

# Contents

|   |      |
|---|------|
| List of Figures   | ix   |
| List of Tables  | xiii |
| List of Abbreviations   | xv   |
| Preface   | xvii |
| <br>  |      |
| 1 Hazards, Defences and Losses                                | 1    |
| Individual and organizational accidents                       | 1    |
| Finding the right level of explanation                        | 1    |
| Production and protection: two universals                     | 3    |
| The nature and variety of defences                            | 7    |
| The 'Swiss cheese' model of defences                          | 9    |
| Active failures and latent conditions                         | 10   |
| The accident trajectory                                       | 11   |
| From the Deadwood stage to jumbo jet                          | 13   |
| Stages in the development of an organizational accident       | 15   |
| Pulling the threads together                                  | 18   |
| <br>  |      |
| 2 Defeating the Defences                                      | 21   |
| Things are not always what they seem                          | 21   |
| Slipping through the cracks in an aircraft maintenance system | 22   |
| The millions that gushed away: the Barings collapse           | 28   |
| The Nakina derailment: a 76-year-old latent failure           | 34   |
| Common features   | 36   |
| <br>  |      |
| 3 Dangerous Defences  | 41   |
| Killed by their armour  | 41   |
| Some paradoxes  | 42   |
| Automation: ironies, traps and surprises                      | 42   |
| Quality control versus quality assurance                      | 46   |
| Writing another procedure                                     | 49   |

|  |            |
|--|------------|
| Causing the next accident by trying to prevent the last one      | 52         |
| Defences-in-depth: protection or dangerous concealment?          | 54         |
| False alarms   | 56         |
| Deliberate weak links  | 57         |
| Summary  | 58         |
| <b>4 The Human Contribution</b>                                  | <b>61</b>  |
| The human factor   | 61         |
| The varieties of administrative controls                         | 62         |
| The stage reached in the organization's life history             | 64         |
| Type of activity   | 65         |
| Level within the organization                                    | 67         |
| The trade-off between training and procedures                    | 67         |
| Three levels of performance                                      | 68         |
| Errors and successful actions                                    | 71         |
| Violations and compliant action                                  | 72         |
| Correct and incorrect actions                                    | 73         |
| The quality of the available procedures                          | 74         |
| Six kinds of rule-related behaviour                              | 75         |
| Some real-life examples  | 76         |
| Assembling the big picture                                       | 79         |
| <b>5 Maintenance can Seriously Damage your System</b>            | <b>85</b>  |
| Close encounters of a risky kind                                 | 85         |
| Organizational accidents and maintenance failures                | 86         |
| Activities and their relative likelihood of performance problems | 91         |
| The vulnerability of installation                                | 93         |
| The prevalence of omissions                                      | 94         |
| Omission-prone task features                                     | 95         |
| The characteristics of a good reminder                           | 98         |
| The rationale for maintenance                                    | 100        |
| Conclusions  | 103        |
| <b>6 Navigating the Safety Space</b>                             | <b>107</b> |
| Assessing safety   | 107        |
| Counting horse kicks   | 108        |
| Introducing the safety space                                     | 110        |
| Currents within the safety space                                 | 111        |
| What fuels the 'safety engine'?                                  | 113        |
| Setting the right safety goals                                   | 114        |
| A test to destruction  | 115        |

|  |            |
|--|------------|
| An overview of the navigational aids                             | 116        |
| Near-miss and incident reporting schemes                         | 118        |
| Proactive process measurement: the priorities                    | 120        |
| Are accidents really necessary?                                  | 123        |
| <b>7 A Practical Guide to Error Management</b>                   | <b>125</b> |
| What is error management?  | 125        |
| Ancient but often misguided practices                            | 125        |
| Errors are consequences not causes                               | 126        |
| The blame cycle  | 127        |
| People or situations?  | 128        |
| An overview of the error management tool box                     | 129        |
| Tripod-Delta   | 132        |
| Review and MESH  | 138        |
| Human Error Assessment and Reduction Technique (HEART)           | 142        |
| The Influence Diagram Approach (IDA)                             | 146        |
| Maintenance Error Decision Aid (MEDA)                            | 151        |
| Tripod-Beta  | 152        |
| Summary of the main principles of error management               | 153        |
| <b>8 The Regulator's Unhappy Lot</b>                             | <b>157</b> |
| Regulators in the frame  | 157        |
| Regulated accidents  | 157        |
| US regulators under fire   | 168        |
| Damned if they do and damned if they don't                       | 171        |
| Legislation and regulation: some major successes                 | 172        |
| Autonomy and dependence as constraints on the regulatory process | 173        |
| The move towards self-regulation                                 | 175        |
| The pluses and minuses of the move to self-regulation            | 181        |
| A possible model for the regulatory process                      | 182        |
| The regulator deserves a better deal                             | 187        |
| <b>9 Engineering a Safety Culture</b>                            | <b>191</b> |
| The scope of the chapter   | 191        |
| What is an organizational culture?                               | 192        |
| The components of a safety culture                               | 195        |
| Engineering a reporting culture                                  | 196        |
| Engineering a just culture                                       | 205        |
| Engineering a flexible culture                                   | 213        |
| Engineering a learning culture                                   | 218        |

|    |  |     |
|----|--|-----|
|    | Safety culture: far more than the sum of its parts                         | 219 |
|    | Postscript: national culture   | 220 |
| 10 | Reconciling the Different Approaches to Safety Management                  | 223 |
|    | Revisiting the distinction between individual and organizational accidents | 223 |
|    | Three approaches to safety management                                      | 224 |
|    | Primary risk areas   | 226 |
|    | The preponderance of risks in different domains                            | 228 |
|    | Can personal injuries predict organizational accidents?                    | 232 |
|    | Latent conditions: the universal risk                                      | 233 |
|    | Has the pendulum swung too far?  | 234 |
|    | Some problems with latent conditions                                       | 236 |
|    | The price of failure   | 237 |
|    | The last word  | 239 |
|    | Index  | 243 |