown to be cost-effective. • Guidewords can be hard to relate to. • Can produce lot of output.

HAZOP Guidewords

Guideword	Standard interpretations for chemical industry	Example interpretation for PES
no	no part of intention is achieved	no data or control signal passed
more	a quantitative increase	data is passed at a higher rate than intended
less	a quantitative decrease	not used here because this is already covered by 'part of'
as well as	all design intent achieved but with additional results	not used here because this already covered by 'more'
part of	only some of the intention is achieved	the data or control signals are incomplete
reverse	covers reverse flow in pipes and reverse chemical reactions	normally not relevant
other than	a result other than the original intention is achieved	the data or control signals are complete but incorrect
early	not used	the signals arrives too early with reference to clock time
late	not used	the signal arrives too late with reference to clock time
before	not used	the signal arrives earlier than intended within a sequence
after	not used	the signal arrives later than intended within a sequence

Technique	Description
	The purpose is to identify what variations from the intended design values (the 'design intent') could occur in the relevant attributes, and then to determine their possible causes and consequences. From their possible consequences, it is seen whether the deviations could cause hazards. The technique was developed by ICI in the 1960s and is well established in the petrochemical sector.
Hazard identification study (HAZID)	A structured brainstorming technique developed for the marine industry. Considers systems or equipments. Used by the International Maritime Organisation (IMO Paper MSC 69/INF 14 dd 98/2/12) for its safety assessments.
Hazard log (HL)	A management tool used to track the identification, mitigation and acceptance of risk and also the control of residual risks associated with the operation. Note that hazards are properties of an entire system and may be defined at any system level (see section 6.2). However, it is essential to select the right level so as to ensure consistency in the hazard log. – A common mistake is to select it too low, which results in too many hazards, no system properties, expensive (impossible) to track and over-engineering.

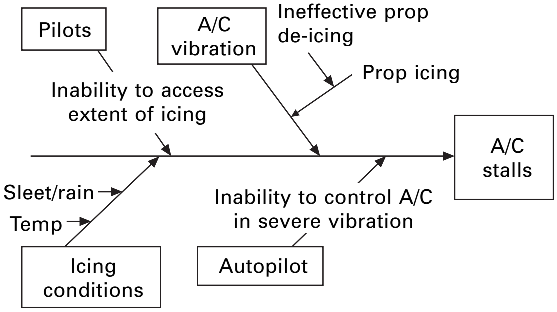
Advantages	Limitations
• Can be applied to each item/function/operation/process/procedure, etc.), but more effective if aimed at the very high-level operating system model. • 'Structured brainstorming' considers individual items and procedures, using a set of guide words as prompts. • Good at identifying operational failures. • Generates operating procedures. • Flexible to the system being analysed. • Useful for electronic systems (sending transit data). • Has both inductive and deductive phases. • The team approach brings a variety of expertise and viewpoints onto a common problem. • The discipline of focusing on hazard identification (rather than just looking for errors) leads to productive sessions and, gratifyingly, there is rarely a defensive approach by the system designers and users. The fact that a team is involved means that there is much less impact caused by a mistake by one team member, in contrast to other techniques that are carried out by individuals (Falla, 1997, Ch 3). • The presence on the team of key personnel associated with the system under analysis means that problem areas are brought immediately to their attention. Because the intent of the HAZOP is to identify hazards, not find errors, it is complementary to other activities of analysis and testing (Falla, Ch 3).	• More operability problems than hazards are usually found. • Requires specially trained team leader. • Requires thorough preparation before the meeting. • Variability is inherent in this approach. • More effective at higher system levels (e.g. FMECA is more effective at lower levels). •
• Similar to SWIFT and HAZOP, but more systematic.	
• A powerful management aid, when implemented on a user-friendly database, to focus on activities requiring action. • Useful for logging failures which are not attributable to equipment functionality (e.g. wind shear). • Hazards are properties (states) of an entire system and may be defined at any level. However, it is essential to select the right level. A common fault is to select it too low, which results in too	• Must be coupled to a logical decision process. • Needs to be rigorously followed up to be affective. • Duplicates information contained elsewhere (e.g. in FMEA and HAZOP). • Not a technique, only a management tool. • MoD intend it as a management tool for operational safety and continued airworthiness. In this instance it can only

Technique	Description
	– If selected too high, then it is hard to ensure the identification and management of all hazards.
Hazardous materials (HAZMAT) list	Not an assessment technique, but a list of hazardous materials contained in a product.
Health hazard analysis (HHA)	Identifies health hazards and recommends measures (e.g. such as ventilation and barriers) to reduce exposure to health hazards. See Mil Std 882C Task 207.
Health hazard assessment	The method is used to identify health hazards and risks associated within any system, sub-system, operation, task or procedure. The method evaluates routine, planned, or unplanned use and releases of hazardous materials or physical agents. The technique is applicable to all systems which transport, handle, transfer, use, or dispose of hazardous materials or physical agents (Tarrents, 1980).
Historical data & past experience	Use information from past experience and accident/incident reports of similar equipment as part of the hazard identification.
Human error analysis (HEA)	A method to evaluate the human interface and error potential within the human/system and to determine human error-related hazards. Contributory hazards are the result of unsafe acts such as errors in design, procedures, and tasks. Many techniques can be applied in this human factors evaluation (Tarrents, 1980).
Human error assessment and reduction technique (HEART)	HEART is an error quantification process that is quick to use. The process defines a set of generic error probabilities for the types of tasks being examined and identifies the error-producing conditions associated with them. For each of the error-producing conditions the human error probability is multiplied by the error-producing condition multiplier. The tool also provides some guidance on approaches towards error reduction. A human performance model-based technique utilising some standard probabilities. Data-based method to assess and reduce human error and improve operational performance.

Advantages	Limitations
many hazards, no system properties, expensive (impossible) to track and over-engineering. If selected too high, then it is hard to ensure complete management. • Provides warning information to those responsible for the handling, maintenance and disposal of materials.	be effective if all modifications on the platform use the same (predefined) safety criteria. • • Seldom provides guidance as to the events/actions needed to cause risk of hazardous exposure.
Should consider presence of toxic/inflammable/explosive materials, systemic poisons, asphyxiates or respiratory irritants, noise, vibration, shock (physical/electrical), heat/cold stress, radiation (ionised and non-ioninised), etc.	
•	•
• Cheap to obtain (where held in a consistent and usable format. • Scenarios are realistic. • Contains the lessons learned. • Feeds into all HA techniques (e.g. FHA, FMEA). • Useful for mature technologies (e.g. mechanical, hydraulic, etc.). • Validation can be made via good engineering judgement.	• Equipment analysed may be obsolete. • Does not address every potential hazard. • Can be difficult to obtain the 'real' causes from the data. • Not always readily available, especially for uncommon hazards. • Possibly different installation, operation, environmental exposure, etc. • Validations require good substantiation.
• Appropriate to evaluate any human/machine interface. • Good at analysing procedures or processes. • Good at identifying results of human error.	• Requires detailed procedural input.
• • Can assess significant sequences within a scenario. • Shows areas of vulnerability.	• • Time consuming. • Accuracy of quantification questionable.

Technique	Description
Human factors analysis	Human factors analysis represents an entire discipline that considers the human engineering aspects of design. There are many methods and techniques to formally and informally consider the human engineering interface of the system. There are special considerations such as ergonomics, bio-machines, anthropometrics. Human factors analysis is appropriate for all situations where the human interfaces with the system and human-related hazards and risks are present. The human is considered a main sub-system (Tarrents, 1980).
Human hazard analysis (HHA)	Examines the ease of use, the effects of error during use, task distribution, and the adequacy of feedback to the user in terms of the ability to recognise quickly if the desired result of the user's actions have not been achieved (*Flight International*, 11–17 Aug 1999, p3).
Human reliability analysis	The purpose of the human reliability analysis is to assess factors that may impact human reliability in the operation of the system. The analysis is appropriate where reliable human performance is necessary for the success of the human-machine systems (Tarrents, 1980). For more information, see *Guide to Practical Human Reliability Assessment*, Barry Kirwan, ISBN: 0748401113.
Incident reviews	These might be for the system itself or for similar systems used elsewhere.
Inductive analysis	Analysis which works forward from a given event (failure) to determine the possibility outcomes (e.g. see consequence analysis). It starts from known causes to forecast unknown effects. Inductive argument is where the argument is firmly based on the evidence presented, but extrapolates beyond the available evidence.
Installation appraisal	A qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.
Integrated performance modelling environment (IPME)	IPME is a Unix/Silicon Graphics based software tool providing a suite of tools to aid human factors practitioners in understanding human-system performance. IPME incorporates mission analysis, function analysis, function allocation, task analysis, and workload/ performance analysis and prediction. It is a tool that does require training in the use of the tool and can be time consuming to use in complex models.
Interface analysis	The analysis is used to identify hazards due to interface incompatibilities.

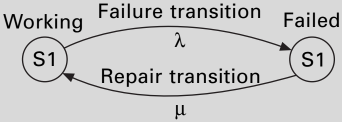
Advantages	Limitations
•	•
Human error remains a causal factor in the majority of serious aircraft accidents. Human error causes accidents of fail-safe, fully functional designs.	• Modelling of human performance and the quantification of human error probability are complex and time-consuming procedures, which require input from specialist industrial psychologists. • Does not identify action required to eliminate the danger.
•	•
• One of the best ways of identifying possible hazards is to look at previous accidents and incidents. • Valuable for the purpose of identifying that a particular hazard is possible.	• Often data-reporting systems are sketchy and this makes them imperfect for estimating rates of occurrence.
•	•
•	• An effective appraisal requires experienced judgement.
•	•
•	•

Technique	Description
	The methodology entails seeking those physical and functional incompatibilities between adjacent, interconnected, or interacting elements of a system which, if allowed to persist under all conditions of operation, would generate risks. Interface analysis is applicable to all systems. All interfaces should be investigated; machine-software, environment, human, environment-machine, human-human, machine-machine, etc. (Tarrents, 1980).
Ishikawa diagrams	Also called cause-and-effect or fishbone diagram. Problem of interest (e.g. hazard or accident) is entered at end of main, 'bone'. All possible causes are then 'fleshed out'.  Pilots A/C vibration Ineffective prop de-icing Prop icing Inability to access extent of icing A/C stalls Sleet/rain Temp Inability to control A/C in severe vibration Icing conditions Autopilot
Job safety analysis	This technique is used to assess the various ways a task may be performed so that the most efficient and appropriate way to do a task is selected. Job safety analysis can be applied to evaluate any job, task, human function, or operation. Each job is broken down into tasks, or steps, and hazards associated with each task or step are identified. Controls are then defined to decrease the risk associated with the particular hazards (Tarrents, 1980).
Justification of human error data information (JHEDI)	JHEDI is derived from the human reliability management system (HMRS) and is a quick form of human reliability analysis that requires little training to apply. The tool consists of a scenario description, task analysis, human error identification, a quantification process, and performance shaping factors and assumptions. JEDHI is a moderate, flexible and auditable tool for use in human reliability analysis. Some expert knowledge of the system under scrutiny is required.
Key issues tool (KIT)	KIT is a software tool designed to support the EHFA (early human factors analysis). It makes the EHFA process easier by providing structure and supporting the difficult aspects of tracking and linking many items. The output from KIT acts as an input to a project's overall risk register, allowing the project manager to see the human factors integration (HFI) risks in a manner which is comparable to other areas of project risk. The tool provides a full record of the analysis conducted on any issue over the life of a project.

Advantages	Limitations
• Identify all possible contributory causes to an accident. • Good at evaluating events if causes + event are known.	• Practical maximum depth is usually about four or five levels. • Not good at drawing out causes vs. events. • Not necessarily time ordered (but can be if first event is on far left and last event on right).
•	•
•	•

Technique	Description
Laser safety analysis	This analysis enables the evaluation of the use of lasers from a safety view. The analysis is appropriate for any laser operation, i.e., construction, experimentation, and testing (Tarrents, 1980).
Layer of protection analysis (LOPA)	Used for SIL determination. Is a relatively new method, developed by the American Institute of Chemical Engineers (CCPS) group in response to the requirements of ISA S84.01 and was formally published in 2001. It effectively combines a number of different techniques into a composite method that is well tailored to assessing process risks and development of hazardous scenarios. As indicated by its name, it involves assessing layers of protection other than just the instrument protective functions. For instance, a contribution toward risk reduction by independent protective layers (IPLs) such as 'alarms and operators' or 'basic process control' is explicitly defined as a risk reduction factor. The combination of the risk reduction factors for all IPLs provides the total risk reduction possible. It is fundamentally a simplified quantitative method that considers the risk reduction contributed from each IPL typically by order of magnitude risk reduction (i.e., say 0.1 for a DCS, or 0.01 for a relief valve, etc.). (Kirkwood D., *Current issues with SIL assessment methods*, Functional Safety Professional Network, Technical Advisory Panel, david.kirkwood@rtel.com)
Life data analysis	See Weibull Analysis
Maintenance error decision aid (MEDA)	Boeing has invested decades of research in maintenance error. It has developed a widely used maintenance error decision aid (MEDA) which is an attempt to systematise evaluation of events, problems and potential problems by using a repeatable, structured evaluation programme. The company has been encouraging its customers to employ the technique.
Management oversight and risk tree (MORT)	MORT technique is used to systematically analyse an accident in order to examine and determine detailed information about the process and accident contributors. This is an accident investigation technique that can be applied to analyse any accident (Tarrents, 1980).

Advantages	Limitations
•	•
• A defined and obvious procedural approach that guides the user to consider a range of factors that contribute to risk reduction. • It is more intuitive than quantitative analysis (for most people involved in the exercise). • It is aligned with assessing the development of hazardous scenarios and consequently provides an additional dimension to the assessment process. • It is also aligned with the assessment process required for mitigation systems. In general, it is quicker than quantitative analysis techniques. • Provides the capability of accounting for risk reduction factors at a finer level than risk graph assessments. • Consider the issue of an alarm to an operator. • Risk graphs provide the user with a digital choice of Pa or Pb with a resultant step of one SIL rating in the result. LOPA however provides a more graduated approach, allowing the user to select an intermediate value with an incremental effect on the final result.	• The disadvantage of the LOPA method is the additional time and effort required to conduct the exercise if environmental impact and asset protection are also considered. • The reliability and safety data on which the exercise relies is often defined subjectively (e.g. consider the contributing factor for a basic control system). There may be a strong temptation for users to simply enter 0.1 for the risk reduction provided by the system without considering the actual performance of the system further and taking into account factors that may change this result. If this is repeated for several IPLs then misleading results could occur. The reliability of elements such as valves and transmitters ultimately depends on their service conditions; it is well understood in industry that reliability is very dependent on environmental factors and the degree of wear and tear of elements. • There is also a potential danger with LOPA that we assume a false degree of accuracy in the results because numerical values are assigned to the elements of the calculation. • LOPA is also slower than typical risk graph techniques and therefore assessing a large number of safety functions could prove prohibitive.
• •	• •
•	•

<table>
<tr><th>Technique</th><th>Description</th></tr>
<tr><td>Man-machine integration design and analysis systems (MIDAS)</td><td>MIDAS is a silicon graphics software tool designed to aid the application of human factors principles and performance models to the design of complex systems. It is intended for use at the earliest stages of the design process and consequently is likely to reduce some of the costs of simulation and prototyping. MIDAS describes a system's operating environment and procedures, and incorporates human performance models into the design process.</td></tr>
<tr><td>Markov analysis (MA)</td><td>Similar to the DD and FTA, but it additionally calculates the probability of the system being in various states as a function of time. Here airworthiness is not a simple mathematical calculation, but depends on relative states of parts of the system.
Provides a means for analysing reliability/availability of systems whose components exhibit strong dependencies.
The <i>Encyclopaedia Britannica</i> defines the Markov process as 'A sequence of possible dependent random variables (x_1, x_2, x_3,...) – identified by increasing values of a parameter, commonly time – with the property that any prediction of the value x_n, knowing the value x_1, $x_2....x_{n-1}$, may be based on x_{n-1} alone. That is, the future value of the variable depends upon the present value and not the sequence of past values'.
See SAE ARP4761
Step 1: Begin State 1 with full functionality.
Step 2: Study consequences of each failure.
Group LRU failures.
Allows transition between two states to occur with specific distributions:


Step 3: Assign failure states for unique consequences of phase 2.
Step 4: Connect arrows between states and add failure rate(s) of each.
Step 5: Repeat Step 2 to 4 for each state.
Step 6: Continue until equipment is totally unserviceable.</td></tr>
<tr><td>Master plan logic diagram (MPLD)</td><td>An outgrowth of the master logic diagram to represent all the physical interrelationships among various plant systems and subsystems in a simple logic diagram. It is used for probabilistic assessments to model and integrate the relationship between all plant functions and equipment (Mauri, 2000).</td></tr>
<tr><td>Materials compatibility analysis</td><td>Provides an assessment of materials utilised within a particular design.
Any potential degradation that can occur due to material incompatibility is evaluated.
Materials compatibility analysis in universally appropriate throughout most systems (Tarrents, 1980).</td></tr>
<tr><td>Maximum credible accident/worst case</td><td>The technique is to determine the upper bounds of a potential environment without regard to the probability of occurrence of the particular potential accident.
Similar to scenario analysis, this technique is used to conduct a system hazard analysis.
The technique is universally appropriate (Tarrents, 1980).</td></tr>
</table>

Advantages	Limitations
•	•
• Provides great flexibility in modelling the timing of events. • Considers transient effects (e.g. shift in centre of gravity due to fuel displacement) • Useful when dealing with deferred maintenance scenarios. • Useful in multi-channel systems where certain failures may be tolerated but not in conjunction with some failure conditions. • Allows modelling of common cause failures. • Allows modelling of failure characteristics of mixed H/W and S/W systems. • Useful for systems where a number of interrelated states may be valid (i.e. when airworthiness depends upon the relative states of parts of the system). • Establishes crew and maintenance tasks and intervals needed to meet the safety objectives. • S/W errors can be qualitatively represented. • Unlike other methods, this does not assume component independence.	• Most expensive reliability and system model. • Assumes constant failure rate and constant repair rate. For other distributions (e.g. Weibull failure rate processes or fixed repair times) Monte Carlo simulation methods are more appropriate.
• Represents the interrelationships amongst various components and can model relationships between functions and systems (Mauri, 2000). • Generates and quantifies accident sequences (Mauri, 2000).	• Does not allow the mapping of couplings which originate common cause failures (Mauri, 2000).
•	•
•	•

Technique	Description
Micro-Saint	Micro-Saint is a discrete-event task network-modelling tool that can be described by flow diagrams and can be analysed to test, for example, alternative solutions or options, assess workload, function allocation, and temporal analysis (albeit based on time estimates). The analysis process requires input from subject matter experts on the task under investigation, training and familiarity with using the tool, and it can be difficult and time consuming to use.
MIL-HDBK-217	'*Reliability Prediction of Electronic Equipment*' – even though this handbook is no longer being kept up to date by the US military, it remains the most widely used approach by both commercial and military analysts. MIL-HDBK-217 has been the mainstay of reliability predictions for about 40 years but it has not been updated since 1995, and there are no plans by the military to update it in the future. For more than ten years Quanterion's Seymour Morris was DoD program manager for MIL-HDBK-217. The handbook includes a series of empirical failure rate models developed using historical piece part failure data for a wide array of component types. There are models for virtually all electrical/electronic parts and a number of electromechanical parts as well. All models predict reliability in terms of failures per million operating hours and assume an exponential distribution (constant failure rate), which allows the addition of failure rates to determine higher assembly reliability. The handbook contains two prediction approaches, the parts stress technique and the parts count technique, and covers 14 separate operational environments, such as ground fixed, airborne inhabited, etc. • As the names imply, the parts stress technique requires knowledge of the stress levels on each part to determine its failure rate. • The parts count technique assumes average stress levels as a means of providing an early design estimate of the failure rate. Typical factors used in determining a part's failure rate include a temperature factor (π_T), power factor (π_p), power stress factor (π_S), quality factor (π_Q) and environmental factor (π_p) in addition to the base failure rate λ_b. For example, the model for a resistor is as follows: $\lambda_{Resistor} = \lambda_b\ \pi_T\pi_P\pi_S\pi_Q\pi_E$.
Modelling/ simulation	There are many forms of modelling techniques that are used in system engineering. Failures, events, flows, functions, energy forms, random variables, hardware configuration, accident sequences, operational tasks, all can be modelled (Tarrents, 1980).
Modified Cooper-Harper scale	Human factors evaluative tool.
Modified pilot subjective evaluation (MPSE)	Human factors evaluative tool. Features custom modifications of the PSE which permit it to be adapted as necessary to meet the specific requirements of a certification while retaining the proven elements of the PSE.

Advantages	Limitations
•	•
• Even though MIL-HDBK-217 is becoming more obsolete every day, it remains the most widely used technique for electronics.	•
• Modelling is appropriate for any system or system safety analysis.	•
• Subjective in terms of safety implications.	• Subjective.
• Subjective in terms of safety implications.	•

Technique	Description
Monte-Carlo analysis (as used by FAA for fuel tank safety assessments)	Analytical method to determine flammability exposure time of a fuel tank. The percentage fleet flammability exposure result can be used to determine if the fuel tanks exist in a flammable state for a long period of time, thereby requiring more rigorous analysis in the SSA. Spreadsheet that simulates uncertain parameters by randomly selecting values from distribution tables. The calculation is performed repetitively and averaged to approximate real conditions.
NASA-task load index	Human factors evaluative tool.
Network logic analysis	A method to examine a system in terms of mathematical representation in order to gain insight into a system that might not ordinarily be achieved. The technique is universally appropriate to complex systems (Tarrents, 1980).
NPRD-95	The nonelectronic parts reliability data (NPRD-95) databook is a widely used data book published by the Reliability Analysis Center that provides a compendium of historical field failure rate data on a wide array of mechanical assemblies. The document provides detailed failure rate data on over 25,000 parts for numerous part categories grouped by environment and quality level. Because the data does not include time-to-failure, the document is forced to report average failure rates to account for both defects and wearout. Cumulatively, the database represents approximately 2.5 trillion part hours and 387,000 failures accumulated from the early 1970s through 1994. The environments addressed include the same ones covered by MIL-HDBK-217; however, data is often very limited for some environments and specific part types. For these cases, it then becomes necessary to use the 'rolled up' estimates provided, which make use of all data available for a broader class of parts and environments. Although the data book approach is generally thought to be less desirable, it remains an economical means of estimating 'ballpark' reliability for mechanical components.
NSWC-94/L07	*Handbook of Reliability Prediction Procedures for Mechanical Equipment* developed by the Naval Surface Warfare Center – Carderock Division. This handbook presents a unique approach for prediction of mechanical component reliability by presenting failure rate models for fundamental classes of mechanical components. Examples of the specific mechanical devices addressed by the document include belts, springs, bearings, seals, brakes, slider-crank mechanisms and clutches. Failure rate models include factors that are known to impact the reliability of the components. For example, the most common failure modes for springs are fracture due to fatigue and excessive load stress relaxation. The reliability of a spring will therefore depend on the material, design characteristics and the operating environment. NSWC-94/L07 models attempt to predict spring reliability based on these input characteristics.

Advantages	Limitations
• Analytical, repeatable results to replace traditional argument.	• Very dependent on input parameters and can produce results without the user understanding the process, increasing the likelihood of false results. • Restricted input data limits applicability, requiring several scenarios to be considered. • Dependent on fuel flash point and LEL values which are dependent on tank characteristics (which are not modelled).
• Subjective in terms of safety implications.	• Subjective.
•	•
For mechanical components, NPRD-95 is the most widely used.	
• For mechanical components, NSWC-94/L07 offers a more accurate alternative than NPRD-95 if the required detailed input data is available and manufacturing defects can be ignored.	• The drawback of the approach is that, like the physics of failure models for electronics, the models require a significant amount of detailed input data (e.g., material properties, applied forces, etc.) that is often not readily available. • Does not address the issue of manufacturing defects.

Technique	Description
Occupational health hazard analysis (OHHA)	Identifies health hazards and recommends provisions such as ventilation, barriers, protective clothing, etc.
Operability analysis	The aim of carrying out operability analysis is to highlight any issues that have a bearing on the operability of a system/equipment. An operability analysis should be designed for operation in the simplest and easiest way possible. Carrying out an operability analysis involves the following: • task analysis • Workload analysis • human reliability analysis • taking due account of the prevailing environmental conditions. Effort invested in the operability analysis will vary with the criticality of the equipment, its interfaces and interactions with other equipment. Therefore the scope of operability assessments can be restricted to a single task or cover a range of tasks. Methods include: • Anthropometrical studies can be used to provide known physical data on the population to assess workplace layout and architecture. • Rapid prototype modelling permits varied configurations to be tested over comparatively short timescales. This technique permits feedback from subject matter experts to be incorporated into the model, and assessed promptly, before possible inclusion into the design. • Task analysis involves a study of the workforce (operators) to ascertain what is required to achieve the system goals. This allows comparison between the task demands and the operators' capabilities. • Workload analysis is an analysis of the demand placed on the operator by the task requirements. • Human reliability analysis recognises the critical area where human error may affect performance. • Operational scenario analysis is an analysis that the activities required to be undertaken, can be successfully completed using the manpower and facilities provided for the purpose.
Operating and support hazard analysis (OSHA)	The analysis is performed to identify and evaluate hazards/risks associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system (Tarrents, 1980). Evaluates hazardous operating, maintenance and support tasks by systematically evaluating each phase of operation and support. Can be divided into two separate analyses: • The operating hazard analysis • The support hazard analysis.
Pareto analysis	A ranking technique based only on past data that identifies the most important items among many. Uses the 80-20 rule, which states that about 80% of the problems are caused by about 20% of the causes.

Advantages	Limitations
• Logical model of a system is repeatedly exercised, each run uses different values of the distributed parameters. • Can be used for system dependability modelling.	• Very expensive in computer time.
An operability analysis will: • Highlight possible operability problems early in the design phase. • Provide the means to remove operability problems from the design. • Instill confidence in the finalised design. • Provide a demonstration of the operability of new and/or modified systems.	•
• Identifies the nature and duration of actions that occur under hazardous conditions.	• Requires input from experienced operators/maintainers.
• Can be used for any type of system, process, or activity as long as enough historical data are available. • Identifies the most important risk contributor so that more detailed risk assessment can be performed later.	•

Technique	Description
Particular risk assessment (PRA)	A form of CCA. Technology or circumstance dependent analysis which considers common events or influences that are outside the system(s) concerned (e.g. fire, lighting) which may violate failure independence claims. Some of these risks may also be the subject of specific airworthiness requirements. PRA examines common events that are external to the systems concerned, but which may violate independence requirements (e.g. uncontained engine rotor failure; fire; bird strike; lightning; HIRF; human factors, etc.). (e.g. damage may result in multiple systems failing; incorrect pilot response could lead to a hazardous flying condition). Each risk is then examined to assess any simultaneous or cascading effects of each risk.
Petri net analysis	Petri net analysis is a method to model unique states of a complex system. Petri Nets can be used to model system components, or subsystems at a wide range of abstraction levels; e.g., conceptual, topdown, detail design, or actual implementations of hardware, software, or combinations (Tarrents, 1980).
Physics-of-failure	This family of approaches differs significantly from the other empirical reliability prediction methodologies and is used primarily at the sub-device level during the design stage. Physics-of-failure approaches attempt to identify the 'weakest link' of a design to ensure that the required equipment life is exceeded by the design. The methodology generally ignores the issue of defects escaping from the manufacturing process and assumes that product reliability is strictly governed by the predicted life of the weakest link. Example models address microcircuit die attach fatigue, bond wire flexure fatigue and die fatigue cracking. The models are very complex and require detailed device geometry information and materials properties. In general, the models are thought to be most useful in the early stages of designing devices (e.g., hybrids) but not at the assembly level when flexibility no longer exists to change device designs.
Pilot subjective evaluation (PSE	Human factors evaluative tool.

Advantages	Limitations
• Allows effects of non-related systems on each other to be evaluated. • May address several zones at the same time. • Typical risks include fire, high energy devices, leaking fluids, hail, ice, snow, birdstrike, tread separation from tyre, wheel rim release, lightning, HIRF, etc.	• Best done at a late design stage to ensure complete picture. • May involve complex calculations or simulation (e.g. trajectories of debris after fan/tyre burst. • Only identifies the risks with respect to the design under consideration, each applicable risk should then be subject to a specific study to examine and document the simultaneous or cascading effect(s) of each risk.
•	•
•	•
• Subjective in terms of safety implications. • Accepted as a means of compliance by the FAA. Requires only limited training since it uses a comparison methodology. This makes it possible for a broad range of operational pilots with both domestic and international experience to participate in an assessment.	• Subjective. • The PSE's major shortcoming is in the data analysis. A large sample population having reference aircraft experience would be required to achieve statistical confidence. Consideration of age/rank, 'seat' experience, and type of aircraft flown expand the sample matrix dramatically. However, the FAA does not require a statistical approach but rather looks for human performance trends and a detailed explanation for any outliers in the data. Such outliers which cannot be resolved by any other means are usually corrected with 'more training'. Unfortunately, the result is that training once again becomes a primary method to mitigate poor or inadequate design.

Technique	Description
PRISM	PRISM is a new technique (released in 2000 based on the Reliability Analysis Centre's databases) which has the ability to model the effects of thermal cycling and dormancy. It provides the ability to update predictions based on test data and addresses factors such as development process robustness. Available as an automated tool (as opposed to a handbook compendium of models like the others), PRISM interfaces directly with RAC's electronic and nonelectronic automated databases and provides an elaborate methodology to assess the quality of the system development process. It includes a means to include software reliability but is limited by the fact that it does not yet include models for all commonly used devices. The PRISM system reliability model is: $\lambda_S = \lambda_{IA}(\pi_P\pi_{IM}\pi_E + \pi_D\pi_G + \pi_M\pi_{IM} + \pi_E\pi_G + \pi_S\pi_G + \pi_I\pi_E + \pi_N + \pi_W\pi_E) + \lambda_{SW}$, where λ_{IA} is the initial assessment failure rate (based on 'RACRates' component failure rate models incorporated into PRISM) for the system based on its parts and the remaining factors address parts processes (π_P), infant mortality (π_{IM}), environment (π_E), design processes (π_D), reliability growth (π_G), manufacturing processes (π_M), system management processes (π_S), induced processes (π_I), no-defect processes (π_N), and wear-out processes (π_W). λ_{SW} is the software failure rate. Quantitative values for the individual factors are determined through an extensive question and answer process intended to benchmark the extent that measures known to enhance reliability are used in design, manufacturing and management processes.
Procedural event analysis tool (PEAT)	PEAT is a structured, cognitively based analytic tool designed to help airline safety officers investigate and analyse serious incidents involving flight-crew procedural deviations. The objective of PEAT is to help airlines develop effective remedial measures to prevent the occurrence of future similar errors. The PEAT process relies on a non-punitive approach to identify key contributing factors to crew decisions. Using this process, the airline safety officer would be able to provide recommendations aimed at controlling the effect of contributing factors. PEAT includes database storage, analysis, and reporting capabilities.
Procedure analysis	Procedure analysis is a step-by-step analysis of specific procedures to identify hazards or risks associated with procedures. The technique is universally appropriate (Tarrents, 1980).
Production system hazard analysis	Production system hazard analysis is used to identify hazards that may be introduced during the production phase of system development which could impair safety and to identify their means of control. The interface between the product and the production process is examined. The technique is appropriate during development and production of complex systems and complex subsystems (Tarrents, 1980).
Prototype development	Prototype development provides a modelling/simulation analysis of the constructors' early pre-production products so that the developer may inspect and test an early version. This technique is appropriate during the early phases of pre-production and test.

Advantages	Limitations
• Provides improved modelling capability compared to MIL-HDBK-217. •	• At this time it is rather limited from a device coverage standpoint but it shows potential for community acceptance as it matures. • Will need to be expanded to include more part categories, and further evaluated by industry prior to widespread adoption.
•	•
•	•
•	•
•	•

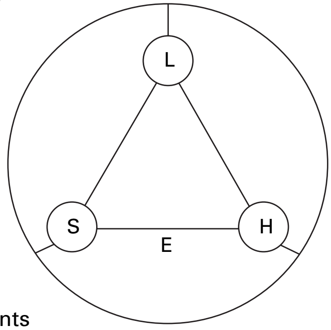
Technique	Description
Qualitative assessment	A collective term for the various methods of assessing causes, severities, and likelihood of potential failure conditions. Typical types of analysis include design appraisal, installation appraisal, FMEA, FTA, DD, reliability block diagrams, etc.
Quantitative assessment	A collective term for the various analyses (such as failure modes and effects, fault tree, or dependence diagram) which also includes numerical probability information. The probabilities of primary failures can be determined from failure rate data and exposure times, using failure rates derived from service experience on identical or similar items, or acceptable industry standards. The conventional mathematics of probability can then be used to calculate the estimated probability of each failure condition as a function of the estimated probabilities of its identified contributory failures or other events. Often used for hazardous or catastrophic failure conditions of systems that are complex, that have insufficient service experience to help substantiate their safety, or that have attributes that differ significantly from those of conventional systems. Quantitative probability terms are usually expressed in terms of acceptable numerical probability ranges for each flight hour, based on a flight of mean duration for the aeroplane type (however, for a function which is used only during a specific flight operation, e.g., take-off, landing, etc., the acceptable probability should be based on, and expressed in terms of, the flight operation's actual duration). a. Probable failure conditions are those having a probability greater than of the order of 1×10^{-5}. b. Improbable failure conditions are divided into two categories as follows: (i) Improbable (remote) failure conditions are those having a probability order of 1×10^{-5} or less but greater than of the order of 1×10^{-7}. (ii) Improbable (extremely remote) failure conditions are those having a probability of the order of 1×10^{-7} or less, but greater than of the order of 1×10^{-9}. c. Extremely improbable failure conditions are those having a probability of the order of 1×10^{-9} or less.
RDF 2000	This is the latest and most comprehensive of the European methodologies developed by CNET. It has not yet received much attention in the US but it could evolve into the new international standard should MIL-HDBK-217 continue to become outdated. Like the PRISM approach, it also addresses thermal cycling and dormant system modelling. RDF 2000 is the new version of the CNET UTEC80810 reliability prediction standard that covers most of the same components as MIL-HDBK-217. The models take into account power on/off cycling as well as temperature cycling and are very complex with predictions for integrated circuits requiring information on equipment outside ambient and print circuit ambient temperatures, type of technology, number of transistors, year of manufacture, junction temperature, working time ratio, storage time ratio, thermal

Advantages	Limitations
• Supports experienced engineering and operational judgement.	• Not all of these methods are structured.
• Used to compare the achieved reliability with the reliability target. If the target is not satisfied, then the design is adapted until it is met.	• It is recognised that, for various reasons, component failure rate data are not precise enough to enable accurate estimates of the probabilities of failure conditions. This results in some degree of uncertainty, as indicated by the expression 'of the order of'. When calculating the estimated probability of each failure condition, this uncertainty should be accounted for in a way that does not compromise safety.

• As this standard becomes more widely used it could become the international successor to the US MIL-HDBK-217.	•

Technique	Description
	expansion characteristics, number of thermal cycles, thermal amplitude of variation, application of the device, as well as per transistor, technology related and package related base failure rates.
Reliability analysis	A full review of the reliability of an aircraft part or component, making use of past data to determine the reliability of a component or maintenance technique.
Reliability block diagram	A graphical means of representing which set of correctly working components may combine to provide the system function. Constructed of blocks and connections representing devices in provision of a function.
Repertory grid analysis	Based in clinical psychology and personality theory, repertory grid analysis is a structured and theoretical form of interview method. Subjects group concepts and justify how the groups are similar and dissimilar. Although a simple technique it does require some familiarity for effective application.
Risk-based decision analysis	An efficient approach to making rational and defensible decisions in complex situations (Tarrents, 1980).
Root cause analysis	This method identifies causal factors to accident or near-miss incidents. The root causes are the underlying contributing causes for observed deficiencies that should be documented in the findings of an investigation (Tarrents, 1980). Root causes are the most basic causes of an event that meet the following conditions: • they can be reasonably identified • management has the ability to fix or influence them. Typically, root causes are the absence, neglect, or deficiencies of management systems that control human actions and equipment performance. Root cause analysis provides a means to determine how and why something occurred. Understanding the accident scenario is not enough. Scenarios tell us what happened, not why it happened. Events in accident scenarios are generally only symptoms of underlying problems in the administrative controls that are supposed to keep those events from occurring. Understanding only the scenario addresses the outward symptoms, but not the underlying problems. More investigation of the underlying problems is needed to find and correct those that will contribute to future accidents.
Safety review	Assesses a system, identify facility conditions, or evaluate operator procedures for hazards in design, the operations, or the associated maintenance. Periodic inspections of a system, operation, procedure, or process

Advantages	Limitations
• Uses factual information. • Highlights areas which need improvement. • Focuses resources. • Feeds into FMEA.	• Many variables may underlie the data used. • Data on failure modes may be out of date. • Not applicable to new products.
• Establishes reliability/availability goals. • Identified design problems and assists in trade-off studies of alternative designs. • Can include failure probability calculations. • Assists in identifying the interdependencies (e.g. for FTA and FMEA).	• Block failures need to be independent of each other.
•	
•	•
• Useful for accident/incident analyses. • Goes beyond the direct causes to identify fundamental reasons for the fault or failure. • Root cause analysis provides a means to investigate underlying problems. • Facilitates understanding of how an accident event occurred by discovering the underlying root causes (management system weaknesses) of the key contributors (causal factors). • Developing and implementing practical and effective recommendations for preventing future accidents.	•
•	•

Technique	Description
	are a valuable way to determine their safety integrity. A safety review might be conducted after a significant or catastrophic event has occurred (Tarrents, 1980).
Scenario analysis	Scenario analysis identifies and corrects hazardous situations by postulating accident scenarios where credible and physically logical scenarios provide a conduit for brainstorming or to test a theory where actual implementation could have catastrophic results. Where system features are novel, subsequently, no historical data is available for guidance or comparison, a scenario analysis may provide insight (Tarrents, 1980).
Scenario-based requirements analysis (SCRAM)	An iterative scenario-based technique based on a mixture of creative and systematic processes. Question probes: What could go wrong at the next step? Influencing factors: What is likely to make things go wrong at the next step? Consider design defence: How could the error/fault be prevented?
SHEL model	An illustration of the interrelationships between the three types of system resource and their environment • S = software (i.e. rules, regulations, SOPs, customs, habits, etc. • H = hardware (i.e. physical assets) • E = environment (i.e. physical, political, social, economic) • L = liveware (i.e. people).  The usual, interfaces: • L–H interface: the interaction between man and the machine (i.e. ergonomics) is probably the cause of most catastrophic accidents. • L–S interface: considers the interaction of human characteristics with the requirements of the rules, procedures, etc. • L–E interface: considers how the human can cope in extreme conditions. Model can be extended to be 3D: • H–H interface (e.g. plug and play devices) • S–S interface (e.g. consistency of company operating procedures) • L–L interface (e.g. command and control).
Single function diagram (SFD)	Shows schematically how a specific function is normally produced.
Single-point failure analysis	This technique is to identify those failures that would produce a catastrophic event in items of injury or monetary loss if they were to occur by themselves. This approach is applicable to hardware systems, software systems, and formalised human operator systems (Tarrents, 1980).

Advantages	Limitations
•	•
• Good for imagining possible events (i.e. works through expected problems. • Good at evaluating human operational effectiveness. • Builds on existing practice (e.g. HAZOP, FMEA, etc.) but adds another layer of analysis. • • Useful to illustrate how any changes in a single resource may have an impact on the system's integrity (e.g. change of H requires adaptation of S and L).	• How many scenarios are enough? • How is the 'right' scenario to be found? • Law of diminishing returns applies (i.e. can continue safety analysis indefinitely but at what cost).
▪ Provides the functional and timing relationships between the H/W, operator actions and S/W.	▪ Does not consider malfunction situations in any way.
•	▪

Technique	Description
Sneak analysis (or sneak circuit analysis)	Looks for unintended paths (flows) within an electrical system. A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system, coded into the software program, or triggered by human error. The traditional approach to sneak circuit analysis is manually to dissect the schematic drawings and transform them into structures called network trees. Sneak clues are then applied to these trees. SNA can be performed using the sneak circuit analysis tool (SCAT), a PC-based software package, and CapFast, an electrical circuit design and schematic editing tool. SCAT integrates with the schematic design package, CapFast. Original version was Sneak Circuit Analysis, devised after Mercury Redstone rocket launch accident (1961). See DEF STAN 00-41 and Mil-Std-1543.
Software failure modes and effects analysis	This technique identifies software-related design deficiencies through analysis of process flow-charting. It also identifies areas for verification/validation and test evaluation (Tarrents, 1980).
Software fault tree analysis	This technique is employed to identify the root cause(s) of a 'top' undesired event. To assure adequate protection of safety critical functions by inhibiting interlocks, and/or hardware (Tarrents, 1980).
Software hazard analysis	The purpose of this technique is to identify, evaluate, and eliminate or mitigate software hazards by means of a structured analytical approach that is integrated into the software development process.
Software hazard analysis and resolution in design (SHARD)	Very HAZOP like, but with different keywords (i.e. early, late, omission, commission and value). Developed by the University of York.
Software sneak circuit analysis	Software sneak circuit analysis (SSCA) is designed to discover program logic that could cause undesired program outputs or inhibits, or concepts sequencing/timing (Tarrents, 1980)
Standard ergonomics assessment methodology (SEAM)	One of the largest human factors teams in the UK, part of Qinetiq's Centre for Human Sciences, has been presented with the Ergonomics Society's 2004 award for Human Factors Integration, sponsored by Thales. In making the award, the Society recognised the importance of the team's development of a software tool (SEAM), which they used to

Advantages	Limitations
• Particularly useful for analysis of electronic system diagrams. • Can also be used for sneak paths caused by H/W, S/W, operator, etc. • Sneaks are latent and are as a result of a failure, so cannot be analysed by FTA, FMEVA, etc. • This technique is applicable to control and energy-delivery delivery circuits of all kinds, whether electronic/electrical, pneumatic, or hydraulic (Tarrents, 1980).	This process is quite expensive and is often limited to highly critical (from the safety viewpoint) systems.
• This methodology can be used for any software process; however, application to software controlled hardware systems is the predominant application. • It can be used to analyse control, sequencing, timing monitoring, and the ability to take a system from an unsafe to a safe condition. •	•
• Any software process at any level of development or change can be analysed deductively. However, the predominant application is software controlled hardware systems.	•
• This practice is universally appropriate to software systems.	•
•	•
• The technique is universally appropriate to any software program.	•
• The software tool was designed for use by all members of the team irrespective of experience and assisted them with data collection, data storage and report writing. • Helps them make rigorous and consistent ergonomic assessments of the system.	•

Technique	Description
	make ergonomic assessments on the Bowman tactical communications system – one of the largest change programmes ever undertaken by the British Army, which will transform the Army's land vehicle and infantry communications. The Qinetiq team was tasked by the Defence Procurement Agency to assess Bowman at five key design stages. SEAM (standard ergonomics assessment methodology) helped them to make rigorous and consistent ergonomic assessments of the system. The software tool was designed for use by all members of the team irrespective of experience. It assisted them with data collection, data storage and report writing and will now be used for other military and civilian projects.
Static source code analysis	The process by which software developers check their code for problems and inconsistencies before compiling. Organisations can automate the source code analysis process by implementing a tool that automatically analyses the entire program, generates charts and reports that graphically present the analysis results, and recommends potential resolutions to identified problems. Static analysis tools scan the source code and automatically detect errors that typically pass through compilers and become latent problems, including the following: • syntax • unreachable code • unconditional branches into loops • undeclared variables • uninitialised variables • parameter type mismatches • uncalled functions and procedures • variables used before initialisation • non-usage of function results • possible array bound errors • misuse of pointers.

Advantages	Limitations
•	• Restricts language choices that may be used and the choice of the structures used within these languages. • Require highly skilled and experienced staff to carry out the tests and analyse the results. • It is not a complete answer for the validation and verification of safety-critical software even with the use of automated tools. Other forms of testing (for example dynamic) are required to verify certain aspects, like executing critical features. • Multitask applications software must be analysed a task at a time. Another form of testing is required to check task interactions. • Dynamic aspects of the software (for example, sequences of program execution) are difficult to model with static analysis techniques. • Most automated tools require translation to an intermediate language before they can analyse the code. Automatic translators are available for some languages, but for others one must either translate manually or write a new translator. Some language features do not have an equivalent in the intermediate language even with the automatic translators; they must be manually translated. The static analysis of the software depends on its translation model and the more skilled the analyst, the more skilled the model produced. The validation of the intermediate language model needs to be considered, as this can be a major problem. • Expensive means of validation of done too late in the development process • Most anomalies identified have no safety implications.

Technique	Description
Statistical distributions	When carrying out the tasks assigned to it, the 'output' of a system can be expressed as a statistical distribution which describes the probabilities that the system output will reach or exceed any particular values.
Structural safety analysis	This method is used to validate mechanical structures. Inadequate structural assessment results in increased risk due to potential for latent design problems (Tarrents, 1980).
Structured what if technique (SWIFT)	High level structured brainstorming technique that originated from the process/manufacturing industry. As the name implies, this process is based around a series of structured and well-defined questions aimed at brainstorming possible failure mechanisms for the system at an early stage of the design. Considers complete systems, subsystems and processes. Has many similarities to HAZOPS, in that it is team-based brainstorming and uses prompts (e.g. checklists) to explore the behaviour of a system and identify hazards. Instead of guide words, SWIFT uses a series of questions which usually, but not always start 'what if ...'. For example: What if • a specific item of equipment fails? • the operator fails to carry out the correct procedure? • the level control fails to operate? • a fire occurs in a particular part of the plant? • a flood occurs? • the maintainer tried to work without isolating the power supply? (Defence Procurement Management Guide, DPMG/TEC/320 Iss1 (Sept98))
Subjective workload assessment technique (SWAT)	Human factors evaluative tool.
Systematic inspection	This technique's purpose is to perform a review or audit of a process or facility (Tarrents, 1980).
Task analysis	Task analysis is a fundamental human factors method and underlies many other techniques. A small selection of known tools include: • applied cognitive task analysis (ACTA) • ATLAS • functional analysis system technique (FAST) • goals, operators, methods and systems (GOMS) • Micro Saint (software program) • repertory grid analysis. Task analysis is a method to evaluate a task performed by one or more personnel from a safety standpoint in order to identify undetected hazards, develop notes/cautions/ warnings for integration in order into procedures, and receive feedback from operating personnel (Tarrents, 1980).

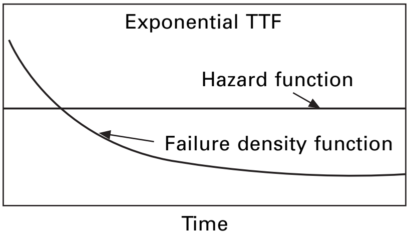
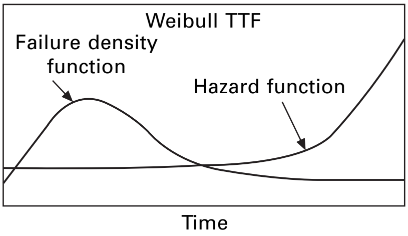
Advantages	Limitations
• Distribution can be determined by simulations measurement/testing.	• For complex systems, which are affected by many variables (e.g. environmental factors), random testing will not suffice. •
• The approach is appropriate to structural design, i.e., airframe.	•
• Useful for identifying hazards of a complete system/operation. • Systematic and thorough. • Effective alternative to HAZOP, but more system orientated. • Efficient, because it focuses on areas of importance (more pertinent than HAZOP). • Strengthened by the use of checklists resulting in additional level of thoroughness. • Scenario based, so useful to identify and evaluate contingency plans. • Generally a higher level than the HAZOPS process and results in a quicker study. •	• Not as rigorous as HAZOP. • Requires thorough preparation before the meeting (the first stage of the process is to generate the list of questions and this should draw on the experience and imagination of team members as well as standard hazard checklists and other documents relevant to that type of system). • The success of the process is reliant, primarily, on the experience of the personnel conducting the review.
• Subjective in terms of safety implications.	• Subjective.
•	•
• Universally appropriate to any operation where there is a human input (Tarrents, 1980).	• Not strictly speaking a safety tool, but does contribute to the HF requirements (e.g. design specification) which can influence safety. • Somewhat surprisingly perhaps, few computer-based tools have been developed to support it (Tarrents, 1980).
	•

Technique	Description
Technique for human error rate prediction (THERP)	This technique provides a quantitative measure of human operator error in a process (Tarrents, 1980). Widely used technique, which encompasses other human factor methods (e.g. FTA, task analysis, performance shaping factors).
Technique for the retrospective analysis of cognitive error (TRACEr)	TRACEr provides a human error identification technique specifically for use in the air traffic control domain. It builds on error models in other fields and integrates model of information processing in ATC. TRACEr is represented in a series of decision flow diagrams. Based on models of human information processing where errors are caused by breakdown in: • perception (misperceive or fail to perceive info correctly) • decision (error of judgement, planning or decision making) • memory (info forgotten or misrecalled). • action (error in carrying out the task). Developed by NATS (see Burret, G and Foley, S, *Integrating Human Error Management Strategies Throughout the System Lifecycle,* National Air Traffic Services, Bournemouth, UK, presented in *Current Issues in Safety Critical Systems,* Proceedings of the 11th Safety Critical Systems Symposium 4–6 Feb 2003).
Test safety analysis	Test safety analysis ensures a safe environment during the conduct of systems and prototype testing. It also provides safety lessons to be incorporated into the design, as application. This approach is especially applicable to the development of new systems, and particularly in the engineering/development phase (Tarrents, 1980).
Tests	Often analysis alone cannot accurately predict precise effects or probability of failures., so it becomes essential to conduct actual tests (i.e. on rigs or *in situ*). Essential in the following circumstances • with circuits which use integrating and differentiating functions or other processing which may be sensitive to changes in time constants. • in control system where it is often necessary to have cross-connections between channels in order to achieve synchronisation or load sharing or cross-monitoring.
The IEEE gold book	IEEE STD 493-1997, *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, provides data on commercial power distribution systems. Provides data concerning equipment reliability used in industrial and commercial power distribution systems. Reliability data for different types of equipment are provided along with other aspects of reliability analysis for power distribution systems, such as basic concepts of reliability analysis, probability methods, fundamentals of power system reliability evaluation, economic evaluation of reliability, and cost of power outage data. The handbook was updated in 1997; however, the most recent reliability data reflected in the document is only through 1989.

Advantages	Limitations
• This technique is the standard method for the quantifying of human error in industry.	•
• Assists in identifying sources of human error. Knowing how and why an error occurred is the only way to successful intervention. • Uses a standardised series of pick-lists and decision trees to enable consistent classification or error information. • The method marks a shift away from knowledge based errors in other error analysis tools to better reflect the visual and auditory nature of ATM. • It has proved successful in analysing errors in AIRPROX reports to derive measures for reducing errors and their adverse effects (Shorrock and Kirwan, 1999).	• Largely reactive. • Needs to be combined with other techniques to enable allocation of safety targets.
• A lessons learned approach of any new systems 'or potentially hazardous subsystems' is provided.	•
• Verify correct functionality. • Inducing failures can be the only way to verify system performance. • Validates assumptions made during the development process.	• Generally more expensive than analysis. • Cannot test everything (e.g. software).
•	•

Technique	Description
The sequentially timed events plot investigation system (STEP)	This method is used to define systems; analyse system operations to discover, assess, and find problems; find and assess options to eliminate or control problems; monitor future performance; and investigate accidents (Tarrents, 1980).
Time/loss analysis for emergency response evaluation	Any airport, airline and other aircraft operators should have an emergency contingency plan to handle unexpected events. This technique is a system safety analysis-based process to semi-quantitatively analyse, measure and evaluate planned or actual loss outcomes resulting from the action of equipment, procedures and personnel during emergencies or accidents. This approach organises data needed to assess the objectives, progress, and outcome of an emergency response; to identify response problems; to find and assess options to eliminate or reduce response problems and risks; to monitor future performance; and to investigate accidents (Tarrents, 1980).
Top-down analysis approach	Starts by identifying the failure condition to be investigated and then proceeds to derive those failure modes (and combinations of failure modes) which can produce it. Built on the assumption that evaluation can be best served by examining the system as a whole (its goals, objectives, operating environment, etc.), and examining the individual sub-systems or components (Garland, *et al.*, 1999). An example top-down approach is the functional hazard analysis (FHA).
Trend(ing) analysis	Trending is performed by sorting various characteristics of events of interest.
Uncertainty analysis	Addresses, quantitatively and qualitatively, those factors that cause the results of an analysis to be uncertain (Tarrents, 1980).
User analysis	Human hazard assessment technique. Potential system users (including maintainers and installers) are identified and characterised for each stage of the system life cycle. The most important user population is those people who will be regular users or 'operators' of the product or system.

Advantages	Limitations
• In accident investigation a sequential time of events may give critical insight into documenting and determining causes of an accident.	•
•	•
• Requires an evaluation of the system as a whole (i.e. the 'big picture'.	•
• Good to learn lessons from history. • Facilitates performance assessments and projections. Identifies persistent management deficiencies (root causes). • Highlights unique, unrecognised, or improperly defined risks. • Identifies misallocated management resources. • Flags sudden changes in performance, either positive or negative. • Provides correlation of changes in performance to events producing such changes. • Highlights risk assessment weaknesses.	Backward looking. Does not allow for effects caused by ageing systems (e.g. aircraft).
•	• This discipline does not typically address uncertainty explicitly and there are arguments that all analyses should. •
•	Even if user characteristics are identified, a simple list of characteristics often fails to influence design. Disembodied user characteristics may result in an 'elastic user' whose characteristics shift as various features are developed. Designing for an

Technique	Description
Walk-through analysis	This technique is a systematic analysis that should be used to determine and correct root causes of unplanned occurrences related to maintenance (Tarrents, 1980).
Weibull analysis	Most reliability analysis uses an exponential time to failure (TTF) distribution, which says that the instantaneous rate of failure is constant over time, and the item is as likely to fail at one moment as another (i.e. it is 'memoryless' – that is, the item is not more likely to fail the next moment simply because it has operated for a long time).   This is not good enough when considering the effect of ageing, when the failure rates are increasing. The question is: how often should this inspection be performed? One very useful distribution for modelling TTF in the presence of ageing is the Weibull distribution, which has the advantages of: 1. being very flexible to fit a large number of field data samples, and 2. collapsing to the exponential TTF distribution when the field data is fairly flat over time, and 3. being a theoretical 'limiting distribution' (which is somewhat beyond the scope of this brief). In Weibull analysis, the practitioner attempts to make predictions about the life of all products in the population by 'fitting' a statistical distribution to life data from a representative sample of units. The parameterised distribution for the data set can then be used to estimate important life characteristics of the product such as reliability or probability of failure at a specific time, the mean life for the product and failure rate. Life data analysis requires the practitioner to: • gather life data for the product

Advantages	Limitations
	elastic user may create a product that fails to satisfy any real user.
•	•
• Is a powerful tool that provides the reliability engineer with a means to quantify the effect that various design options will have on reliability and cost. • Predict failure rates and provides a description of the failure of parts and equipment. • Provides useful insight into the following issues. – characteristic life – standard deviation of life – mean life – reliability functions – reliable life – median life initial failure rate per unit time.	•

Technique	Description
	• select a lifetime distribution that will fit the data and model the life of the product • estimate the parameters that will fit the distribution to the data • generate plots and results that estimate the life characteristics, like reliability or mean life, of the product.
What-if analysis	What-if analysis methodology identifies hazards, hazardous situations, or specific accident events that could produce an undesirable consequence. It is a simple method of applying logic in a deterministic manner (Tarrents, 1980). A problem-solving approach that uses loosely structured questioning to (i) suggest upsets that may result in accidents or system performance problems and (ii) make sure the proper safeguards against those problems are in place. Typical qualitative probability terms are: a. Probable failure conditions are those anticipated to occur one or more times during the entire operational life of each aeroplane. b. Improbable failure conditions are divided into two categories as follows: (i) Remote. Unlikely to occur to each aeroplane during its total life but which may occur several times when considering the total operational life of a number of aeroplanes of the type. (ii) Extremely remote. Unlikely to occur when considering the total operational life of all aeroplanes of the type, but nevertheless has to be considered as being possible. c. Extremely improbable failure conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all aeroplanes of one type.
Zonal safety analysis (ZSA)/Zonal hazard analysis (ZHA)	CCA technique which specifically considers physical proximity of different technologies. Theoretical and visual examination of each physical zone to ensure that interference and interactions with adjacent systems do not violate the independence requirements. Used to: • determine compliance with the installation rules • identify any potential cascade failures due to system interaction • identify any potential areas for maintenance errors • identify potential areas for system malfunction due to environmental factors. This technique is used to look at the complex interactions that can occur between high-energy systems and is specifically concerned with their physical position in relation to each other. The zonal hazard analysis techniques are also used to assess the effects of the proliferation of hazards into adjacent physical areas or compartments. They can be used to identify the routes by which the hazards may spread and in so doing, solutions can be developed to control and mitigate the effects of the hazard. See SAE ARP5754 p38

Advantages	Limitations
• Useful for any type of system, process or activity. • Useful when more precise methods (e.g. FMEA, HAZOPS) are not possible or practical. • Especially useful if combined with checklists.	•
• Highlights potential hazards from adjacent non-related systems (e.g. heating pipes near sensitive electronic equipment, hot air leaks, drips from pipes, multi-channels through same connectors, EMI effects on multi-channel configurations, etc.). • Considers any potential interactions between high-energy sources and sensitive items. •	• Best done at a later stage in the design when all equipment can be considered. This means that changes are likely to be expensive. • Tends to be very subjective, difficult to systematise. • Restricted to each specific zone considered. • Requires system experience. • Checklists can be utilised in the process to identify hazards, they can also be used to check that designs comply with certain standards and codes of practice, or that protective measures are correctly employed. They are however, reliant on the knowledge and experience of those persons compiling the lists.

Appendix B

Safety criteria

There is a measure in everything. There are fixed limits beyond which and short of which right cannot find a resting place

Horace (65 BC–8 BC)

B.1 Introduction

Regulations have different definitions for the various categories of failures and/or hazards. In order to guide the safety assessment process, it is necessary firstly to define the criteria used to evaluate the various failures and hazards present and judge the acceptability of their occurrence. It has been said that: ‘You cannot manage what you cannot measure’. We therefore need to define the exact terminology and allocate a measure of performance. These definitions are fundamental keys to understanding the data presented, as the resultant ‘safety acceptance criteria’ form the baseline standards against which the system is then evaluated during the safety assessment.

The broad range of accidents/hazards (see Chapter 6), their associated risks, and the particular circumstances of each potential accident situation means that it may not be practicable to have one single set of criteria covering all contingencies. However, irrespective of which criteria are chosen, they must be substantiated and agreed by the relevant regulatory authority. To measure is to know, but first we need to define the measuring stick. Hence the production of the safety criteria report. The criteria should be formulated so as to provide effective safety measures, be readily understood in terms of both concept and application, and be flexible to provide scope for user contribution.

The aim of this Appendix is to summarise some of the commonly used safety criteria that may be useful in evaluating the safety of a system. This chapter must be read with an understanding of the contents of Chapters 4 and 5. It is for the safety assessor (with regulatory authority concurrence) to select the optimum criteria (or combination of criteria) from applicable regulations to apply to the specific system level (see Fig. 8.1) under consideration. Most importantly, the chosen criteria must be applied consistently throughtout the complete system safety assessment/safety case. If this is not done then efficient risk comparison will be compromised, and the integration of lower-level safety assessments is bound to be exceedingly complicated.

B.2 ICAO accepted safety criteria

B.2.1 Background

With reference to Chapter 5 section 5.2, the ICAO *Airworthiness Manual* (Appendix H to Chapter 4, page IIA-4h-I) states the following for large civil aircraft:

> Where it is necessary to use numerical assessments the values given below may be used in providing a common point of reference:[1]
>
> - 'Frequent' may be interpreted as a probability of occurrence greater than 10^{-3} per hour of flight for the expected mean flight time of the type of aeroplane involved.
> - 'Reasonably probable' may be interpreted as a probability of occurrence in the range of 10^{-3} to 10^{-5} per hour of flight for the expected mean flight time of the type of aeroplane involved.
> - 'Remote' may be interpreted as a probability of occurrence in the range of 10^{-5} to 10^{-7} per hour of flight for the expected mean flight time of the type of aeroplane involved.
> - 'Extremely remote' may be interpreted as a probability of occurrence in the range of 10^{-7} to 10^{-9} per hour of flight for the expected mean flight time of the type of aeroplane involved.
> - 'Extremely improbable' may be interpreted as a probability of occurrence of less than 10^{-9} per hour of flight for the expected mean flight time of the type of aeroplane involved.
>
> The numerical values are goals rather than precise values and judgement should be used in their application.
>
> The probability should be established taking into account the appropriate time of risk. Such statistical methods should be used to complement engineering judgement and should not be regarded as a substitute.
>
> Critical combinations of failures should be investigated and may be accepted on the basis of assessed numerical probability values where these values can be substantiated, and a suitable analysis technique has been employed. When the failure of a device can remain undetected in normal operation, the frequency with which the device is checked will directly influence the probability that such a failure is present on any particular occasion.

When using quantitative analyses to help determine compliance with FAR/CS 25.1309(b), these descriptions of the probability terms have become commonly accepted as aids to engineering judgement. They are expressed in terms of acceptable ranges for the average probability per flight hour.

The JAA/EASA and FAA allocate these numerical goals to failure conditions of aircraft systems as follows (refer FAR/JAR/CS25.1309):

[1] Note that these levels are for aircraft systems only and should not be applied to quantitative safety levels for aircraft operations.

The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that –

(1) Any Catastrophic failure condition:
- is Extremely Improbable; and
- does not result from a single failure; and

(2) Any Hazardous failure condition is Extremely Remote; and
(3) Any Major failure condition is Remote.

Note that this is the goal-based approach as discussed in Chapter 5.

B.2.2 Application

These criteria are applied as per Tables B.1 to B.6.

- Failures affecting airworthiness can be defined according to the severity categories in Table B.1.
- In accordance with ACJ25.1309 and JAA Notice for Proposed Amendment (NPA) 25F-281, each failure is allocated a qualitative safety objectives (i.e. minimum probability of occurrence) based on the worst potential consequence of the hazard as per Table B.2.
- For qualitative assessments the following assertions/claims in Table B.3 (if properly substantiated) may satisfy the qualitative objectives.
- For quantitative assessments the limits for probability of hazard occurrence in Table B.4 are commonly accepted as aids to engineering judgement.
- ACJ25.1309 provides an indication of the level of effort that is needed to satisfy these objectives and these are summarised in Table B.5.
- Table B.5 can be illustrated as the flowchart in Fig. B.1.

For software induced hazards, Table B.6 (refer RTCA-DO178B) allocates a development assurance level[2] (DAL) as an objective to each hazard's severity category. Proof of the level of development assurance may lead to qualitative occurrence claim level as indicated.

[2] Typically one would apply a software development standard and then use a software assurance level to make sure all the needed visibility and characteristics have been captured by the specific instantiation of the chosen software development standard. DAL provides:

- an orderly and repeatable software development process (planning, requirements, design, code and test).
- a means to establish that certain attributes are present in a development (i.e. correct, reliable, verifiable and maintainable).

Table B.1 Failure[1] severity categories

	No safety effect	Minor	Major	Critical	Catastrophic
Failure definition	Failure conditions which would not affect aeroplane safety in any manner.	Failure conditions that would not significantly reduce aeroplane safety and which involve crew actions that are well within their capabilities.	Failure that would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions.	Failure conditions which would significantly reduce the capability of the aeroplane or the ability of the crew to to cope with adverse operating conditions.	Failure conditions which would prevent continued safe flight and landing. Normally with hull loss.
Effect/consequence of failure	At most a nuisance.	Slight reduction in safety margins or functional capabilities. Slight increase in crew workload (e.g. routine flight path changes). Some inconvenience to occupants. May require operating limitations or emergency procedures.	Significant reduction in safety margins or functional capabilities. Significant increase in crew workload impairing crew efficiency. Discomfort to occupants, possibly including injuries. Would require operating limitations or emergency procedures.	Large reduction in safety margins or functional capabilities. Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely. Serious or fatal injury to a relatively small number of the occupants.	Multiple deaths, usually with loss of aircraft.

[1] This is often referred to as 'hazard severity', which can cause confusion. See Fig. 6.1.

Table B.2 Qualitative safety objectives

No safety effect	Minor	Major	Critical	Catastrophic
Frequent	Probable	Remote	Extremely remote	Extremely improbable

Table B.3 Qualitative safety objectives

Frequent	Probable	Remote	Extremely remote	Extremely improbable
Conditions anticipated to occur several times.	Conditions anticipated to occur one or more times during the entire operational life of each aeroplane.	Conditions unlikely to occur to each aeroplane during its entire life but which may occur several times when considering the total operational life of a number of aeroplanes of this type.	Conditions unlikely to occur when considering the total operational life of all aeroplanes of the type, but nevertheless have to be considered as being possible.	Conditions so unlikely to occur that they are not anticipated to occur during the entire operational life of all aeroplanes of the type.[1]

1. Experienced engineering judgement may enable an assessment that such a failure is not foreseeable. The assessment logic and rationale should be readily obvious that a knowledgeable, experienced person would unequivocally conclude that the failure condition simply would not occur. When making such an assessment, all possible and relevant considerations should be taken into account, including all relevant attributes of the design. Extensive service experience alone showing that the failure condition has not yet occurred is not sufficient reason to indicate that a single failure condition cannot exist.

Table B.4 Quantitative safety objectives

Frequent	Probable	Remote	Extremely remote	Extremely improbable
No requirement	$10^{-5} < p \leq 10^{-3}$ per flight hour	$10^{-7} < p \leq 10^{-5}$ per flight hour	$10^{-9} < p \leq 10^{-7}$ per flight hour	$p \leq 10^{-9}$ per flight hour

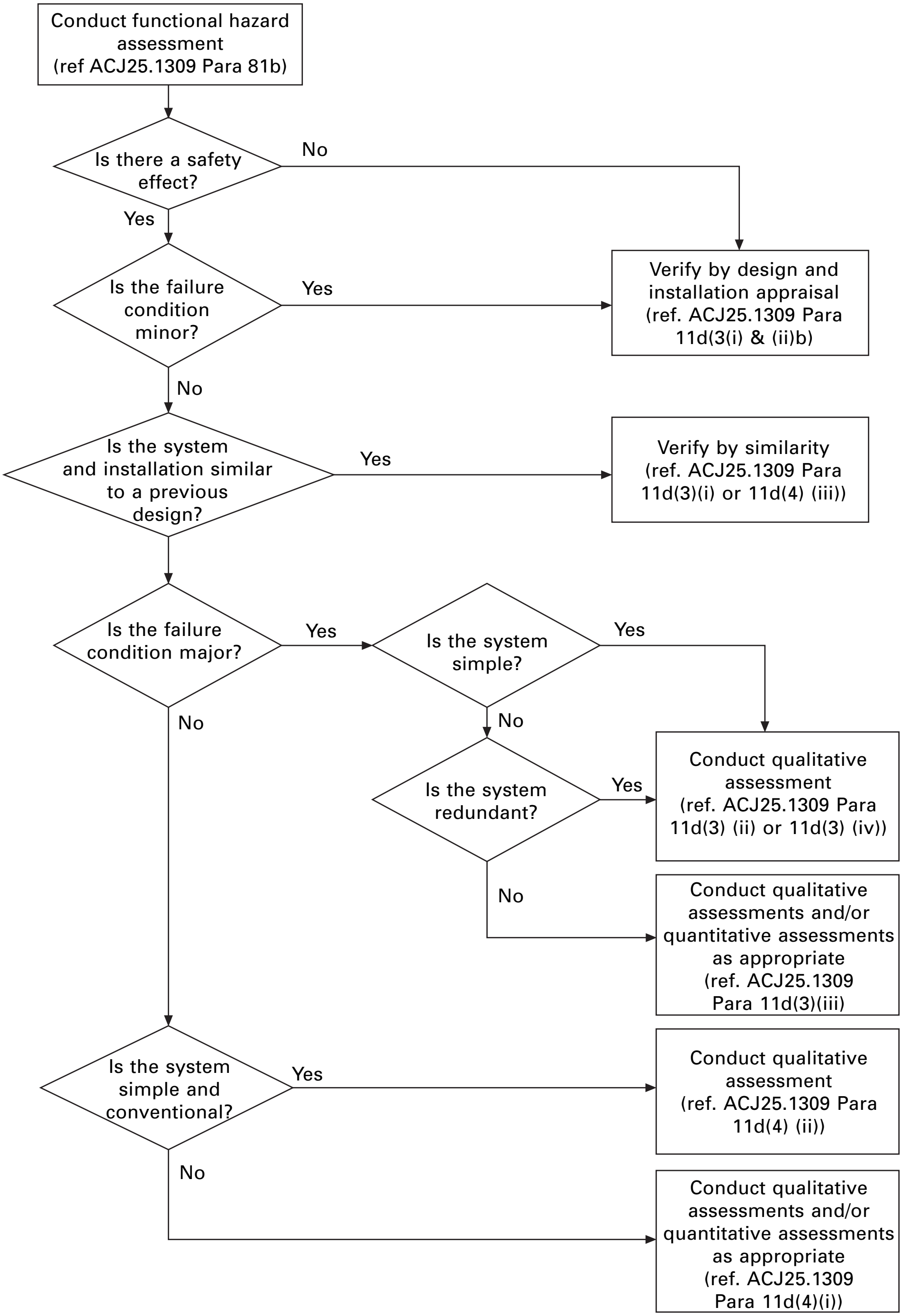
Table B.5 Depth of analysis required to meet safety target[1]

Frequent	Probable	Remote	Extremely remote/ Extremely improbable
None required	Design and installation appraisal to verify independence of function and physical separation from airworthiness-related components. (Verify that failures of the system will not contribute to more	1. If the complexity of the system is low, and the system is similar in its relevant attributes to those used in other aeroplanes and the effects of failure would be the same, then design and installation appraisals, and satisfactory service	Except as specified in paragraph (2), a detailed safety analysis will be necessary for each hazardous and catastrophic failure condition identified by the functional hazard assessment. The analysis will usually be a combination of qualitative and quantitative

Table B.5 Continued

Frequent	Probable	Remote	Extremely remote/ Extremely improbable
	severe failure conditions if combined with other systems or functions.) If still minor, then no further action required to be 25.1309 compliant.	history of the equipment being analysed, or of similar design, will usually be acceptable for showing compliance. 2. If similarity cannot be justified, but the system is conventional in its relevant attributes, then compliance may be shown by means of a qualitative assessment. This also applies to systems of high complexity, provided that there is reasonable confidence that the failure condition is not worse than major. 3. For complex systems which include functional redundancy, a qualitative failure mode and effects analysis or fault tree may be necessary to determine that redundancy actually exists (e.g. no single failure affects all functional channels), and to show that the failure modes of the equipment do not have any airworthiness-related effects on other functions.	assessments of the design. Probability levels which are related to catastrophic failure conditions should not be assessed only on a numerical basis, unless this basis can be substantiated beyond reasonable doubt. For very simple and conventional installations, i.e., low complexity and similarity in relevant attributes, it may be possible to assess a catastrophic failure condition as being extremely improbable, on the basis of experienced engineering judgement, without using all the formal procedures listed above. The basis for the assessment will be the degree of redundancy, the established independence and isolation of the channels and the reliability record of the technology involved. Satisfactory service experience on similar systems commonly used in many aeroplanes may be sufficient when a close similarity is established in respect of both the system design and operating conditions. As discussed in paragraphs (1) and (2) compliance for a system or part thereof that is not complex may sometimes be shown by design and installation appraisals and evidence of satisfactoryservice experience on other aeroplanes using the same or other systems that are similar in their relevant attributes.

1. Refer ARP4761 (p14 and 23), and AMC25.1309.


Conduct functional hazard assessment (ref ACJ25.1309 Para 81b)
Is there a safety effect?
No
Yes
Is the failure condition minor?
Yes
Verify by design and installation appraisal (ref. ACJ25.1309 Para 11d(3(i) & (ii)b)
No
Is the system and installation similar to a previous design?
Yes
Verify by similarity (ref. ACJ25.1309 Para 11d(3)(i) or 11d(4) (iii))
Is the failure condition major?
Yes
Is the system simple?
Yes
No
No
Is the system redundant?
Yes
Conduct qualitative assessment (ref. ACJ25.1309 Para 11d(3) (ii) or 11d(3) (iv))
No
Conduct qualitative assessments and/or quantitative assessments as appropriate (ref. ACJ25.1309 Para 11d(3)(iii)
Is the system simple and conventional?
Yes
Conduct qualitative assessment (ref. ACJ25.1309 Para 11d(4) (ii))
No
Conduct qualitative assessments and/or quantitative assessments as appropriate (ref. ACJ25.1309 Para 11d(4)(i))

B.1 Depth of analysis flowchart (AMC.25.130 (Fig A2-2) in CS25).

Table B.6 Software development assurance levels

	No safety effect	Minor	Major	Critical	Catastrophic
Required DAL	No requirement	Level D	Level C	Level B	Level A
Occurrence claim level	Frequent	Reasonably probable	Remote	Extremely remote	Extremely improbable

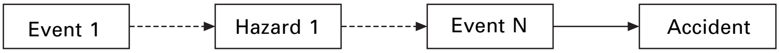
B.3 UK Ministry of Defence safety criteria

B.3.1 Background

In the UK military aviation industry, two distinct sets of safety criteria are applied:

1. Accident/health and safety criteria (refer to the Health and Safety at Work Act), which considers the risk (i.e. probability and severity) of a potential accident.[3] These criteria are derived from the risk-based approach discussed in Chapter 4, which is based on an accident sequence model,[4] a simple example is illustrated by Fig. B.2.

   As can be seen, the probability of the accident is dependent on the probability of the system hazard and the probability of the intermediate events (e.g., friendly fire or human error). The severity of the accident is dependent on the extent of injuries involved or damage caused.
2. Airworthiness criteria, where safety assessments for airborne equipment are represented in terms reflecting aviation-specific standards and requirements. The term 'airworthiness' is used here within the context of the aircraft's ability to continue safe flight and landing. Regulations such as JSP553 (and CS25.1309) use 'failure'[5] severity categories rather than 'accident' severity categories, because there is really only one accident being considered (i.e. the aircraft crashes). It



B.2 Simple linear accident.

[3] Defence Standard 00-56 criteria are founded on these principles and are applicable to all defence systems, not only aeronautical.

[4] See accident (i.e. not hazard) classifications in DEF STAN 00-56 and JSP318B Appendix 1 to Annex J Para 0.2 (i.e. chain of events).

[5] A failure condition is defined at the level of each technical system by its effects on the functioning of that system. It is characterised by its effects on other systems and on the whole system. All single failures and combinations of failures, which have the same effects on the system under consideration, are grouped in the same failure condition.

also tends to embed directly the probability of the accident happening, given that the hazard has happened, into the hazard severity definition (in other words, it considers the ability to continue safe flight and landing following the occurrence of a hazardous situation).

Whilst there is no direct relationship between these two sets of criteria, by virtue of considering and mitigating aircraft system hazards, the system safety assessment will naturally contain some OH&S considerations.

B.3.2 Accident criteria

For the variety of systems[6] and operational conditions within the MOD's remit, DEF STAN 00-56 Part 1 Para 7.3.2 categorises accident severity in accordance with the impact on personnel as defined in Table B.7. The DEF STAN 00-56 approach assumes an accident sequence model similar to that shown in Fig. B.3. The hazard is that state of the system being considered which causes/permits/exacerbates the risk of the accident arising. The probability of the accident is dependent on the probability of the system hazard and the probability of the intermediate events (considered to be external to the system, but are necessary conditions for the accident to occur). In accordance with DEF STAN 00-56 Part 1 para 7.3.2(d) the accident probability of occurrence shall be categorised during risk estimation in accordance with the definitions in Table B.8.

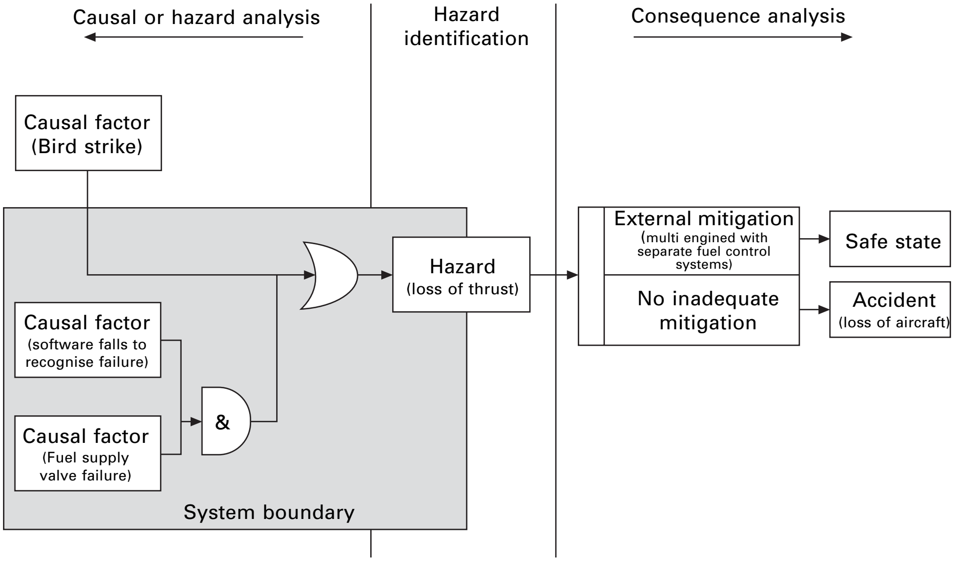
Table B.7 Accident severity categories

	Negligible	Marginal	Critical	Catastrophic
Definition	At most a single minor injury or minor occupational illness	A single severe injury or occupational illness; and/or multiple minor injuries or minor occupational illnesses	A single death; and/or multiple severe injuries or severe occupational illnesses	Multiple deaths

1. DEF STAN 00-56 (Part 1 section 7.3.2) does allow for these definitions to be modified if not appropriate for the system being considered.

The UK MOD base their acceptance of hazards on a risk classification scheme, which is based on the combination of the severity, probability and time of exposure for each particular hazard. For the purposes of the accident risk classification scheme, accidents are considered single events (Table B.9). These classifications can be combined to determine a hazard risk index (HRI), which is a numerical risk factor that can be used to prioritise the need for corrective action or resolution. The HRI matrix in Table B.10 is an example showing how the hazard severity and the hazard probability categories combine to yield the HRI.

[6] These systems could range from tanks to aircraft to submarines.


Causal or hazard analysis
Hazard identification
Consequence analysis
Causal factor (Bird strike)
Causal factor (software falls to recognise failure)
Causal factor (Fuel supply valve failure)
&
Hazard (loss of thrust)
System boundary
External mitigation (multi engined with separate fuel control systems)
No inadequate mitigation
Safe state
Accident (loss of aircraft)

B.3 Accidents, hazards and cause relationship model.

Table B.8 Accident probability categories[1]

Accident probability (qualitative probability)	Occurrence (during operational life considering all instances of the system)	Quantitative probability per operating hour[2]
Frequent	Likely to be continually experienced	$< 1 \times 10^{-2}$
Probable	Likely to occur often	$< 1 \times 10^{-4}$
Occasional	Likely to occur several times	$< 1 \times 10^{-6}$
Remote	Likely to occur at some time	$< 1 \times 10^{-8}$
Improbable	Unlikely, but may exceptionally occur	$< 1 \times 10^{-10}$
Incredible	Extremely unlikely that the event will occur at all, given the assumptions recorded about the domain of the system	$< 1 \times 10^{-12}$

[1] Refer DEF STAN 00-56 Part 1 section 7.3.2.

[2] Note that the term 'operating hour' does not necessarily correlate with 'flight hours' (as discussed in Table 5.1 and section 1.5.4). Within the risk-based approach, operating hours could include the hours during maintenance (e.g. for hazards presented to ground crew). Or, from another perspective, a fleet of ten aircraft flying in formation for two operating hours will accumulate 20 flying hours.

Table B.9 Risk classification[1]

	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	C	D	D	D

[1] Source Data: DEF STAN 00-56 Part 1 page 26 Table 5. Can be tailored if agreed by the accepting authority and the independent safety auditor (ISA). Sometimes it may be that different safety criteria are applied to individual risk groups (e.g. safety of passengers vs. safety of armament personnel), refer DEF STAN 00-56 (Part 1 Section 7.3.2.b).

Class A: these risks are intolerable and shall be removed by the use of safety features.
Class B: these risks are undesirable, and shall only be accepted when risk reduction is impracticable.
Class C: these risks are tolerable with the endorsement of the Project Safety Review Committee. May need to show that risk is ALARP.
Class D: these risks are tolerable with the endorsement of normal project reviews. No further action needed.

Table B.10 Example hazard risk index matrix[1]

	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

[1] See BAe Safety System (Doc No. AWN/GEN/996, dd March 98).
With:

- HRI 1 to 5: high risk. Unacceptable. Design changes or other action required.
- HRI 6 to 11: moderate risk. Acceptable with customer/safety management review. Justification required.
- HRI 12 to 20: low risk. Acceptable after safety working group review.

B.3.3 Airworthiness criteria

In accordance with JSP553 (Iss 1 Para 1.38), for peacetime flying, the design standard of a UK military aircraft type may be considered airworthy where the conditions of either (a) and (b) or (a) and (c) below are met as appropriate:

(a) For all military aircraft types, their associated equipment and software, the aircraft designer has satisfactorily demonstrated, in a safety case, the airworthiness of the design. This demonstration may include design analysis, application of specific standards (such as DEF STAN 00-970) and procedures, historical evidence of successful use of particular design features, system tests, and ground and air tests to arrive at an overall assessment of airworthiness.

(b) The cumulative probability of loss of an aircraft due to technical fault, and the cumulative probability of the aircraft (inclusive of its systems, structures and stores) which could result in the death of any aircrew or passengers, should both be assessed to be of the order of one in a million per flying hour (probability of occurrence 1×10^{-6} per flying hour) when operated within the conditions used for the airworthiness demonstration.

(c) Aircraft derived from civil passenger aircraft and used by the MoD in the passenger-carrying airliner role should meet a higher standard of safety. Such aircraft may be considered airworthy if the cumulative probability of loss of an aircraft due to a technical fault, and the cumulative probability of a technical failure of the aircraft (inclusive of all its systems, structures and stores) which could result in the death of any aircrew or passengers are both assessed to be in the order of not more than one in ten million per flying hour (probability of occurrence 1×10^{-7} per flying hour) when operated within the conditions used for the airworthiness demonstration.

Note: Practicably, this data is seldom available to fully populate all the accident models and combine them to achieve a prediction of their combined probability (i.e. some kind of loss-model). For large transport aircraft, the civil aviation authorities have similar targets[7] as for (c) above and provide the following assumptions to assist the assessment process (refer AMC25.1309):

- Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 per cent of the total were attributed to failure conditions caused by the aeroplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs.
- It is thus reasonable to expect that the probability of a serious accident from all such failure conditions be not greater than one per ten million flight hours or 1×10^{-7} per flight hour for a newly designed aeroplane.
- It is arbitrarily assumed that there are about 100 potential failure conditions in an aeroplane which would prevent continued safe flight and landing. The target allowable risk of 1×10^{-7} was thus apportioned equally among these conditions, resulting in a risk allocation of not greater than 1×10^{-9} to each. The upper-risk limit for 'failure conditions which would prevent continued safe flight and landing' would be 1×10^{-9} for each hour of flight which establishes an approximate probability value for the term 'Extremely improbable'. Failure conditions having less severe effects could be relatively more likely to occur (see Table B.1).

The tolerance for safety risks affecting civil aviation during peacetime is likely to be very different from the tolerance of safety risks to military aircraft during conflict (operational safety criteria may be less severe). In accordance with DEF STAN 00-56 (Part 1 Para 7.3.2.c), some systems have a defensive role whereby inaction under hostile circumstances may constitute a hazard. Safety targets for such systems shall address the requirements to reduce, to a tolerable level, the risk resulting from inaction under hostile circumstances.

[7] Note that, in contrast to the risk-based approach in section B.2.2, this approach uses the goal-based approach.

Example

Loss/malfunction of a missile approach warning system (MAWS) may not affect the airworthiness of the aircraft, and could be classified as a minor failure condition (using the goal-based approach) and may be probable in occurrence. However, in accordance with DEF STAN 00-56, this loss could cause loss of the platform as no warning would result in no evasive or protective action, and should thus be classified as a catastrophic failure condition, which should be extremely improbable in occurrence.

Where there is a conflict between the practicable realisation of safety targets for action and inaction within the system's operational role, a reasonable balance of risk reduction shall be established and agreed between the design authority, the independent safety auditor and the ministry of Defence's programme manager.

B.4 Air traffic management risk matrix

During 1999, the European Commission ARIBA[8] project attempted to build an accident risk tolerability matrix for air traffic operations on UK Health and Safety Executive lines. The main reason for this was due to the fact that UK industry safety assessments usually use the HSE studies and guidelines about 'tolerable' and 'acceptable risk', with the following (simplified) HSE definitions:

- ALARP principle. The principle that no risk in the tolerability region can be accepted unless reduced 'As Low As Reasonably Practicable'.
- Broadly acceptable risk. A risk which is generally acceptable without further reduction.
- Intolerable risk. A risk which cannot be accepted and must be reduced.
- Tolerability region. A region of risk which is neither high enough to be unacceptable nor low enough to be broadly acceptable. Risks in this region must be reduced ALARP.

The AMC 25.1309 guidance then allows failure conditions with the combinations of severity and frequency shown in Table B.11 (Brooker, 2004, Appendix A).

ARIBA then produced a matrix (Table B.12) indicating how the ALARP concept might be integrated into this framework. The three regions indicate the management decision-making and action required:

1. The intolerable region shows risk which cannot be accepted and must be reduced.
2. In the ALARP region, specific safety management measures should be defined (e.g. safety monitoring, safety improvement projects, etc.) as long as such is reasonably practicable.
3. Tolerable risks may be managed through normal procedures.

[8] ARIBA stands for 'ATM system safety criticality Raises Issues in Balancing Actors responsibility'. It is a project carried out on behalf of DGVII of the European Commission in 1998–1999 and addresses certification in ATM services (see Brooker, P, Delivering Safety in the Context of Environmental Restrictions, CAA Paper 2004/8, www.caa.co.uk , July 2004 Appendix A).

Table B.11 Failure condition tolerability matrix[1]

Probability (per flight hour)	Severity			
	Minor	Major	Hazardous	Catastrophic
Probable ($>10^{-5}$)	Tolerable	Intolerable	Intolerable	Intolerable
Remote (10^{-7} to 10^{-5})	Negligible	Tolerable	Intolerable	Intolerable
Extremely remote (10^{-9} to 10^{-7})	Negligible	Negligible	Tolerable	Intolerable
Extremely improbable ($<10^{-9}$)	Negligible	Negligible	Negligible	Tolerable

[1] It must be stressed that the words 'intolerable', 'tolerable' and 'negligible' are as suggested by ARIBA, and not the JAA/EASA.

Table B.12 Possible aviation accident risk tolerability matrix

Severity of accident	Frequency of accident				
Expected fatalities	1 a year in civil aviation	>1 a year in civil aviation	1 a year per large airline	>1 a year per large airline	1 a year per aircraft
Hundred(s) of fatalities	ALARP	ALARP	Intolerable	Intolerable	Intolerable
Many fatalities	Tolerable	ALARP	ALARP	Intolerable	Intolerable
Single fatality	Tolerable	Tolerable	ALARP	ALARP	Intolerable
Major injury	Tolerable	Tolerable	Tolerable	ALARP	ALARP
Minor injury	Tolerable	Tolerable	Tolerable	Tolerable	ALARP
No injury	Tolerable	Tolerable	Tolerable	Tolerable	Tolerable

B.5 MIL-STD-882D criteria

The MIL-STD approach is to make decisions regarding resolution of identified hazards based on the assessment of the risk involved. It requires the identification of the risk category by combining the 'mishap' severity with the 'mishap' probability. In this case, 'mishap' is the same as an accident.[9]

B.5.1 Mishap severity

Mishap severity categories are defined to provide qualitative measures of the worst credible mishap (i.e. accident) resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure/malfunction as shown in Table B.13.

[9] Previous issues of MIL-STD-882 used the term 'hazard' (defined as 'a condition that is a prerequisite to a mishap', and went on to define hazard severity and hazard probability levels (see Tables B.13 and B.14). This was definitively incorrect, as these categories described accidents (or mishaps) – not hazards.

Table B.13 Suggested mishap severity categories[1]

Description	Category	Definition
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

1. These severity categories provide guidance to a wide variety of programmes (not only aviation). MIL-STD-882D does allow adaptation to a particular programme if agreed by the approval authority.

B.5.2 Mishap probability

MIL-STD-882D (para A.4.4.3.2.2) states that ‘Mishap probability is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in potential occurrences per unit time, events, population, items, or activity’. Suggested mishap probability levels are shown in Table B.14.

Table B.14 Suggested mishap probability levels

Description	Level	Specific individual item	Fleet or inventory
Frequent	A	Likely to occur often in the life of an item with a probability of occurrence greater than 10^{-1} in that life	Continuously experienced
Probable	B	Will occur several times in the life of an item with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life	Will occur several times
Remote	D	Unlikely to occur in the life of the item with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced with a probability of occurrence less than 10^{-6} in that life	Unlikely to occur, but possible

B.5.3 Mishap risk assessment

MIL-STD 882D (para A.4.4.3.2.3) provides the matrix in Table B.15 for mishap risk assessment.

B.6 Other useful criteria

It is up to the asssessor to propose the most appropriate safety criteria, which will be used to judge acceptability of the system, and to agree these criteria with the appropriate authority. The following subsections provide examples of other safety criteria which may be usefully tailored to the unique circumstances of the system under consideration.

B.6.1 Impact on the mission

Safety and reliability are not synonymous because not all failures are hazardous. However, these failures could significantly impact the mission. Tables B.16 and B.17 provide criteria which can be tailored to specific circumstances.

B.6.2 Risk to environment and assets

Tables B.18 and B.19 provide criteria that may be useful to assess the risk that the hazard poses to the environment, assets, company reputation, etc.

Table B.15 Example risk assessment matrix

Severity category Mishap probability	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Mishap risk definitions:
1–5 = high – requiring acceptance by the Component Acquisition Executive
6–9 = serious – requiring acceptance by the Program Executive Officer.
10–17 = medium – requiring acceptance by the Program Manager.
18–20 = low – required acceptance as directed.

Table B.16 Operational criteria example 1

Category 1 failure	Category 2 failure	Category 3 failure	Category 4 failure	Category 5 failure
No restriction on operational capability	Little restriction on operational capability	Restriction on operational capability	Severe restriction on operational capability	Total or near total loss of operational capability

Table B.17 Operational criteria example 2

	No effect	Negligible	Marginal	Critical	Catastrophic
Operation	Normal operation	Restricted operation	Minimum safe operation	Controllable to an evacuable flight condition	Catastrophic condition
Performance	Full performance	Degraded mission performance	Loss of mission performance	Satisfactory for pilot ejection	Loss of controllability
Effects on	Mission reliability and capability		Mission safety and survivability		
Assessment required	Mission analysis		Safety analysis		

Table B.18 Risk assessment matrix example 1

Potential consequences of the incident					Increasing probability				
					A	B	C	D	E
Rating	People	Environment	Assets	Reputation	Unknown in aviation industry	Known in aviation industry	Happened before in company	Reported >3x/yr in company	Reported >3x/yr in location
0	No injury	Zero effect	Zero damage	No impact	3	3	3	3	3
1	Slight injury	Slight effect	Slight damage	Slight impact	3	3	3	3	2
2	Minor injury	Minor effect	Minor damage	Limited impact	3	3	3	2	2
3	Serious injury	Localised effect	Local damage	Considerable impact	3	3	2	2	1
4	Single fatality	Major effect	Major damage	National impact	3	2	2	1	1
5	Multiple fatality	Massive effect	Extensive damage	International impact	2	2	1	1	1

1 = Intolerable.

2 = Incorporate risk reduction measure.

3 = Manage through normal health and safety procedures.

Table B.19 Risk assessment matrix example 2

Potential consequence					Probability of the occurrence					
	People	Environment	Assets	Reputation	Frequent (likely to be continually experienced) $(p\geq 1\times 10^{-2}/h)$	Probable (likely to occur often) $(p\geq 1\times 10^{-4}/h)$	Occasional (likely to occur several times) $(p\geq 1\times 10^{-6}/h)$	Remote (likely to occur as some time) $(p\geq 1\times 10^{-8}/h)$	Improbable (unlikely, but may exceptionally occur) $(p\geq 1\times 10^{-10}/h)$	Incredible (extremely unlikely that the event will occur at all) $(p\geq 1\times 10^{-12}/h)$
No safety effect	No injury	Zero effect	Zero damage	No impact	C	D	D	D	D	D
Negligible	At most a single minor injury or minor occupational illness	Slight effect	Slight damage (< £xx)	Slight impact	B	C	C	D	D	D
Marginal	A single severe injury or occupational illness; and/or multiple minor injuries or minor occupational illnesses	Localised effect	Local damage (< £xx)	Limited impact	B	B	C	C	D	D
Critical	A single death; and/or multiple severe injuries or severe occupational illnesses	Major effect	Major damage (< £xx)	National impact	A	A	B	B	C	D

Catastrophic	Multiple deaths	Massive effect	Extensive damage (< £xx)	International impact	A	A	A	B	B	C

Class A: these risks are intolerable and shall be removed by the use of safety features.
Class B: these risks are undesirable, and shall only be accepted when risk reduction is impracticable.
Class C: these risks are tolerable with the endorsement of the Project Safety Review Committee. May need to show that risk is ALARP.
Class D: These risks are tolerable and, with the endorsement of normal project reviews, can be managed by normal safety management practices.

B.7 Safety critical system components

B.7.1 Background

Whilst we are on the subject of severity classification, it may be useful to clarify the use of the term 'safety critical', which is often used as the basis for design guidance, continued airworthiness, and maintenance. To this purpose, the following information is summarised from a draft FAA memorandum (ANM-03-117-10), which provides the criteria for identifying flight-critical system components as applied to large aircraft.

First, we need some definitions:

- A 'component' is (ANM-03-117-10, page 2) any software or equipment that would normally be part-number controlled at the aircraft level and is applicable to all aircraft systems and associated non-structural components, including the interfaces with structural components, and items consumed by the systems, such as lubrication, fuel, and hydraulic fluid. These part numbers are typically shown on the system or aeroplane-level installation drawings.
- A 'failure' means (ANM-03-117-10, page 2) failure to function as intended, i.e., a loss of function or a malfunction. Failures of sub-components, safety features, or consumable items associated with a part-number-controlled component are considered within the context of the higher-level component failure effect. The failures to be considered are based on the most severe aeroplane-level effect that cannot be reasonably ruled out by knowledgeable persons.

B.7.2 FAA policy

The FAA considers (ANM-03-117-10, page 3) a component to be safety critical when it has one or more of the following attributes:

- Its single failure results in a hazardous or catastrophic failure condition (see Table B.1 above). Although the design and certification processes normally strive to eliminate single failures that could result in catastrophic events, the FAA policy is intended to also cover the continued airworthiness process where potentially catastrophic single failures may be discovered. Common cause or cascading failures are considered single failures. When specific regulations allow exceptions for potentially catastrophic single failures, such as uncontained engine failures and flight control jams, those regulations shall take precedence.
- When a combination of two failures results in a hazardous failure condition, or a combination of three failures results in a catastrophic failure condition, every component in the combination is a flight-critical system component regardless of its individual hazard classification. There may be cases where a combination of four (or more) failures warrants additional review and validation.
- All components contributing to a significant latent failure condition are considered flight critical.

The identification of safety-critical features of the aircraft should ensure that future alterations, maintenance, repairs, or changes to operational procedures can be made with cognisance of those safety features.

Appendix C

GSN safety argument

The most perfidious way of harming a cause consists of defending it deliberately with faulty arguments

Friedrich Nietzsche (1844–1900)

C.1 Introduction

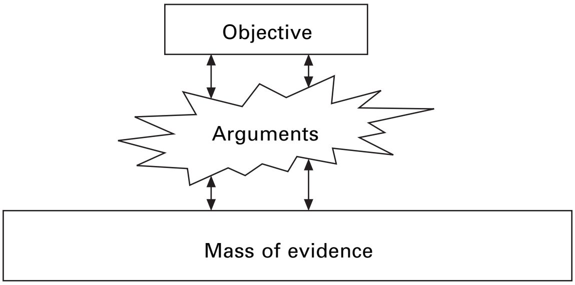
Any convincing argument (refer Ch. 8 para 4 and Ch. 9 para 3.1) or report requires three elements:

1. a distinct objective(s) or goal
2. supporting evidence
3. a clearly discernible 'thread' or argument, which communicates the relationship between the evidence and objectives.

This is illustrated in Fig. C.1.

A safety assessment (or safety case report) is no different. A 'mass of evidence' is generated during system development and certification (e.g. stress analysis, electrical load analysis, fatigue test, flight tests, performance verification, FHA, ZHA, FTA, regulatory compliance checklists, etc.) as well as during service experience (e.g. user confidence, training, etc.). This mass of evidence all provides substantiation for our confidence in the safety of the system. The challenge is to tie all this evidence to our safety objective via a logical, systematic and complete safety argument. This argument can be provided in textual format but is likely to be cumbersome and, for complex arguments, the 'devil may get lost in the details'. How many times have we read a wordy safety report which on the surface seems impressive, but is actually a little confusing and leaves you with the question: 'But what have we missed?'

It is easier with pictures – especially if the picture 'carries' the reader through the



C.1 The three elements in an argument.

argument with sufficient, judiciously placed ‘stepping stones’ (i.e. sub-goals and sub-arguments down to an inevitable solution). Goal structuring notation[1] (GSN) is a graphical notation method for developing complex arguments which explicitly represents the individual elements of any safety argument, i.e., requirements, claims, evidence and context and (perhaps more significantly) the relationships that exist between these elements, i.e., how individual requirements are supported by specific claims, how claims are supported by evidence and the assumed context that is defined for the argument.

The purpose of GSN is to provide that ‘discernible thread’ (i.e. linking the objectives with the evidence) by means of a logical argument. The fundamental approach of GSN is to show how:

- goals ▭ are broken into sub-goals ▭
- and eventually supported by evidence (solutions) ○
- whilst making clear the strategies ▱ adopted,
- the rationale for the approach (assumptions and justifications) ⬭
- the context ▢ in which the goals are stated.

C.2 GSN notation

The following notation is often used in a GSN argument.

▭ Goals (claims, premises and conclusions are represented as goals).

▱ Strategies (an inference from one or more premises (also known as propositions or grounds) to a conclusion.

○ Solutions (or evidence).

⬭ Assumption/justification.

▢ Context.

▭◇ Goal to be supported.

▭△ Goal to be instantiated (i.e. to be replaced with something ‘real’ at a later date).

→ Solved by/supported by.

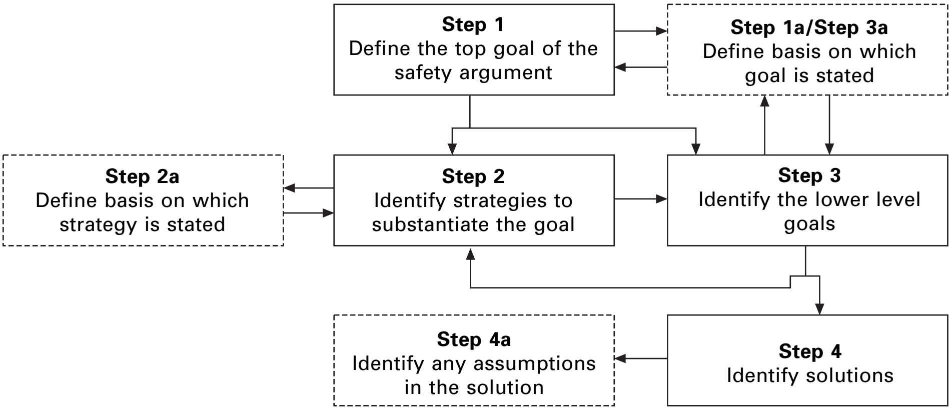
⟶ In context of.

◇ Model (i.e. leads to information outside the GSN structure).

C.3 GSN process

Most logical arguments are naturally hierarchical so that each argument can be broken down hierarchically into claims, arguments, sub-claims, sub-arguments, and eventually evidence. This suits the application of GSN, which illustrates how goals are broken

[1] GSN is sometimes called the goal structured notation or goal structure notation.


Step 1
Define the top goal of the safety argument
Step 1a/Step 3a
Define basis on which goal is stated
Step 2a
Define basis on which strategy is stated
Step 2
Identify strategies to substantiate the goal
Step 3
Identify the lower level goals
Step 4a
Identify any assumptions in the solution
Step 4
Identify solutions

C.2 Formulating a GSN safety argument.

into sub-goals, and eventually supported by evidence (solutions) whilst making clear the strategies adopted, the rationale for the approach (assumptions, justifications) and the context in which goals are stated. The GSN argument thus follows the following process:

- claim/objective (i.e. what we want to show)
- argument/premise (i.e. why we believe, subject to any assumptions/justifications, the claims met), based on
- evidence/solutions (e.g. tests, analyses, etc.).

The GSN Safety Argument can be formulated by following the process summarised in Fig. C.2 (tailored from the six-step method by Kelly).

C.3.1 Step 1

The top goal is the seed from which the argument can develop and is the ultimate aim of the system safety assessment or safety case. The following guidelines apply:

- Goals should be phrased as positive propositions, i.e., statements which can be said to be either true or false. Kelly (1998) advises that goals are best expressed in a <*noun-phrase*><*verb-phrase*>' format (i.e. noun-phrase identifies the subject of the goals, and the verb-phrase defines the predicate over the subject) (e.g. 'The sky is blue')
- Be careful of oversimplification (e.g. 'System X is safe' vs. 'System X is acceptably safe within context Y' (refer to section 2.1).

C.3.2 Step 1a (Step 3a)

Having presented a goal, make clear the basis on which that goal is stated. This is done by inserting context information, assumptions, Justifications and/or models which ensure that the goal is unambiguous.

C.3.3 Step 2

Work out how to substantiate the goals (i.e. what reasons are there for saying the goal is 'true'. This may require that you break the argument down into a number of smaller goals. Two options are available: if the argument is implicit, go to Step 3 (i.e. straight from goal to sub-goal) or, if an explicit argument is required, then insert it between the goal and the sub-goal. Kelly (1998) advises that strategies are best expressed in the noun-phrase form: 'Argument by … <*approach*>' (e.g. 'argument by consideration of historical data')

C.3.4 Step 2a

As per Step 1a (i.e. ask yourself what information is required in order to expand/fulfil the strategy outlined).

C.3.5 Step 3

Having identified an approach, it is necessary to lay out the goals that fulfil that approach (i.e. by going into sub-goals). Here it is important not to lose the argument by making too big a leap. As soon as the question 'why' is raised, then consideration should be given to going 'up' a level to provide another 'stepping stone' to the argument. Kelly (1998) advises concentrating on the breadth of the argument first, before getting wrapped-up in the depth of it.

C.3.6 Step 4

Eventually, faced with a goal that does not need further expansion/refinement/explanation, add (or reference) the solution. Ideally solutions should be noun-phrases (e.g. 'software tests result XYZ') (Kelly 1998), but is it often useful to refer to reports/assessments where the solutions can be found (e.g. an FHA need not be taken from tabular format into individual GSN arguments for each functional failure mode).

C.3.7 Step 4a

Declare (or reference) any assumptions needed in the development of the solution. A solution might be 'not applicable', in which case a 'justification' will be required.

C.4 Discussion

Argument without supporting evidence is unfounded, and therefore unconvincing. Evidence without argument is unexplained – it can be unclear that (or how) safety objectives have been satisfied (Kelly and Weaver, 1994). GSN is most useful wherever:

- there is most uncertainty about the argument (i.e. key claims and evidence)
- the argument is currently confused or is over-complex
- there is disagreement about the argument

- the consequences of having a wrong argument are high.

Advantages of using a GSN Safety Argument include:

- improved comprehension of existing arguments
- useful way to define safety assessment/case strategy
- easy to read – even for a novice
- presents logical argument to get from a goal to its logical solution (forces a logical argument)
- identifies holes in an argument
- positively identifies assumptions
- removes ambiguity (i.e. measurable goals have to be defined)
- assists in managing programme risk (i.e. solution planning and prioritising)
- easy to audit
- prevents duplication of solutions
- prevents unnecessary work (e.g. if not required by a goal)
- defines scope of work, so assists in planning and budgeting
- arguments can be reused in another project.

However, GSN is not without its limitations:

- It takes a lot of effort to develop the arguments. Needs experience and skill to do it efficiently.
- Can easily go into too much complicated detail (e.g. sometimes it is more efficient to make the solution a separate compliance matrix rather than trying to argue compliance via GSN).
- Arguments are always subjective, so every person will compile a GSN differently. A lot of time can be spent agreeing an argument instead of getting on with the required solutions. So, it may be more efficient to restrain GSN to a top-level argument only and not to repeat each finding which exists in tabular format (e.g. such as in a functional hazard assessment).
- GSN is not as user friendly in hard copy format, because a complex and large GSN needs hyperlinks to facilitate ease of use.

The high-level safety argument must be developed as early as possible as it provides a clear picture of the methodology by which safety will be substantiated. If agreed with the applicable authority, this argument scopes all future safety-related activities to generating lower-level arguments and solutions. If the high-level argument shows (with justification) that a particular solution is not applicable, then no further action is required for that solution.

Possible approaches to the inclusion of GSN argument in a document such as a safety assessment/safety case include:

- in full as an appendix/annex to the report
- as a chapter/paragraph in a report, which guides the reader through a potentially confusing and intimidating report
- as an ‘executive summary’ at the beginning of the report
- as a separate, stand-alone, index document (i.e. to link separate documents together).

C.5 Further reading

The application of GSN in the safety environment has been developed and refined by Dr Tim Kelly, whose doctoral research at the University of York focused upon safety argument presentation, maintenance, and reuse. For more information on Dr Kelly's work, see:

Kelly, T and Weaver R, *The Goal Structuring Notation – A Safety Argument Notation*, http://www-users.cs.york.ac.uk/~rob/papers/DSN04.pdf Department of Computer Science and Department of Management Studies, University of York, York, YO10 5DD UK, tim.kelly@cs.york.ac.uk, rw24@york.ac.uk

http://www-users.cs.york.ac.uk/~tpk/scomp99.pdf

Abbreviations and acronyms

λ	Constant Failure Rate = 1/MTBF
θ	MTBF
Π	‘Product of’ (i.e. a mathematical operator)
Σ	‘Sum of’ (i.e. a mathematical operator)
a/c	Aircraft
AC	Advisory Circular
ACJ	Advisory Circular Joint
ACS	Aircraft Systems
ADF	Automatic Direction Finder
ADRP	Airworthiness Design Requirements and Procedures (UK MoD)
ADU	Air Data Unit
AECMA	Aircraft European Manufacturers Association
AFCC	Air Force Command Council
ALARP	As Low As Reasonably Practicable
ALC	Air Logistics Command
AMC	Advisory Material Circular
AMJ	Advisory Material Joint
APD	Air Publications Depot
APU	Auxiliary Power Unit
ARIBA	ATM system safety criticality Raises Issues in Balancing Actors responsibility
ARINC	Aeronautical Radio Inc.
ARP	Aerospace Recommended Practices
ASIP	Airframe Structural Integrity Program
ATA	Air Transport Association of America
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Transport System
AWO	All Weather Operations
BCAR	British Civil Aviation Regulation
BS	British Standard
C of G	Centre of Gravity
CAA	Civil Aviation Authorities

CAA	Civil Aviation Administration
CAF	Chief of the Air Force
CAS OPS	Chief of Air Staff Operations
CCA	Common Cause Analysis
CDR	Critical Design Review
CEO	Chief Executive Officer
CFDS	Chaff and Flare Dispensing System
CFE	Customer Furnished Equipment
CFIT	Controlled Flight Into Terrain
CFT	Certificate for Flight Trials
CHIRP	Confidential Hazard & Incident Reporting Program
CIDS	Critical Item Development Specification (C-Spec)
CM	Configuration Management
CMP	Configuration Management Plan
CofC	Certificate of Conformance
COTS	Commercial Off The Shelf
COTS	Consumed Off The Shelf
CS	Certification Specification
CSANDF	Chief of the South African National Defence Force
CSCI	Computer Software Configuration Items
CVR	Cockpit Voice Recorder
CWAP	Caution and Warning Advisory Panel
DA	Design Authority
DAA	Design Approval Authority
DAFA	Director Air Force Acquisition
DAL	Development Assurance Level
DD	Dependence Diagram
DDP	Declaration of Design and Performance
DEF STAN	Defence Standard
DME	Distance Measuring Equipment
DoD	Department of Defence
DRACAS	Data Reporting, Analysis and Corrective Action System
DSI	Director System Integration
EA	Engineering Authority
ECCM	Electronic Counter Counter Measures
EDA	Excess Defence Articles
EFIS	Electronic Flight Instrumentation System
EIDS	Engine Instruments Display System
ELT	Emergency Locator Transmitter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ENSIP	Engine Structural Integrity Program
ESDU	Electronic Safety Disarm Unit
ETA	Event Tree Analysis
EUROCAE	European Organisation for Civil Aviation Equipment

EW	Electronic Warfare
F	Frequency (i.e. the average rate at which an event will occur)
FAA	Federal Aviation Administration
FAD	First Aircraft Delivery
FADEC	Full Authority Digital Engine Control
FAR	Federal Aviation Regulations
FCS	Flight Control System
FDR	Flight Data Recorder
FOD	Foreign Object Damage
FDR	Final Design Review
FHA	Functional Hazard Assessment
FL	Flight Level
FMC	Flight Material Certificate
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effect and Criticality Analysis
FMS	Flight Management System
FRACAS	Failure Reporting, Analysis and Corrective Action System
FTA	Fault Tree Analysis
FTRR	Flight test readiness Review
GCU	Generator Control Unit
GM	Guidance material
GPS	Global Positioning System
GSN	Goal Structuring Notation
H/W	Hardware
HAZOPs	Hazard and Operability Study
HF	High Frequency
HIRF	High Intensity Radio Frequency
HSA	Hard Systems Approach
HSC	Health and Safety Commission
HSE	Health and Safety Executive
HSWA	Health and Safety at Work Act
HUMS	Health & Usage Monitoring System
ICAO	International Civil Aviation Organisation
ICD	Interface Control Document
IEC	International Electrotechnical Commission
IFF	Identification Friend or Foe
IFR	Instrument Flight Rules
ILS	Instrument Landing System
ILS	Integrated Logistic Support
IMC	Instrument Meteorological Conditions
INS	Inertial Navigation System
IPT	Integrated Project Team
ISP	Integrated Support Plan
ISSA	Interim System Safety Assessment
JAA	Joint Aviation Authorities

JAR	Joint Aviation Regulations
LOC	Loss of Control
LRU	Line Replaceable Unit
LSP	Logistic Support Plan
MA	Markov Analysis
MAA	Military Airworthiness Authority
MAWS	Missile Approach and Warning System
MCDU	Multi-functional Control and Display Unit
MEL	Minimum Equipment List
MIL-STD	Military Standard
MMEL	Master Minimum Equipment List
MoD	Ministry of Defence
MRI	Master Record Index
MTBF	Mean Time Between Failures
NAA	National Approval Authority
NPA	Notice for Proposed Amendment
NPRM	Notice of Proposed Rule Making
OEM	Original Equipment Manufacturer
OHSA	Occupational Health and Safety Act
OPS	Operations
P	Probability of occurrence
p	Probability per unit time (usually per hour)
PCCB	Project Configuration Control Board
PDR	Preliminary Design Review
PE	Professional Engineer
PECP	Project Engineering Change Proposal
PIDS	Prime Item Development Specification (B-Spec)
PRA	Particular Risk Analysis
PSSA	Preliminary System Safety Assessment
Q	Probability of event not occurring
QA	Quality Assurance
QB	Qualification Board
QMG	Quality Management Group
R	Reliability (i.e. the probability of success)
ROTE	Release for Operational Test and Evaluation
RTCA	Radio Technical Commission for Aeronautics
RTCA	Requirements and Technical Concepts for Aviation
RTS	Release to Service
S/W	Software
SAAF	South African Air Force
SAE	Society of Automotive Engineers (Aerospace Division)
SAPT	South African Project Team
SAS	Software Accomplishment Summary
SDRL	Supplier Data Requirements List
Sec Def	Secretary of Defence

SELCAL	Selective Calling
SIL	Safety Integrity Level
SMP	Safety Management Plan
SMS	Safety Management System
SOP	Standard Operating Procedures
SOW	Statement of Work
SQA	Software Quality Assurance
SRS	Software Requirement Specification
SSA	System Safety Assessment
SSAP	System Safety Assessment process
t	Elapsed time
T	Fixed period of time
TACAN	Tactical Air Navigation System
TCAS	Traffic Collision Avoidance System
TRU	Transformer Rectifier Unit
TWA	Transworld Airlines
UK	United Kingdom
URS	User Requirement Statement
USA	United States of America
USAF	United States Air Force
VDD	Version Description Document
VFR	Visual Flight Rules
VHF	Very High Frequency
VOR	VHF Omni-directional radio ranging
ZHA	Zonal Hazard Assessment

Definitions

Accident An unplanned event or series of events resulting in death, injury, occupational illness to people, or damage to the environment.

Accident severity category Qualitative description of worst-case credible consequences of hazard.

Airworthiness The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function (SAE ARP4754 p. 75).

The ability of an air system to operate without significant hazard to aircrew, ground crew, passengers (where relevant) or to the general public or friendly military personnel over which such airborne systems are flown. The concept of airworthiness defines the condition of an air system/subsystem, and supplies the basis for the judgement of its suitability for flight operations in its intended role and application, in that it has been designed and manufactured, and is managed, maintained and operated, to approved standards and limitations, by competent and approved individuals, who are acting as members of approved organisations, and whose work is authorised, certified as correct, and accepted on behalf of the Air Force (SAAF).

ALARP As low as reasonably practicable defines the region in which the risk taken is acceptable only if justified by the benefits, and where the cost of further risk reduction would exceed the benefits.

Analysis Generally implies a more specific, more detailed investigation. The terms ‘analysis’ and ‘assessment’ have broad definitions and the two terms are to some extent interchangeable. However, the term analysis generally implies a more specific, more detailed evaluation, while the term assessment may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application, e.g., fault tree analysis, Markov analysis, preliminary system safety assessment, etc. (AMC to CS25.1309).

Annunciated Warning or indication of failure is given to the flight crew in sufficient time to react to the failure (AMC to CS25.1309).

Annunciation Any form of visual or aural presentation designed to draw the attention of the flight or ground crew to an abnormal system operating condition (AMC to CS25.1309).

Assessment An assessment is a more general, or broader, evaluation and may include one or more types of analysis. The terms 'analysis' and 'assessment' has broad definitions and the two terms are to some extent interchangeable. However, the term analysis generally implies a more specific, more detailed evaluation, while the term assessment may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application, e.g., fault tree analysis, Markov analysis, preliminary system safety assessment, etc. (AMC to CS25.1309).

Average probability per flight hour A representation of the number of times the subject failure condition is predicted to occur during the entire operating life of all aeroplanes of the type divided by the anticipated total operating hours of all aeroplanes of that type (AMC to CS25.1309). (Note: the average probability per flight hour is normally calculated as the probability of a failure condition occurring during a typical flight of mean duration divided by that mean duration.)

Candidate certification maintenance requirements (CCMR) A periodic maintenance or flight crew check may be used in a safety analysis to help demonstrate compliance with JAR 25.1309(b) for hazardous and catastrophic failure conditions. Where such checks cannot be accepted as basic servicing or airmanship they become candidate certification maintenance requirements (CCMRs) (AMC to CS25.1309). (Note: AMC 25.19 defines a method by which certification maintenance requirements (CMRs) are identified from the candidates. A CMR becomes a required periodic maintenance check identified as an operating limitation of the type certificate for the aeroplane.)

Certification Certification means the legal recognition by the certification authority that a product, service, organisation or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organisation or person and the formal recognition of compliance with the applicable requirements by issue of a certificate, licence, approval or other documents as required by national laws and procedures. In particular, certification of a product involves:

i The process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety.

ii The process of assessing an individual product to ensure that it conforms with the certified type design.

iii The issue of any certificate required by national laws to declare that compliance or conformity has been found with standards in accordance with items (i) or (ii) above (ARP4754).

Certification is the end result of a qualification process. It is the act whereby the design, manufacture and engineering quality of a product is endorsed. It entails the legal recognition by the certification authority that a product, service, organisation, or person complies with the requirements.

Check An examination (e.g., an inspection or test) to determine the physical integrity and/or functional capability of an item (AMC to CS25.1309).

Complex A system is complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods (AMC to CS25.1309). Applicable to systems whose architecture and logic are difficult to comprehend without the aid of analytical tools (e.g. FMEAs, FTAs, RBDs, etc.) and whose safety cannot be shown solely by tests.

Component A 'component' is any software or equipment that would normally be part-number-controlled at the aircraft level and are applicable to all aircraft systems and associated non-structural components including the interfaces with structural components and items consumed by the systems, such as lubrication, fuel, and hydraulic fluid. These part numbers are typically shown on the system or airplane-level installation drawings (ANM-03-117-10, p. 2).

Conclusion A judgement or statement arrived at by any reasoning process (*Oxford English Dictionary* 1991).

Condition An existing or potential state such as exposure to harm, toxicity, energy source, activity, etc.

Contributing factors Other conditions (whether normal states/events or coincident failures) which must hold for a given event to lead to a hazard or accident.

Conventional A system is considered to be conventional if its functionality, the technological means used to implement its functionality, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly used (AMC to CS25.1309).

Cut sets Ways in which failure can occur. Used in fault tree analysis.

Design The whole intellectual process of converting a requirement into a set of manufacturing drawings.

Design appraisal This is a qualitative appraisal of the integrity and safety of the system design (AMC to CS25.1309).

Design rigour Extent (quantity and quality) of effort during the design process.

Detected Failure is detected by the function or system and some mitigating action is automatically implemented by the function or system, which may involve annunciation of the failure (AMC to CS25.1309).

Development assurance All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis (AMC to CS25.1309).

Development assurance level A (qualitative) specification or description of how much reliance will be placed on a particular system function. Used to prescribe the level of rigour which must be applied when developing the function.

Display Any form of visual presentation of system operation information to the flight or ground crew (AMC to CS25.1309).

Diversion A diversion is the landing of an aircraft at an airport other than the airport of origin or destination (AMC to CS25.1309).

Erroneous indication A display where a difference of scale exists between the actual and displayed values (AMC to CS25.1309).

Error An omission or incorrect action by a crew member or maintenance personnel, or a mistake in requirements, design, or implementation (AMC to CS25.1309).

An act that through ignorance, deficiency, or accident departs from or fails to achieve what should be done. Errors can be predictable and random. Errors can also be categorised as primary or contributory. Primary errors are those committed by personnel immediately and directly involved with the accident. Contributory errors result from actions on the part of personnel whose duties preceded and affected the situation during which the results of the error became apparent. The difference between a computed, observed, or measured value or condition and true, specified, or theoretically correct value or condition. A mistake in engineering, requirement specification, or design, implementation, or operation which could result in a failure, and/or contributory hazard. There are four types of human errors:

1. omission
2. commission
3. sequence
4. timing.

Event An occurrence which has its origin distinct from the aeroplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage (AMC to CS25.1309).

Explosion proof The item is designed to withstand an internal explosion; designed to vent explosive gases below ignition temperature.

Fail-operational A characteristic in design which permits continued operation in spite of the occurrence of a discrete malfunction.

Fail-safe A characteristic of a system whereby any malfunction affecting the system safety will cause the system to revert to a state that is known to be within acceptable risk parameters.

Fail-soft Pertaining to a system that continues to provide partial operational capability in the event of a certain malfunction.

Failure An occurrence which affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). (Note: errors may cause failures, but are not considered to be failures (ACJ25.1309).

The inability of a system, sub-system, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

The termination of the ability of an item to perform its intended function(s), i.e., a loss of function or a malfunction. Failures of sub-components, safety features, or consumable items associated with a part-number-controlled component are considered within the context of the higher-level component failure effect. The failures to be considered are based on the most severe aeroplane-level effect that cannot be reasonably ruled out by knowledgeable persons (ANM-03-117-10, p. 2).

Failure condition A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events (AMC to CS25.1309).

Failure mode The way in which the failure of an item occurs.

False indication A display where logical difference exists between actual and displayed conditions (AMC to CS25.1309).

Formal qualification The process that allows the determination of whether a configuration item complies with the requirements allocated to it.

Formal qualification review Formal evaluation by top management of the status and adequacy of the quality system in relation to quality policy and objectives.

Formal verification The process of evaluating the products of a given phase using formal mathematical proofs to ensure correctness and consistency with respect to the products and standards provided as input to that phase.

Fracture mechanics In materials science fracture mechanics applies the physics of stress and strain, in particular the theories of elasticity and plasticity, to the microscopic crystallographic defects found in real materials in order to predict the macroscopic mechanical failure of bodies. In modern materials science, it is an important tool in improving the mechanical performance of materials and components.

Frequency The expected number of occasions of the event per unit time (usually year, or hour, or product lifetime). In reliability analysis this is also known as 'failure rate'.

Hazard Any real or potential condition that can cause injury, illness, or death to personnel, damage to or loss of a system, equipment or property, or damage to the environment (MIL-STD-882D).

A set of conditions in the operation of a product with the potential for initiating or contributing to events that could result in personal injury, damage to property or harm to the environment.

Hazard analysis (HA) A generic term describing a whole collection of techniques whose combined strengths have a good chance of revealing most of the hazards. The techniques chosen depend upon the industry, stage of the project, the information available and the complexity and criticality of the equipment.

Hazardous material Any substance that, due to its chemical, physical, or biological nature, causes safety, public health, or environmental concerns that would require an elevated level of effort to manage (MIL-STD-882D).

Highly integrated Refers to systems that perform or contribute to multiple aircraft level functions.

Inadvertent An inadvertent action may be performed by the pilot who did not mean to do it (unintended but demanded operation). This term is normally used to consider the consequences of an unintended action by a crew member (ground, flight or cargo crew) (AMC to CS25.1309).

Incident A near miss accident with minor consequences that could have resulted in greater loss. An unplanned event that could have resulted in an accident, or did result in minor damage, and which indicates the existence of, though may not define, a hazard or hazardous condition. Sometimes called a mishap.

Initiating events Initiating events; initiator; the contributory hazard; unsafe act and/or unsafe condition that initiated the adverse event flow, which resulted in the hazardous event under evaluation; also see root cause.

Inspection A static technique that relies on visual examination of development products to detect deviations, violations or other problems.

Installation appraisal This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service (AMC to CS25.1309).

Item Any level of hardware assembly (system, sub-system, equipment, component, etc.) including associated software or firmware.

Latent Present and capable of becoming, though not now visible or active.

Latent failure A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one which would in combination with one or more specific failures or events result in a hazardous or catastrophic failure condition (AMC to CS25.1309).

Life cycle All phases of the system's life including design, research, development, testing and evaluation, production, deployment (inventory), operations and support, and disposal (MIL-STD-882D).

Likelihood Likelihood defines in quantitative or qualitative terms, the estimated probability of the specific hazardous event under study. Likelihood is one element of associated risk (the other being severity). Fault trees and other models can be constructed and individual hazard probabilities are estimated, and likelihood can be calculated via Boolean Logic.

Maintainability The ability of an item to be retained in or restored to a specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures, resources and equipment at each prescribed level of maintenance and repair.

Malfunction Failure to operate in the normal or usual manner. Any anomaly which results in system deviation.

Mean time between failures (MTBF) Indicates mean life of repairable items. As the reciprocal of failure rate, MTBF is an alternative for describing the random failure portion of the bath-tub curve.

Mean time to failure (MTTF) Indicates mean life of non-repairable items.

Methodology A particular procedure or set of procedures.

Mishap An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882D).

Mishap risk An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence (MIL-STD-882D).

Mitigation Any downstream circumstances or functions that reduce the probability of a malfunction escalating to an accident.

Objective evidence Information that can be proved true, based on facts obtained through observation, measurement, test or other means.

Optimum safety The associated risks that have been identified have been accepted provided that all identified controls are implemented and enforced.

Pareto principle In 1906, Italian economist Vilfredo Pareto created a mathematical formula to describe the unequal distribution of wealth in his country, observing that twenty per cent of the people owned eighty per cent of the wealth. In the late 1940s, Dr Joseph M. Juran inaccurately attributed the 80/20 rule to Pareto, calling it Pareto's Principle. While it may be misnamed, Pareto's Principle or Pareto's Law as it is sometimes called, can be a very effective tool to help effective management. As a result, Dr Juran's observation of the 'vital few and trivial many', the principle that 20 per cent of something always are responsible for 80 per cent of the results, became known as Pareto's Principle or the 80/20 Rule.

Partitioning Partitioning is a technique for providing isolation between functionally independent software components to contain and/or isolate faults and potentially reduce the effort of the software verification process.

Path sets Routes to success.

Phase Defined segment of work. (Note: a phase does not imply the use of any specific life-cycle model, nor does it imply a period of time in the development of a product.)

Practice Recommended methods, rules, and designs for voluntary compliance.

Premise A previous statement or proposition from which another is inferred or follows as a conclusion (*Oxford English Dictionary* 1991).

Probability The probability of the event occurring in a given time period or the conditional probability of it occurring given that a previous event has occurred.

Process Set of interrelated resources and activities, which transform inputs into outputs.

Product Any system in the form of an integrated platform, facility, sub-system, equipment, software, or service, which is either to be provided to a customer or taken into service by the company as an entity, or being developed for such purposes.

Product liability Generic term used to describe the onus on a producer or others to make restitution for loss related to personal injury, property damage or other harm caused by a product.

Product safety The risks of hazards to operators, the public, property and the environment, when used for their intended purpose. Or in any reasonably foreseeable way, including disposal of the product.

Product service history Historical data generated by activities at the interface between the supplier and the customer and by supplier internal activities to meet the customer needs regarding the quality, reliability and safety trends of the product or service.

Qualification Qualification is the systematic process during the design of an aircraft or airborne system, of demonstrating conformance to the design objective/requirement and a set of specific and predetermined airworthiness regulations for a specific type and category of aircraft. These regulations, (such as FARs, DEF STAN 00-970, etc.), are determined by the relevant airworthiness authority. The qualification process is satisfied as soon as it is objectively proven that the laid down regulations and requirements for that specific aircraft type and category have been satisfied so as to ensure continuous airworthiness.

Qualification process Process of demonstrating whether an entity is capable of fulfilling specified requirements.

Qualitative Those analytical processes that assess system and aeroplane safety in an objective, non-numerical manner (AMC to CS25.1309).

Quantitative Those analytical processes that apply mathematical methods to assess system and aeroplane safety (AMC to CJ25.1309).

Random failure Failure that results from a variety of degradation mechanisms in the hardware. Failure rates arising from these are assumed to be constant over the useful life of the item and can be quantified with reasonable accuracy.

Redundancy Multiple independent methods incorporated to accomplish a given function, each one of them is sufficient to accomplish the function or flight operation (AMC to CS25.1309).

Reliability The probability ratio that a system or product will perform in a satisfactory manner under stated conditions for a stated period of time, assuming it was in proper condition at the mission beginning.

Requirements Statements describing essential, necessary or desired attributes.

Requirements specification Specification that sets forth the requirements for a system or system component.

Risk An expression of the possibility and impact of an event in terms of hazard severity and hazard probability. In other words, it is the combined effect of the probability of occurrence of an undesirable event, and the severity of that event.

Safe life The safe life design technique is employed in critical systems which are either very difficult to repair or may cause severe damage to life and property. These systems are designed to work for years without requirement of any repairs.

Safety Freedom from those conditions that can cause death, injury, occupational illness or damage to or loss of property, or damage to the environment. It is the state in which risk is lower than the boundary risk. The boundary risk is the upper limit of acceptable risk. It is specific for a technical purpose or state (SAE ARP 4754, p. 80).

Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (MIL-STD-882D).

Safety assessment The safety assessment is a structured body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment. It is a collection of documents that, taken together, provide objective evidence that all reasonable steps were taken to ensure product safety. It may also provide data that the customer finds helpful throughout the life of the product. Note that the safety assessment is applicable to one specific point in time only and is a deliverable to the system manager/owner.

Safety case The Health and Safety Commission defines a safety case as: ‘a suite of documents providing a written demonstration that risks have been reduced as low as is reasonably practicable. It is intended to be a living dossier which underpins every safety-related decision made by the licensee.’

Note that it is a living dossier, which implies that it needs continuous management to ensure its currency and validity. This implies that it falls within the remit of the system owner/manager. The safety case(s) of an organisation are subordinate to the corporate safety management system but are used to interact with the SMS (i.e.

the SMS is the facilitator of a live safety case; the safety case, in turn, can receive inputs from a safety assessments.

Safety critical A term applied to a condition, event, operation, process or item which is essential to safe system operation or use (e.g. safety critical function, safety critical path, safety critical item, etc.). All interactions, elements, components, subsystems, functions, processes, interfaces, within the system that can affect a predetermined level of risk.

Safety critical computer software module Those computer software modules whose errors can result in a hazardous or catastrophic or critical severity.

Safety critical item An item whose failure can cause hazards of catastrophic or critical severity.

Safety incident Any unplanned event or series of events, other than an actual accident, which have the potential to cause death, injury, or occupational illness to people; or otherwise cause damage to the environment.

Safety integrity level (SIL) The likelihood of a safety related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. An indication of the required level of protection against failure (degree to which a component must be free from flaws).

Safety management The application of engineering and management principles and techniques in order to optimise all aspects of safety within constraints of operational effectiveness, time and cost. It is a systematic and explicit approach to managing safety. A methodology that drives safety as a measurable design parameter (ensuring that an acceptable level of safety is designed into the product) and provides a form of measure of that achievement.

Safety management system A 'safety management system' is an explicit element of the corporate management responsibility which sets out a company's safety policy and defines how it intends to manage safety as an integral part of its overall business. The SMS is a management tool for executing safety throughout the life cycle of a project.

Safety monitoring Safety monitoring, as related to digital systems, is a means of protecting against specific failure conditions by directly monitoring a function for failures that could contribute to the failure condition. Monitoring functions may be implemented in hardware, software, or a combination of both. Through the use of monitoring techniques, the software level of the monitored function may be reduced to the level associated with the loss of its related function. To allow this level of reduction, there are four important attributes of the monitor that should be determined.

1. Software level. Safety monitoring software is assigned the software level associated with the most severe failure condition category for the monitored function.
2. System fault coverage. Assessment of the system fault coverage of a monitor ensures that the monitor's design and implementation are such that the faults which it is intended to detect will be detected under all necessary conditions.
3. Independence of function and monitor. The monitor and protective mechanism are not rendered inoperative by the same functional failure condition that causes the hazard.

4. Hardware integrity. The monitor hardware integrity will need to be commensurate with the hazard. A configuration which requires high-integrity monitor software but proposes low-integrity monitor hardware would be unacceptable.

Severity An expression of consequence used in the assessment of a specific hazard.

Severity category Qualitative description of worst case credible consequences of hazard.

Sub-system An element of a system that, in itself, may constitute a system. A grouping of items satisfying a logical group of functions within a particular system (MIL-STD-882D).

System A combination of components, parts, and elements which are interconnected to perform one or more functions (AMC to 25.1309).

An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective (MIL-STD-882D).

System safety The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle (MIL-STD-882D).

A standardised management and engineering discipline that integrates the consideration of man, machine, and environment in planning, designing, testing, operating, procedures, and acquisition projects.

System safety is the systematic process of the identification and resolution of hazards during the life cycle of an aircraft or airborne system. The resolutions of identified hazards are basically through three means:

1. the elimination (normally by design) of an identified hazard
2. the control of a hazard during testing or operational usage of an aircraft, or airborne system
3. the acceptance of a hazard without any elimination or control action where the hazard criticality and probability is sufficiently low to be able to accept the risk.

System safety analysis The analysis of a complex system by means of methods, techniques, and/or processes, to comprehensively evaluate safety-related risks that are associated with the system under study.

System safety engineer An engineer qualified by appropriate credentials: training, education, registration, certification, and/or experience to perform system safety engineering should have an appropriate background and credentials directly related to system safety in order to practise in the field, i.e., CSP, PE, training, education, and actual experience.

System safety engineering An engineering discipline requiring specialised professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate, or reduce safety-related risks (refer MIL-STD-882D *et al.*).

System safety manager A person responsible for managing a system safety programme.

System safety working group A formally charted group of persons representing organisations associated with the system under study, organised to assist management in achieving the system safety objectives.

Systematic failures A failure caused by errors in the specification, design, construction operation or maintenance which cause the item to fail under some particular combination of inputs or conditions. All software failures are systematic failures.

Systems approach A step-by-step procedure for solving problems; a decision-making process which moves from the general to the specific; an iterative process.

Technical airworthiness A concept, the application of which defines the condition of an aircraft, and supplies the basis for judgement of the suitability for flight of that aircraft in that it has been designed, constructed, operated and maintained to approved standards by competent individuals, who are acting as members of an authorised organisation and whose work is both certified as correct and accepted on behalf of the regulatory authority.

Type certificate The type certificate is considered to include the type design, the operating limitations, the type certificate data sheet, the applicable requirements with which the authority records compliance, and any other conditions or limitations prescribed for the product in the appropriate regulatory code (JAR21.4).

Unanunciated No warning or indication is given to the flight crew, or warning/indication gives insufficient time for the flight crew to react to the failure (AMC to CS25.1309).

Uncommanded This term is used to consider the consequences of a system/equipment failure resulting in the 'unintended and undemanded' operation (AMC to CS25.1309).

Undetected Failure is not detected by the function or system or no timely mitigating action is possible, and the failure is not annunciated (AMC to CS25.1309).

Waiver A written authorisation by the engineering authority to accept an item (or limited quantity of), which during manufacture, or after submission for inspection or acceptance, is found to depart from specified requirements, but nevertheless is considered suitable for use 'as is' or after repair by an approved method. Also known as a concession.

References and further reading

AC20-138 (undated) *Airworthiness Approval of Global Positioning System (GPS) Navigation Equipment for use as a VFR and IFR Supplemental Navigation System,* FAA, US Department of Transportation.

AC 25.1309 –1A (undated) *System Design and Analysis*, Advisory Circular.

Aerospace International (2004) November, p. 8, Royal Aeronautical Society, London.

AMJ 25.1309 (2000) *System Design & Analysis,* (Amendment 16 Joint Aviation Authorities, October 1, Hoofddorp, Holland.

Angove, D. (1999) *Practical Safety Management*, Aviation Safety Management Conference, 20 May 1999, London, IBC UK Conferences Ltd, London.

ANM-03-117-10, *Identification of Flight Critical System Components*, FAA Memorandum (Draft), US Department of Transportation.

Arbuckle, P. D., Abbott, T. S., Schutte, P. C. (1998) *Future Flight Decks*, Paper Number 98-1.9.3, 21st Congress, International Council of Aeronautical Sciences, Melbourne, Australia, 13-17 September.

ASD-100-SSE-1 Rev 7D, *NAS Modernisation System Safety Management Programme,* US Dept of Transportation, FAA.

Ashford, R (1994) *The Need for Harmonisation,* The Future Airworthiness Regulatory Environment, 22 June, London, p. 17, Royal Aeronautical Society, London.

Ashford, R. (1998) Secretary General, JAA, Netherlands.

Australian Air Publication (AAP) 7001.054, *Airworthiness Design Requirements Manual.*

Avizienis, A. *et al*. (1996) *The N-Version Approach to Fault-Tolerant Software*, IEEE Transactions on Software Engineering, SE-11(12): 1491–1501, December.

Barnes, R. B. *et al*. *Retrofit to 'Classics*' and IEC, Geneva. *– the increasing need for human factors involvement*.

Boeing 2003 Statistical Summary (2004) May, www.boeing.com/news/techissues, Airplane Safety, Boeing Commercial Airplanes, P.O. Box 3707 M/S 67-TC, Seattle, Washington 98124-2207, USA (425) 237-1692.

Bradshaw, T. (1998) *System Safety,* Military Aircraft Airworthiness Course, Cranfield.

Brooker, P. (2004) *Delivering Safety in the Context of Environmental Restrictions,* CAA Paper 2004/8, www.caa.co.uk, July.

C-05-005-001/AG-001, *Technical Airworthiness Manual*, Canada National Defence, 2003-02-13.

CAP 549, *Master Minimum Equipment Lists (MMEL) and Minimum Equipment Lists (MEL),* (at www.caa.co.uk, Publications, Design and Production).

Card, S. K. *et al*. (1993) *The Psychology of Human-Computer Interaction*, Lawrence Erlbaum Associates, Inc.

Cherry, R. G. W. (1995) *The Probabilistic Approach to Safety – success or failure?*, Procs Instn Mech Engrs, Vol 209, I MechE.

Christy, R. J. (1994) *Safety Assessment of Aircraft Systems, The Application of Minimum Equipment Lists*.

Collins, P. H. and Perry, B. L. (2003) 'Systems and Avionics', *The Aeronautical Journal*, June, Royal Aeronautical Society, London.

Creasy, R. (1980) *Problem Solving, the Fast Way*. Proceedings of Society of Added-Value Engineers Conference, Irving, Texas: Society of Added-Value Engineers, pp. 173–175.

CS25, EUDecision no. 2003/2/RM, dd 17 Oct 2003, http://www.easa.eu.int/doc/Agency_Mesures/Certification_Spec/decision_ED_2003_02_RM.pdf.

Dallimore, C. (2003) *MoD Approach to Airworthiness in Safety Management Context,* What Price Aviation Safety Conference, Bristol, 22 June.

Daly, K. C. (1995) as reported on http://alumnus.caltech.edu/~rdv/comp-arch-storage/FAQ-2.jp.12.html (downloaded on 1 June 2005).

David, R. (2002) *An Introduction to System Safety Management & Assurance,* Issue 1 Advantage Technical Consulting, UK MoD Abbey Wood, Bristol, Feb.

DEF STAN 00-56, Iss 2, *Safety Management Requirements for Defence Systems,* 13 December 1996, UK Ministry of Defence.

DEF STAN 00-970 Iss 1 Amm 14, *Design and Airworthiness Requirements for Service Aircraft,* UK MoD, Abbey Wood, UK.

Dunn, M. B. (1998) *Certification and QA for future a/c.* 41st Annual International Air Safety Seminar on Futuristic Aircraft Technologies, Dec., RAeS, Hamilton Place, London.

Edwards, C. J. (1999) Extracts from a lecture given to the Aviation Safety Management Conference held in London, 20–21 May.

FAA System Safety Handbook, December 30, 2000. http://www.asy.faa.gov/Risk/SSHandbook/contents.htm

Fairfield, R. (2003) *High Quality Good Value Safety*, I-Mech E What Price Aviation Safety Conference, Bristol, 2003-06-11.

Falla, M. (1997) *Advances in Safety Critical Systems, Results and Achievements from the DTI/EPSRC R&D Programme in Safety Critical Systems,* June. http://www.comp.lancs.ac.uk/computing/resources/scs/#APPENDICES

Garland, D. J., Wise, J. A. and Hopkin, V. D. (1999) *Handbook of Aviation Human Factors,* IEA Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey.

Hadden-Cave (1999) 'Managing Safety', *Aerospace International*, July, RAeS, London.

Hamilton, D. B. and Bierbaum, C. R. (1990) Task Analysis/Workload (TAWL): A methodology for predicting operator workload. Proceedings of the Human Factors Society 34th Annual Meeting, San Monica: Human Factors and Ergonomics Society, pp. 1117–1121.

The Hazards Forum (2002) *Safety-Related Systems, Guidance for Engineers*, Aug, The Hazards Forum, Institute of Electrical Engineers, 1 Great George St, London, SW1P 3AA, ISBN 0 9525103 0 8. http://www.iee.org/policy/areas/scs/hazpub.cfm

Health and Safety Executive (1975) *The Flixborough Disaster: Report of the Court of Inquiry*, HMSO, ISBN 0113610750.

Helmreich, B. (1999) 'Managing Safety', University of Texas, as reported in *Aerospace International*, July.

Howard, R. (2000) 'Planning for Super Safety: The fail-safe dimension', *The Aeronautical Journal*, Royal Aeronautical Society, 4 Hamilton Place, London, Volume 104 Number 1041, Nov.

ICAO Airworthiness Manual (Doc No 9760) first edition 2001, International Civil Aviation Organisation, Toronto, Canada.

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, Institute of Electrical Engineers, Savoy Place, London, WC2R 0BL.

INT/POL/25/14, *JAA Interim Policy on Human Factors for Certification of Flight Decks,* adopted June 2001, JAA, Hoofddorp, The Netherlands.

ISO/IEC Guide 51:1999, *Safety Aspects – Guideline for their Inclusion in Standards*, ISO

JAR 25.1309, *Equipment, Systems And Installations* (Amendment 16), Joint Airworthiness Authorities, Hoofddorp, Netherlands.

JAR-MMEL/MEL, May 2000, Joint Aviation Authority Hoofddorp, Holland.

Jenkins, A. M. (1999) *The Basic Principle of a Safety Management System*, Aviation Safety Management Conference, 20 May 1999, London, IBC UK Conferences Ltd, London.

Johnson, C. W. (2003) *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*, University of Glasgow Press, Glasgow, Scotland, October. ISBN 0-85261-784-4. Free downloaded: http://www.dcs.gla.ac.uk/~johnson/book/

JSP553, *Military Airworthiness Regulations,* 1st Edition, Change 2 (27 Aug 2004), Chairman Defence Aviation Safety Board, Military Aviation Regulatory Group, UK Ministry of Defence.

Keely, T. (2000) *It Only Stands to Reason*, Focus on Commercial Aviation Safety, Iss 37 p. 6, Woking, Surrey.

Kelly, T. P. (1998) *Arguing Safety – A Systematic Approach to Safety Case Management*, DPhil Thesis YCST99-05, Department of Computer Science, University of York, UK. http://www.cs.york.ac.uk/ftpdir/reports/YCST-99-05.ps.gz University of Strathclyde, Ship Safety Management Training Course Notes, 1997.

Kelley, T. P. (2003) *Managing Complex Safety Cases,* Proceedings of the 11th Safety Critical Systems Symposium (p. 107), Bristol, UK, 406 Feb.

Kelly, T. and Weaver, R. (1994) *The Goal Structuring Notation – A Safety Argument Notation*, Department of Computer Science and Department of Management Studies, University of York, YO10 5DD UK. http://www-users.cs.york.ac.uk/~rob/papers/DSN04.pdf

Kirwan, B. and Ainsworth, L. K. (eds) (1992) *A Guide to Task Analysis,* London: Taylor and Francis.

Kuo, C. (1990) *Managing Ship Safety*, LLP Limited, ISBN 1-85-978841-6.

Kuo, C. (1997a) *Ship Safety Fundamentals Course*, Ministry of Defence and Det Norske Veritas, http://www.mod.uk/dpa/project_services/Ship_Safety_Management.htm

Kuo, C. (1997b) *Ship Safety Management Training Course*, Ministry of Defence and Det Norske Veritas.

Lloyd, E. and Tye, W. (1995) *Systematic Safety – Safety Assessment of Aircraft Systems,* Errington Print.

McLean, I. (1997) 'On moles and the habits of birds: the unpolitics of Aberfan; *20th Century British History,* 8, 285–309.

Markey, P. D. (1994) *The Military Regulation of Airworthiness, The Future Airworthiness Regulatory Environment*, 22 June, London, p. 21, Royal Aeronautical Society, London.

Matthews, S. (2004) 'The Changing Face of Safety', edited version of the 30th Sir Geoffrey de Haviland lecture at the Royal Aeronautical Society, 4 Hamilton Place, London in April 2004 and reported in *Aerospace International*, October.

Mauri, G. (2000) *Integrating Safety Analysis Techniques, Supporting Identification of Common Cause Failures,* University of York. http://www.cs.york.ac.uk/ftpdir/reports/YCST-2001-02.pdf

MIL-HDBK-217F, *Reliability Prediction of Electronic Components*, US Department of Defense, Rome Laboratory/ERSR, 425 Brooks Rd, Griffos AFB, NY 13441-4505.

Miller, C. O. (2003) *System Safety,* Proceedings of the 11th Safety Critical Systems Symposium (p. 105), Bristol, UK, 406 Feb.

MIL-STD-882C (1993) *System Safety Program Requirements, USA Department of Defence*, 19 January.

Murphy, C. S. (1991) *Hazard Analysis*. Paper presented at Design for Safety: Proceedings of One-Day Conference held at the Aeroplane and Armament Experimental Establishment, Boscombe Down, Thursday 11 April, Royal Aeronautical Society, London.

Notice for Proposed Amendment (NPA) 25F-281 Iss 3 dated 6/10/98, AA, Hoofddorp, The Netherlands.

Papoulis, A. (1984) *Probability, Random Variables, and Stochastic Processes,* 2nd edn, New York: McGraw-Hill, pp. 548–549.

Pfeiffer, P. E. and Schum, D. A. (1973) *Introduction to Applied Probability,* New York: Academic Press.

Passmore, J. (1999) *The Development of an Integrated Safety Management System for an Airline,* Presentation at IBC UK Conferences Ltd, 20 May.

Perry, B. L. (1998) *Handbook of Avionic and Related Standards for Civil Aircraft,* Civil Avionics Support Group, CASG/10/2/4 Issue 3, May.

Profit, R. (1999) *European Safety Regulation and Harmonization – The Impact on Safety Management*, IBC Safety Management Conference, 17 May.

Profit, R. (1999) Keynote Address: *European Safety Regulation and Harmonisation*, Aviation Safety Management Conference, 20 May, London, IBC UK Conferences Ltd, London.

Quintana R. and Nair A. (1997) *Continuous Safety Sampling Methodology,* PubMed Central (PMC), US National Institutes of Health, PMII 1062592.

Rasmussen, J. (1986) *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*. New York: North-Holland.

Ravden, S. J. and Johnson, G. I. (1989) *Evaluating Usability of Human Computer Interfaces*, Chichester: Ellis Horwood (see http://www.eurocontrol.int/hifa/public/standard_page/Hifa_HifaData_Ref.html#r)

Reason J. (1997) *Managing the Risks of Organisational Accidents*. Brookfield, VT: Ashgate. http://www.healthinsight.org/home_health/tips/assets/pdf/Tip%20of%20Month%20May.pdf
http://www.eurocontrol.int/eatmp/events/docs/ssap/Reason.ppt
http://www.aviation.unsw.edu.au/about/articles/swisscheese.html

Rhys, D. (2002) *An Introduction to System Safety Management & Assurance*, Advantage Technical Consulting for MoD Abbey Wood, Bristol, BS34 8JH.

RTCA-D0 178B, *Software Considerations in Airborne Systems and Equipment Certification,* Prepared by Technical Committee SC-167, December 1, 1992, RTCA Inc. 1140 Connecticut Avenue, N.W., Suite 1020 Washington, DC 20036-4001 USA.

SAE ARP 4754 Aerospace Recommended Practice (1996), *Certification Considerations for Highly Integrated or Complex Aircraft Systems,* The Engineering Society for Advanced Mobility Land Sea Air and Space, Warrendale, USA.

SAE ARP 4761 Aerospace Recommended Practise (1996), *Guidelines and Methods for Conducting the Safety Assessment on Civil Airborne Systems and Equipment,* The Engineering Society for Advanced Mobility Land Sea Air and Space, Warrendale, USA.

SAE ARP 5150, *Safety Assessment of Transport Airplanes in Commercial Service,* SAE Publications, 400 Commonwealth Drive, Warrendale, PA 15096-0001.

Senker, J. (1990) 'Technology and competitive strategy in food retailing', in Loveridge, R. and Pitt, M. (eds) *The Strategic Management of Technological Innovation,* Chichester, John Wiley.

Sherwin, R. (undated) Selected Topics in Assurance Related Technologies, Application of the Poisson Distribution, *START* Vol 9 Number 1, A publication of the DOD Reliability Analysis Center, http://rac.alionscience.com/pdf/POIS_APP.pdf.

Smith, D. (1999) *Making Sense of Disaster,* Aviation Safety Management Conference, 20 May 1999, London, IBC UK Conferences Ltd, London.

SRG (CAA Safety Regulatory Group) SMS Guidelines, Extract of, IBC Safety Management Conference, UK, 17 May 1999.

Tarrents, W. E. (1980) *The Measurement of Safety Performance*, Garland STPM Press.

TGL 26, *Guidance Documents for MEL Policy*, June 2004, Joint Aviation Authority Hoofddorp, Holland (at www.jaa.nl, Operations, JOEB)

Vicente, K. J. (1999) *Cognitive work analysis: Toward safe, productive, and healthy computer-based work*. Mahwah, NJ: Lawrence Erlbaum & Associates.

Weaver, R. A. and McDermid (2002) J.'*T P Kelly Software Safety Arguments: Towards a Systematic Categorisation of Evidence*' in Proceedings of the 20th International System Safety Conference (ISSC 2002), System Safety Society, Denver, Colorado, USA.

Weir, A. (2000) *The Tombstone Imperative – The Truth about Air Safety*, Pocket Books.

Williams, R. (2003) *Airworthiness: The Legal Issues and Awareness,* What Price Aviation Safety Conference, IMechE, Bristol, 11 June.

Index

Aberfan disaster (1966) 129
accident analysis 214
accident criteria 299–302
accident probability 44, 45, 68, 122
accident probability categories 46, 47, 300, 301
accident rate 204–5
accident sequence 60–4
accident sequence evaluation programme (ASEP) 214
accident sequence models 44–5, 299–300
accident severity 44, 45, 46, 74
accident severity categories 46, 122, 300–1, 324
accidents 141, 200–1, 324
  and hazards 69, 70, 71, 73
  major accidents 129–32
  see also under individual accidents
action error analysis 214
active failures 76, 83
active redundancy 96–7
Advisory Committee on Major Hazards (ACMH) 130, 133
air traffic management risk matrix 304–5
air transport oversight system (ATOS) 194
airworthiness 24–6, 324
  design standards and 24–5
  system safety and 25–6
airworthiness criteria
  ICAO 297
  Ministry of Defence 299, 302–4
ALARP (as low as reasonably practicable) 2, 141, 145–6, 207, 324
  air traffic management risk matrix 304, 305
  risk-based approach 46–9, 50, 54
altitude display 54, 65
analysis 324
annunciated 324
annunciation 324
anthropometrical studies 266
Antonov An-24 accident, Ndjole (2004) 78
Antonov An-28 accident, Tallinn (2004) 76
approved code of practice (ACOP) 39
architectural design, quality of 99–101
argument *see* safety argument
ARIBA project 304–5
as far as reasonably practicable 7–8, 48
as low as reasonably practicable *see* ALARP
assembly/unit 107
assessment 324–5
ATC Electronic Checklist 222
ATLAS 214
audit trail 207
automation 102, 208
average flight 166–7
average probability per flight 167
average probability per flight hour 168, 325
aviation trends 204–5
avoidance of risk 50, 94

BAC1-11 accident, Blossburg (1967) 77
back-up systems 96–7
  see also redundancy
Balfour Beatty 5
Ballard, David 7
barrier analysis 214
Basic Regulation 33, 34, 35
bathtub curve 151–2
Bayesian belief networks (BBNs) 214–16
Bedford scale 216
Bellcore TR332 approach 216
benefits 18
benefits analysis 216
bent pin analysis 218
blame-free environment 196

Boeing 707 accident, Paris (1973) 89
Boeing 747-200F accident, London (1999) 77
Boeing 747-400 accident, Jeddah (1999) 82
bottom-up analysis approach ('hardware' method) 119, 218
boundary risk 18–19
bow tie analysis 218–20
brainstorming 220
British Rail 131–2
'burn-in' failures 151–2
business risk 44

cable failure matrix analysis 220
candidate certification maintenance requirements (CCMR) 325
cascade failures 79, 224
catastrophic accidents/hazards 46, 59, 61, 66, 67
causal analysis 220
causal techniques 90
cause-and-effect diagrams 256
cause consequence analysis 220
causes, and hazards 69–74
certification 40, 325
 system safety and 25–6
certification by design 40
certification specifications (CS) 34, 35
Challenger Shuttle disaster (1986) 73–4, 195
change analysis 222
checkability 98
checklists 90, 222
checks 325
chi-squared method 224
Civil Aviation Act (1982) 39
Civil Aviation Authority (CAA) (UK) 34
civil liability 2–4
 organisational response 8–9
civil regulatory authorities 28–34
 EASA 29, 32, 33–4, 35
 FAA 21, 23–4, 29, 31–2
 ICAO 28, 29–30
 JAA 21, 29, 32–3
Clapham Junction disaster (1988) 131–2
Code of Professional Practice on Engineers and Risk Issues 13–14
cognitive event tree system (COGENT) 224
cognitive reliability assessment technique (CREATE) 224
cognitive work analysis (CWA) 224
collaboration 196
collaborative projects 210–11
combined combat forces 109
combined occurrences 157–8
common cause analysis (CCA) 224–6
common cause failures 78–9, 102–3, 162–3, 224
common mode analysis (CMA) 226
common mode failures 78–9, 102–3, 162–3, 224
common part failures 78, 224
comparator 85
comparison-to-criteria 226
competency 200
complex systems 104, 183, 208, 325–6
component manufacturers 10
components 107, 109, 317, 326
 failures due to 94
 in parallel 159
 safety critical 317–21, 332
 in series 158–9
computerised control systems 102, 208
conclusions 326
Concorde SST accident, Paris (2005) 79
condition 326
conditional active redundancy 97
confidence levels 176
confined space safety 226
consequence 18
 relationship to frequency 59, 184
 suddenness of 18
consequence analysis 226
consequence probability 66–8, 293
consequence techniques 91
Consumer Protection Act (1987) 3, 4
 organisational responses 9–11
contingency analysis 228
continuous safety sampling methodology (CSSM) 228
contracts 11–13
contributing factors 326
contributory errors 327
control 18
control rating code 228
Convention on International Civil Aviation (Chicago Convention) 29
conventional systems 326
corporate killing 5, 6
corporate liability 1
corrosion prevention 179
cost 17
cost benefit analysis 48, 54, 228
crew operations 98, 101–2, 168–9
criminal liability 1–2
 organisational response 7–8

critical design review (CDR) 126
critical incident technique 230
critical path analysis 230
critical risks 46
CRT display checklist 222
culture, safety 195–6, 209–10
cut sets 326
cyclical loading 96, 101
cyclohexane 129–30

damage modes and effects analysis 230
damage protection redundancy 100–1
damage tolerance 98
dangerous systems, legal liability for 6–7
DC8 accident, Toronto (1970) 81
DC10 accident, Chicago (1980) 88–9
DC10 accident, Paris (1974) 78
deactivation safety analysis 230
decision analysis 230–1
deductive analysis 230
DEF-STAN 00-55 38
DEF-STAN 00-56 38, 118, 300, 301, 302
defect reporting analysis and corrective action system (DRACAS) 230
defective products 3–4
defective systems, legal liability for 6–7
Defence Aviation Safety Board (DASB) 37
Defence Standards 21, 38
degraded functionality/performance 82–4
Delta Airlines 737 accident, Salt Lake City (2004) 84
dependence diagrams 232
dependent events 155
dependent failures 78–80
depth of analysis 296–7, 298
design 326
  deficiencies 85, 87, 89, 94
  design life cycle 124–6
  designed failure path and damage tolerance 98
  designed integrity and quality 96
  for minimum risk 52
  quality of architectural design 99–101
  system safety assessment report 123–6
  system safety design requirements 106–7
design appraisal 232, 326
design for certification 40
design rigour 326
design standards 24–5
detected failures 326
development assurance 326
development assurance levels (DALs) 90, 170, 297, 303, 305, 326
development process, safety during 112–14
development risk defence 10
digital systems 169–71
directors 7
display 326
dissimilar redundancy 80
diversion 326
documentation 9, 14, 15, 200
dormant failures *see* latent failures
double failure 168–9
dread 18
duty of care 3, 12–13
dynamic workload scale 232

Edwards vs *The National Coal Board* 49
electromagnetic compatibility analysis 232
electronic equipment 178–9
elimination of risk 50, 52
emergence, problems of 208
employees 7
endogenous hazards 74
energy analysis 232
energy trace analysis 232–4
energy trace and barrier analysis 234
energy trace checklist 234
engineering
  engineers and legal framework 13–15
  safety engineering competence 209
Engineering Council 13, 15
engineering register 14
environmental analysis 234
environmental deficiencies 87, 94
environmental risk analysis 234
equipment failures and faults 76–80
  active 76, 83
  independent vs dependent 77–80
  latent 77, 83, 164, 329
  obvious vs non-obvious 77
  random 80, 152, 331
  wear-out 80, 151–2
Ergonomics Audit Program (ERNAP) 222
erroneous indication 326
error tolerance 99
errors 326–7
  human error *see* human error
established equivalence 21
European Aviation Safety Agency (EASA) 29, 32, 33–4, 35
European Civil Aviation Conference (ECAC) 32
European Union (EU) 33
  Basic Regulation 33, 34, 35
  Implementation Regulations 29, 34, 35
  ‘Sevesco Directive’ 130

event and causal factor charting 234
event probabilities, aircraft-related 171, 173–4
event tree analysis (ETA) 236
events 327
exclusion clauses 12
exogenous hazards 74
explosion proof 327
Explosives Act (1875) 39
explosives safety analysis 236
exponential failure curve 153–4
exposure, time of 164–8
extended master plan logic diagram (MPLD) 236–7
external events analysis 236–8
external influences 101
external suppliers 199
extremely improbable 59, 61, 62, 63, 67, 293
extremely remote probability 59, 61, 62, 63, 67, 293

facility system safety analysis 238
factors of safety 99
fail-operational 327
fail-safe 57, 77, 78, 94–103, 327
  applying fail–safe principles 99–102
    crew operations 101–2
    external influences 101
    quality of architectural design 99–101
  definition 95
  principles 96–9
fail-soft 94–5, 327
failure condition tolerability matrix 304, 305
failure conditions 327–8
  analysis approaches 118–19
failure containment 98
failure-free operation 82–3
failure logic analysis for system hierarchies (FLASH) 238
failure mode and effects analysis (FMEA) 104, 238
failure mode and effects summary (FMES) 238
failure modes 159, 206, 328
failure modes, effects and criticality analysis (FMECA) 238
failure propagation and transformation notation (FPTN) 240
failure rate
  bathtub curve 151–2
  models 181
  relationship to probability and MTBF 152–4
failure reporting analysis and corrective action system (FRACAS) 230–1
failure sequences 163–4
failure severity categories 60, 61, 66, 120, 294, 295
failure severity levels 57–60, 66–8, 74
failure-survivability 99
failure warning/indication 97–8
failures 327
  defences against 94–5
  equipment failures and faults 76–80, 83
  reasons for failure 94
  safety critical system components 312
  systemic 85–90, 334
false indication 328
familiarity 17
fatigue 96, 101
fatigue strength 179
fault hazard analysis 240
fault isolation methodology 240
fault liability 2–4
fault masking 94
fault tolerance 94–5, 99
fault tree analysis (FTA) 163–4, 240–2
fault trees 170–1
Federal Aviation Administration (FAA) 21, 23–4, 29, 31–2, 194
  internal safety management system 66, 67
  safety critical system components 312
Federal Aviation Regulations (FARs) 29, 30, 32, 39
Federal Railroad Administration 23
final design review (FDR) 126
fines 5
fire hazards analysis 242
fishbone diagrams 256
flight procedures 98, 101–2, 168–9
flight trials readiness review (FTRR) 126
Flixborough disaster (1974) 129–30
flow analysis 242
formal qualification 328
formal qualification review 328
formal verification 328
formalised rules 20
fracture mechanics 96, 328
frequency 17, 328
  relationship to consequence 59, 184
frequency-estimating methods 171, 172
frequent probability 61, 62, 63, 293
full active redundancy 97
function and task analysis 242–4
functional analysis system technique (FAST) 244

functional block diagrams 111
functional failure analysis (FFA) *see* functional hazard analysis
functional failure path analysis 244
functional hazard analysis (FHA) 117, 118, 120, 244
functional safety 20
functional verification 98
functionality, degraded 82–4, 94

gathered fault tree combination 244
generic error modelling system (GEMS) 246
global positioning system (GPS) navigation equipment 105
goal-based approach 21, 57–68
  advantages 60–5
  combining with risk-based approach 66–8
  ICAO 293–4
  limitations 65
  probability targets vs failure severity levels 57–60
  qualitative probability terms 60, 62
  quantitative probability values 60, 63
  safety objectives 60, 61, 64
  system safety assessment 120–1
goal structured notation (GSN) 112, 137, 246–8
  safety argument 112, 313–18
    notation used 314
    process 314–16
goals, operators, methods and systems (GOMS) 246
'good practice' 11
graceful degradation (fail-soft) 94–5, 327
gross carelessness, killing by 6
guidance/advisory material 20, 28
  safety instructions/guidance 197, 198, 201–2

hard systems approach (HSA) 115, 116
hardware redundancy 97
hardware/software safety analysis 248
hardware watchdog 77
harmonisation 40
hazard analysis (HA) 248, 328
hazard and operability studies (HAZOPs) 248–50
hazard identification study (HAZID) 250
hazard log (HL) 136, 137–9, 145, 250–2
hazard management process 49–50, 145
hazard risk index (HRI) 300, 302
hazard severity 57–60, 66–8, 74
hazard severity categories 60, 61, 66, 120, 294, 295
hazardous material 328
hazardous materials (HAZMAT) list 252
hazards 68, 69–93, 207, 328
  definitions 69
  equipment failures and faults 76–80
  identifying 49–50, 51, 74–6, 90, 117, 120, 122
  of a normal functioning system 80–5
  safety assessment tools and techniques 90–1, 213–91
  systemic failures 85–90, 334
  and their causes 69–74
health hazard analysis (HHA) 252
health hazard assessment 252
Health and Safety Commission (HSC) 2
health and safety director 8, 9
Health and Safety Executive (HSE) 2, 194
Health and Safety Policy (organisational) 8
health and safety regulations 38–40
Health and Safety at Work Act (1974) 2, 5, 7–8, 37, 39–40, 46–8, 129
Herald of Free Enterprise disaster (1987) 131, 132
highly integrated systems 328
historic data 252
  probability assessment 171–7
human error 94, 101–2, 135
  types of 327
human error analysis (HEA) 252
human error assessment and reduction technique (HEART) 252
human factors analysis 254
human hazard analysis (HHA) 254
human information processing 81–2
human reliability analysis 254, 269

IEC 1508 28
IEEE gold book 284
ignorance 17
Implementation Regulations (IRs) 29, 34, 35
Improvement Notices 2
inadvertent actions 328
incident planning 201
incident reviews 254
incidents 200–1, 328
inconvenience 17
independent events 155–6
independent failures 77–8
independent protective layers (IPLs) 260
inductive analysis 254

infant mortality ('burn-in') failures 151–2
informal guidelines 20
information redundancy 97
initiating events 329
inspection 329
installation appraisal 254, 329
instructions/guidance, safety 197, 198, 201–2
insurance 9
insurance risk 44
integral/primary redundancy 100
integrated performance modelling environment (IPME) 254
interface analysis 254–6
interference 94
International Civil Aviation Organisation (ICAO) 28, 29–30
  safety criteria 293–9
    application 294–9, 300
    background 293–4
International Safety Management (ISM) Code 131
Ishikawa diagrams 256
isolation 97
items 329

job safety analysis 256
Joint Aviation Authorities (JAA) 21, 29, 32–3
Joint Aviation Requirements (JARs) 29, 30, 32, 33, 39, 194
Joint Service Publications (JSP) 37–8
judgement 15, 207
justification of human error data information (JHEDI) 256

key issues tool (KIT) 256
King's Cross fire (1987) 131

laser safety analysis 258
latent 329
latent failures 77, 83, 164, 329
Law Commission 5–6
layer of protection analysis (LOPA) 258
legal charges 4
legal framework 1–16
  civil liability 2–4
  criminal liability 1–2
  implications for the engineer 13–15
  organisational responses 6–13
    civil law 8–9
    Consumer Protection Act 9–11
    contracts 11–13
    criminal law 7–8
    legal liability for dangerous or defective systems 6–7
  sentencing trends 4–6
lesson dissemination 201–2
level of effort 294, 296–7, 298
liability of tort 3
life cycle 329
life-cycle safety activities 200
life data analysis *see* Weibull analysis
likelihood 66–8, 329

maintainability 329
maintenance checks 184, 185, 186
maintenance deficiencies/errors 87, 94
maintenance error decision aid (MEDA) 258
major failure conditions 59, 61, 66, 67
malfunction 329
man-machine integration design and analysis systems (MIDAS) 260
management 9
  relationship with safety specialists 210
Management of Health and Safety at Work Regulations (1992) 39
management oversight and risk tree (MORT) 258
manslaughter 5
manufacturing errors/deficiencies 87, 94
marginal risks 46
margins of safety 99
marketing risk 44
Markov analysis (MA) 260
master minimum equipment list (MMEL) 183, 184
  equipment included 191–2
  see also minimum equipment lists
master plan logic diagram (MPLD) 260
material/process characteristics 109
materials compatibility analysis 260
maximum credible accident/worst case 260
MD83 Alaska Airlines accident (2000) 88
mean time between failures (MTBF) 154, 159, 172–5, 180–1, 206, 329
  failure rate, probability and 152–4
mean time to failure (MTTF) 329
mechanical failures, applying probabilities to 179–80
media 17
Merchant Shipping Act (1995) 39
methodology 329
Micro Saint 262
MIL-HDBK-217 handbook 178–9, 262
MIL-STD-810E 37

MIL-STD-882 36–7
MIL-STD-882C 51–2
MIL-STD-882D 36
  criteria 305–7
    mishap probability 306
    mishap risk assessment 307
    mishap severity 305–6
Milan Linate airport collision (2001) 8
military regulatory authorities 34–8
  UK Ministry of Defence 37–8
  US military 36–7
Military Standards (US) 21, 36–7
minimum equipment lists (MELs) 182–92, 206
  concept 182–4
  equipment included 191–2
  generic approach 184–5
  process 185–90
minimum standards 133, 134
Ministry of Defence (MoD) (UK) 37–8
  hazard log 137
  safety criteria 299–304
    accident criteria 299–302
    airworthiness criteria 299–300, 302–4
    background 299–300
minor failure conditions 59, 61, 66, 67
mishap 329
mishap probability 306
mishap risk 329
mishap risk assessment 307
mishap severity 305–6
mitigations 64, 65, 329
modelling 262
  safety assessment process 114–20
    aim of assessment 115–16
    choice of routes to objectives 119
    defining safety criteria 116–17
    describing the system 116
    evaluation 119
    generation of routes to objectives 118
    identifying safety objectives and constraints 117–18
    implementation 119–20
    modelling 118–19
    problem owner/decision maker 115
modified Cooper-Harper scale 262
modified pilot subjective evaluation (MPSE) 262
monitoring, safety 200, 332–3
Monte-Carlo analysis 264
mutually exclusive events 156–7
NASA Challenger accident (1986) 73–4, 195
NASA task load index 264
National Approval Authorities (NAAs) 33
national cultures 210
negligence 11, 12–13
negligible risks 46
network logic analysis 264
new technologies 207–8
non-obvious failures 77
normal functioning system 81–2
Notices of Proposed Amendments (NPA) 28–9
Notices of Proposed Rulemaking (NPRM) 28–9
NPRD-95 databook 180, 264
NSWC-94/L07 handbook 180, 264
numerical probabilistic approach *see* probability assessment
NUREG-0700 checklist 222

objective evidence 329
objective regulations 20–1, 27, 36
obvious failures 77
occupational health hazard analysis (OHHA) 266
operability analysis 266
operating and support hazard analysis (OSHA) 266
operational causes of accidents 57, 127
operational forces 109
operational safety 20
operational safety criteria 306, 307
operational scenario analysis 266
operator error *see* human error
optimum safety 329
organisational cultures 210
organisations
  impact of regulations/standards 40–1
  responses to legal framework 6–13

parallel architectures 84, 159
Pareto analysis 266
Pareto principle 329
partial active redundancy 97
particular risk assessment (PRA) 268
partitioning 330
parts *see* components
parts count technique 178–9, 262
parts stress technique 178, 262
passive failures *see* latent failures
past experience 252
path sets 330
performance, degraded 82–4, 94

performance analysis 83–4
performance specification 36, 40
personal risk 18
Petri net analysis 268
phase 330
physical safety 20
physics-of-failure 268
pilot error 81–2
pilot subjective evaluation (PSE) 268
planning 206
  safety management plans and procedures 8, 197, 198, 200–1, 206
  system safety assessment 110–12
Poisson distributions 175–6
policy statements, safety management 197, 198–9
practice 330
preliminary design review (PDR) 126
preliminary system safety assessment (PSSA) 111–12, 113
premise 330
prescriptive regulations 21, 25, 27, 134
preventive maintenance 152, 180
primary errors 327
primary/integral redundancy 100
PRISM 270
probability 184–5, 330
  accident 44, 45, 68, 122
  categories 66, 67, 293
  combining goal-based and risk-based approaches 66–8
  goal-based approach
    probability targets vs failure severity levels 57–60
    qualitative probability terms 60, 62
    quantitative probability terms 60, 63
probability assessment 148–81, 272
  applied quantitative assessment 155–9
  assessment process 160–2
    assembling numerical values needed 160–1
    considering acceptability of assessed probability 162
    defining circumstances for hazardous condition to be present 161
    defining precise failure sequences 161
    describing system behaviour 160
    stating undesired event 160
    summarising probability of hazardous event occurring 161
  bathtub curve 151–2
  determining failure rates of basic events 171–80
    applying probabilities to mechanical failures 179–80
    historic data 171–7
    probability estimation 171, 172
    reliability predictions 178–9
  ICAO 293
  probability vs reliability 154–5
  probability scale 149–50
  relationship between failure rate, probability and MTBF 152–4
  specific issues of concern 162–71
    applying failure probabilities to digital systems 169–71
    common mode failures 162–3
    failure sequences 163–4
    latent failures 164
    time of exposure 164–8
    where flight procedures are important 168–9
  symbols commonly used 149
  UK Ministry of Defence 302–3
probability density 177
probability scale 149–50
procedural event analysis tool (PEAT) 270
procedure analysis 270
procedures 52, 134
  safety management plans and procedures 8, 197, 198, 200–1, 206
process 330
process/material characteristics 109
product 109, 330
product liability 2–4, 8–9, 330
product life cycle 124, 125
product safety 330
product service history 330
product subsystems 109
product systems 109
production deficiencies/errors 87, 94
production system hazard analysis 270
professional cultures 210
professionalism 15
programme plan 112
Prohibition Notices 2
project risk 44
projects, collaborative 210–11
prosecutions 5–6
prototype development 270
proven reliability 97
Provision and Use of Work Equipment Regulations (PUWER) 49
qualification 330
qualification process 330
qualitative assessment 272, 331

qualitative safety objectives 294, 296
quality 179
  of architectural design 99–101
quantitative assessment 272, 331
  probability assessment *see* probability assessment
quantitative safety objectives 294, 296

random failures 80, 152, 331
rapid prototype modelling 266
Ravden & Johnson Checklist 222
RDF 2000 272–4
reasonably probable 59, 61, 62, 63, 67, 293
reckless killing 6
recommendations 146
reduction of risk 50–1, 55, 122
redundancy 24, 179, 331
  fail-safe 96–7
  MEL 184, 185, 192
  quality of architectural design 99–101
regulations/standards 20–1, 23–42, 83, 90, 134, 199
  airworthiness 24–6
  civil regulatory authorities 28–34, 35
  health and safety regulations 38–40
  impact on organisations 40–1
  military regulatory authorities 34–8
  regulatory failures 132–3
  and safety management system 41, 194, 199
  source of 26–8
reliability 331
  predictions 178–9, 181
  probability vs 154–5
reliability analysis 274
reliability block diagram 274
remote probability 59, 61, 62, 63, 67, 293
repertory grid analysis 274
requirements 331
requirements specification 27, 331
risk 331
  boundary risk 18–19
risk acceptance 50
risk analysis 145–6
risk assessment 40, 45–6, 49–50, 51, 56, 122
  matrices 66–8, 307, 309, 310
  mishap risk assessment 307
  processes 55
risk avoidance 50, 94
risk-based approach 21, 43–56
  advantages 53
  ALARP 46–9, 50, 54
  assessing risk 45–6
  combining with goal-based approach 66–8
  defining risk 44–5
  disadvantages 53–4
  managing the risk 49–52
  steps 52
  system safety assessment 122–3
risk-based decision analysis 274
risk classification 45, 46, 300, 302
risk control 49–50, 55–6
risk elimination 50, 52
risk management 15, 43, 49–52, 122, 145–6
  general principles 55
risk reduction 50–1, 55, 122
risk spreading 50
risk tolerability matrix 304–5
risk tracking 50
risk transfer 50
Road Traffic Act (1991) 39
root cause analysis 274
rules 20

safe life 97, 331
safety 17–22, 331
  definitions 17, 18–19
  ensuring 20–2
  factors influencing perception of safety risk 17–18
  importance of 18–19
  segments 19–20
safety argument 14, 111–12, 136, 137, 144–5
  GSN 112, 313–18
safety assessment 14, 70, 146, 184, 205–7, 212, 313, 331
safety assessment tools and techniques 90–3, 213–89
safety audits 201
safety case 14, 36, 129–47, 199–200, 205–7, 212, 322, 331–2
  core components 136–41
    hazard log 136, 137–9, 145, 250–1
    safety argument *see* safety argument
    safety management system *see* safety management system
  defining 133–4
  history 129–33
  rationale for 134–5
  relationship to SSA 135–6
  report 141–6
    aim, scope and objectives 142–3
    defining the system 142

recommendations and limitations 146
risk analysis 145–6
safety case strategy/argument 144–5
safety requirements and safety criteria 143–4
safety constraints 117–18
safety criteria 199, 292–312
air traffic management risk matrix 304–5
ICAO accepted 293–9
MIL-STD-882D criteria 305–7
other useful criteria 307–11
safety case report 143–4
safety critical system components 312
system safety assessment 110–11, 116–17
UK Ministry of Defence 299–304
safety critical 185, 332
safety critical computer software module 332
safety critical system components 312, 332
safety culture 195–6, 209–10
safety devices 52
safety engineering competence 209
Safety Health Environment and Fire Board (SHEFB) 37
safety improvement 201
safety incidents 332
safety instructions/guidance 197, 198, 201–2
safety integrity levels (SILs) 90, 170, 332
safety management 198, 205–7, 332
safety management plans and procedures 8, 197, 198, 200–1, 206
safety management policy statements 197, 198–9
safety management principles 197, 198, 199–200
safety management system (SMS) 8, 9, 136, 139–41, 193–203, 332
background 193–4
basic characteristics 195
developing 197–202
documentation pyramid 197–8
safety instructions/guidance 197, 198, 201–2
safety management plans and procedures 8, 197, 198, 200–1
safety management policy statements 197, 198–9
safety management principles 197, 198, 199–200
nature of 194–5
regulations/standards and 41, 194, 199
safety culture 195–6
safety monitoring 200, 332–3
safety objectives 60, 61, 64, 198
ICAO 294, 296
system safety assessment 117–18, 120–1
safety priority 199
safety records 200
safety requirements 143–4
safety responsibility 198
safety review 274–6
safety significant events 200–1
safety specialists: relationship with management 210
safety targets *see* safety objectives
Sale of Goods Act (1979) 11–12
Sale of Goods (Amendments) Act (1994) 11
scenario analysis 276
scenario-based requirements analysis (SCRAM) 276
secondary redundancy architecture 100
sentencing trends 4–6
sequentially timed events plot investigation system (STEP) 284–6
series architectures 84–5, 158–9
severity 184–5, 333
accident 44, 45, 46, 74
combining risk-based and goal-based approaches 66–8
hazard 57–60, 66–8, 74
severity categories 333
accident 46, 122, 300, 333
hazard 60, 61, 66, 120, 294, 295
Sevesco disaster (1976) 130
SHEL model 276
simulation *see* modelling
single function diagram (SFD) 276
single-point failure analysis 276
sneak analysis (sneak circuit analysis) 278
society 18
software
applying failure probabilities to 169–71
dissimilarity 80
failure 87
redundancy 97
software failure modes and effects analysis 278
software fault tree analysis 278
software hazard analysis 278
software hazard analysis and resolution in design (SHARD) 278
software sneak circuit analysis 278
software specification review (SSR) 124, 126
South African Air Force (SAAF) 108, 109

Special Federal Aviation Regulation (SFAR) 88 105
spreading risk 50
stakeholders 110, 115
standard ergonomics assessment methodology (SEAM) 278–80
standards *see* regulations/standards
standby redundancy 96–7
standby system 160–2, 186–90
Stark vs *Post Office* 49
static source code analysis 280
static strength 179
statistical distributions 83–4, 282
strict liability 4
structural safety analysis 282
structured what if technique (SWIFT) 282
subjective approach 21
subjective workload assessment technique (SWAT) 282
subsystems 107, 333
suddenness of consequence 18
suppliers, external 199
Supply of Goods and Services Act (1982) 11
Supply of Machinery (Safety) Regulations (1992) 39
Swissair MD–11 disaster, Nova Scotia (1998) 101–2
system design review (SDR) 124, 126
system levels 108, 109, 111, 135–6
system requirements review (SRR) 124, 126
system safety 25, 333
  and airworthiness 25–6
system safety analysis 333
system safety assessment (SSA) 36, 104–28, 199
  aims and objectives 105–7
    system safety aim 105–6
    system safety objectives 106
    system safety design requirements 106–7
  conducting a safety assessment 120–3
    goal-based safety assessment 120–1
    risk-based safety assessment 122–3
  generating system safety assessment report 123–7
  history 104–5
  modelling the safety assessment process 114–20
  planning the safety assessment 110–12
  relationship to safety case 135–6
  safety during development process 112–14
  system and its relationship to safety 107–10
system safety engineer 333
system safety engineering 334
system safety manager 334
system safety working group 333–4
system state 75–6
systematic inspection 282
systemic (systematic) failures 85–90, 334
systems 74–5, 333
  defining in safety case report 142
  description 111, 116
  hazards of a normal functioning system 80–5
    degraded functionality/performance 82–4
    normal functioning 81–2
    unwanted operation 84–5
  relationship to safety 107–10
  safety engineering competence 209
systems approach 334

task analysis 268–9, 282
technical airworthiness 334
technical causes of accidents 57, 127
technique for human error rate prediction (THERP) 284
technique for the retrospective analysis of cognitive error (TRACEr) 284
technology 212
  new technologies 207–8
technology-based approach 21
Telcordia approach 216–17
test safety analysis 284
tests 284
tetrachlorodibenzo-p-dioxin (TCDD) 130
through-life approach 133, 207
time of exposure 164–8
time/loss analysis for emergency response evaluation 286
time redundancy 97
top-down analysis approach 119, 286
tort 2, 3
training 15, 52
transfer of risk 50
trend(ing) analysis 286
TWA800 accident, New York (1996) 86, 105
type certificate 334

unacceptable harm 19
unanunciated failures 334
uncertainty analysis 286

uncommanded 334
undetected failures 334
Unfair Contract Terms Act (1977) 12
Unfair Terms in Consumer Contracts
Regulations (1995) 12
unit/assembly 107
United Kingdom
CAA 34
Defence Standards 21, 38
Ministry of Defence *see* Ministry of
Defence
United States
FAA *see* Federal Aviation Administration
FARs 29, 30, 32, 39
military regulatory authorities 36–7
Military Standards 21, 36–7
unrevealed failures *see* latent failures
unwanted operation 84–5
useful life 151, 152
user analysis 286–8
user systems 109

Viscount 732 accident (1958) 87

waiver 334
walk-through analysis 288
warning devices 52
warning system 160–2, 186–90
wear-out failures 80, 151–2
Weibull analysis 180, 288–90
what-if analysis 290
working systems 134–5
workload analysis 266

zonal hazard analysis (ZHA) 290
zonal safety analysis (ZSA) 290