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

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

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).

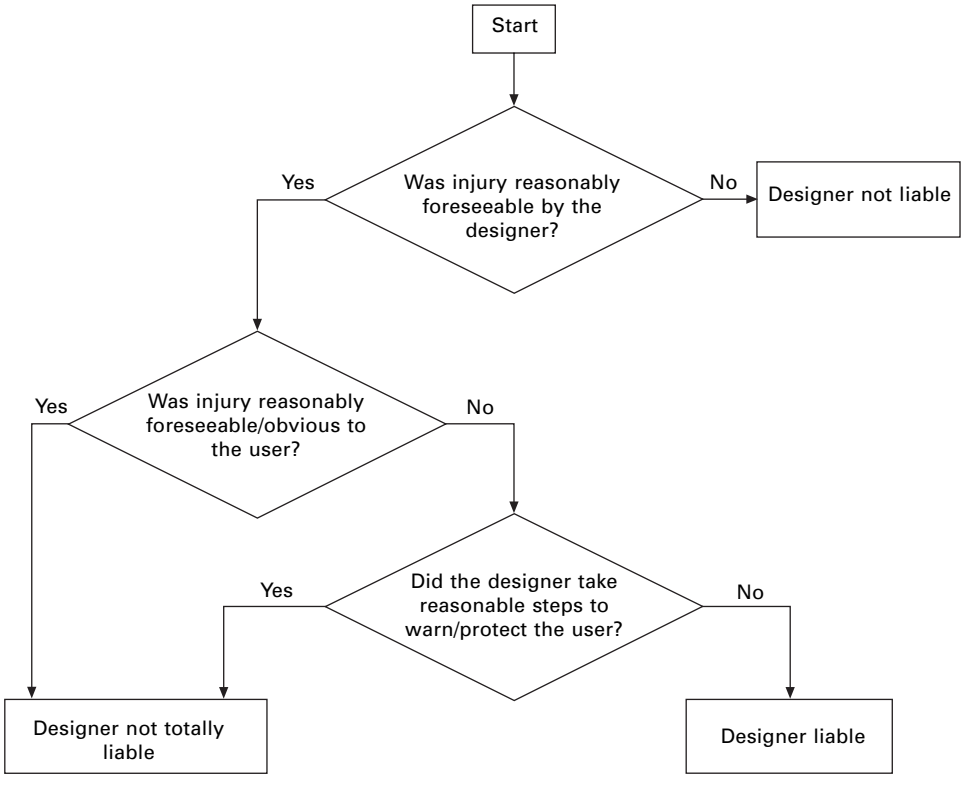
Civil liability for a defective system can arise under the laws of contract, misrepresentation, tort, other common law doctrines and under current UK legislation. Liability can fall on the manufacturer, supplier, distributor or certifier of products (Falla, 1997). In practice, such a supplier or manufacturer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



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.