

# Contents

<i>List of Figures</i>	<i>ix</i>
<i>List of Tables</i>	<i>x</i>
<i>Preface</i>	<i>xi</i>
<i>Acknowledgements</i>	<i>xiii</i>
1. Accidents and Safety	1
Introduction	1
The Safety Case	3
The Safety Case Report	5
Health and Safety Plan	5
System Safety Approach Documentation	7
Control of Major Accident Hazards (COMAH)	9
Summary	11
2. The Language of Safety	12
The Concepts of Language	12
The Language of Risk, Chance, Probability and Hazard	13
The Origins of Chance, Risk and Probability	14
The Origins of Hazard	15
The Origins of Safety and Safety Case	16
Modern use of Safety Language	17
Development of the Safety Case in the UK	17
Development of Safety Reports in the US	19
Summary	20
3. The Safety Management System	22
The Components of a Safety Management System	22
Designing a Safety Management System	23
Safety Management Planning	25
Example of a UK Safety Plan	25
Example of a US Safety Plan	26
Safety Planning Meetings	27
4. The Purpose of a Safety Case	30
Why Are You Constructing a Safety Case?	30
The Safety Case as a Record of Residual Risk	30
Safety Cases as a Management Tool During Change	31
Safety Cases as a Record of Engineering Practice	31

Safety Cases as a Tool in a Court of Law	32
Safety Cases as a Marketing Tool	32
Safety Cases as a Route to Fewer Accidents	33
Understand your Particular Purpose(s)	33
5. The Requirement for a Safety Case	34
Why Do You Need a Safety Case Anyway?	34
Legislation for Safety Cases	34
Evidence for the Need to Have a Safety Case	37
Goal-based and Prescriptive Requirements	38
6. Setting a Safety Boundary	41
What is a Safety Boundary?	41
Deriving the Safety Boundary	42
Boundary Diagrams	43
When a Diagram Might Not Work	44
Other Boundary Considerations	44
7. Measuring Safety Performance	47
Judging Safety Performance	47
Measurement Scales	48
Safety Measurement Scales	49
Event Severity Scales	49
Event Frequency Scales	52
The Risk Matrix for Communicating About Safety	55
Populating a Risk Matrix	56
Special Note	60
The Layout of a Risk Matrix	60
The Final Check	60
Summary	61
8. Safety Targets	62
The Role of Safety Targets	62
Setting a Safety Target	62
Quantitative Targets	63
Target Apportionment	63
Quantitative Targets in Use	64
Qualitative Targets	65
9. So Far as is Reasonably Practicable	67
So Far as is Reasonably Practicable	67
The ALARP Concept	68
Demonstrating ALARP	69
The Accident Tetrahedron	70
Problems with ALARP as a Safety Target	71
Real Use of the ALARP Process in Industry	72
The GALE Principle	73

10. Individual, Group and Population Risk	76
Sharing Risk	76
Individual Risk	76
Group Risk	77
Population Risk	80
Use of FN Curves	82
Worker vs. Public Risk	82
Multiple Safety Targets in a Safety Case	83
11. The Safety Team	85
Why Have a Team at All?	85
What the Team has to Do	86
Who is in the Team?	87
The Project Safety Committee	88
Forming a Safety Committee	89
Who Owns the Safety Case?	90
12. Costs in Safety	92
The Measurements of Costs	92
The Cost of Having Accidents	92
The Value of a Prevented Fatality	95
Cost Indicators from Criminal Fines	98
Cost Indicators from Other Fines	98
13. Techniques and Tools for Safety Cases	100
Introduction	100
HAZOP	100
Structured What-if Technique (SWIFT)	101
Fault-tree Analysis	103
Event tree Analysis	105
Zonal Analysis	107
Failure Mode Effect Analysis (FMEA)	108
Human Hazard Analysis	109
Human Reliability Analysis	110
Stored Energy Analysis	111
Summary	112
14. The Hazard Log	113
The Role of the Hazard Log	113
The Requirement for a Hazard Log	113
The Content of a Hazard Log	115
Examples of Real Hazard Logs	115
15. Human Factors in Safety Cases	120
Introduction to Human Factors	120
The Human Caused the Accident	120
The Human Prevented the Accident	123

Human Systems Integration	125
Safety Documents from the Human Factors Domain	126
Human Factors Analysis	127
Summary	130
16. Software Factors in Safety Cases	131
Introduction to Software Factors	131
The Software Caused the Accident	131
Commercial-off-the-shelf (COTS) Systems	133
Software of Uncertain Pedigree (SOUP)	134
How to Treat the Risks of Software	135
Software Testing Methods	139
Safety Documents from the Software Domain	141
17. Management Factors in Safety Cases	144
Introduction to Management Factors	144
The Managers Caused the Accident	145
Managers and the Law	146
Promoting a Safety Culture	147
Evidence from Managers for the Safety Case	149
18. Independent Safety Review	152
The Principles of a Review	152
How Independent is ‘Independent’?	152
A Review by the Regulators	153
Assessor, Advisor or Auditor	153
Competency of the Reviewer	155
The Terms of Reference	156
19. Presentation of the Safety Case	158
Introduction to Presenting Safety Cases	158
The Paper-based Safety Case	158
Recommended Layouts for a Paper-based Safety Case	159
The IT-based Safety Case	162
Recommended Layouts for an IT-based Safety Case	163
Goal Structuring Notation Tool Support	165
20. Maintenance of the Safety Case	168
What Happens to Safety Cases?	168
Managing Change	170
Review and Update Cycles	171
<i>Epilogue</i>	172
<i>Index</i>	173