The risk management of safety and dependability
A guide for directors, managers and engineers

W. Wong
## Contents

- About the author  xi
- Acknowledgements  xii
- Preface  xiii

1  Ever-present danger: an introduction to the principles of risk management  1
   1.1 Introduction  1
   1.2 The principles of risk assessment  2
   1.3 The risk assessment matrix  3
   1.4 Risk evaluation and control  4
   1.5 Dependability  5
   1.6 The risk management process  5
   1.7 Examples of risk management failures  5
   1.8 General precepts  16
   1.9 Summary  18
   1.10 References  18

2  Ignorance is no defence: legislation and the corporate role in managing risk  19
   2.1 Introduction: management failures  19
   2.2 An overview of the law in the UK  21
   2.3 The Health and Safety at Work etc. Act 1974  24
   2.4 The Management of Health and Safety at Work Regulations 1999 (MHSWR)  25
   2.5 The Provision and Use of Work Equipment Regulations 1998 (PUWER)  26
   2.6 The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)  26
   2.7 The Control of Substances Hazardous to Health Regulations 1994 (COSHH)  27
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.8</td>
<td>The Supply of Machinery Safety Regulations 2008 (Machinery Directive 2006/42/EC)</td>
<td>27</td>
</tr>
<tr>
<td>2.9</td>
<td>The Electromagnetic Compatibility (Amendment) Regulations 2006</td>
<td>30</td>
</tr>
<tr>
<td>2.10</td>
<td>The Control of Major Accident Hazards Regulations 1999 (COMAH) Amended 2005</td>
<td>31</td>
</tr>
<tr>
<td>2.11</td>
<td>The Construction (Design and Management) (CDM) Regulations 2007</td>
<td>32</td>
</tr>
<tr>
<td>2.12</td>
<td>The Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR)</td>
<td>35</td>
</tr>
<tr>
<td>2.14</td>
<td>The Pressure Equipment Directive 1999 (PED)</td>
<td>42</td>
</tr>
<tr>
<td>2.15</td>
<td>The Pressure Systems Safety Regulations 2000</td>
<td>43</td>
</tr>
<tr>
<td>2.16</td>
<td>The Lifting Operations and Lifting Equipment Regulations 1998 (LOLER)</td>
<td>43</td>
</tr>
<tr>
<td>2.17</td>
<td>Other regulations and standards</td>
<td>44</td>
</tr>
<tr>
<td>2.18</td>
<td>International health and safety</td>
<td>44</td>
</tr>
<tr>
<td>2.19</td>
<td>Summary</td>
<td>45</td>
</tr>
<tr>
<td>2.20</td>
<td>References</td>
<td>45</td>
</tr>
<tr>
<td>3</td>
<td>How to recognise hazards: learning about generic industrial hazards</td>
<td>47</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>47</td>
</tr>
<tr>
<td>3.2</td>
<td>Human vulnerability</td>
<td>48</td>
</tr>
<tr>
<td>3.3</td>
<td>Hazards from waste emissions</td>
<td>48</td>
</tr>
<tr>
<td>3.4</td>
<td>Hazards from heat emissions and hot surfaces</td>
<td>56</td>
</tr>
<tr>
<td>3.5</td>
<td>Hazards from noise emissions</td>
<td>56</td>
</tr>
<tr>
<td>3.6</td>
<td>Hazards from radiation</td>
<td>62</td>
</tr>
<tr>
<td>3.7</td>
<td>Hazards from latent energy</td>
<td>63</td>
</tr>
<tr>
<td>3.8</td>
<td>Hazards from other sources</td>
<td>64</td>
</tr>
<tr>
<td>3.9</td>
<td>Hazards from design error</td>
<td>69</td>
</tr>
<tr>
<td>3.10</td>
<td>Complacency</td>
<td>70</td>
</tr>
<tr>
<td>3.11</td>
<td>Summary</td>
<td>71</td>
</tr>
<tr>
<td>3.12</td>
<td>References</td>
<td>71</td>
</tr>
<tr>
<td>4</td>
<td>Human factors in risk management: understanding why humans fail and are unreliable</td>
<td>72</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>72</td>
</tr>
<tr>
<td>4.2</td>
<td>Ergonomics</td>
<td>74</td>
</tr>
<tr>
<td>4.3</td>
<td>Anthropometrics</td>
<td>85</td>
</tr>
<tr>
<td>4.4</td>
<td>Physiology</td>
<td>85</td>
</tr>
</tbody>
</table>
4.5 Psychology 87
4.6 Case histories 89
4.7 Summary 96
4.8 References 96

5 Exposing hazards: techniques to find possible risks of unacceptable failures in procedures, machines and systems 98
5.1 Introduction 98
5.2 ‘What if’ procedure 98
5.3 Block flow diagrams 101
5.4 Failure mode and effects analysis (FMEA) 105
5.5 Hazard and operability studies (HAZOP) 110
5.6 A cautionary example 117
5.7 Summary 117
5.8 References 118

6 Safe enough? Methods and procedures for evaluating and reducing risk in the design of processes, plant and machinery 119
6.1 Introduction 119
6.2 Bow Tie analysis 122
6.3 Human error 124
6.4 Redundancy 128
6.5 Series systems 131
6.6 Reliability 132
6.7 Component failure 132
6.8 Fault tree analysis (FTA) 136
6.9 Pressure control system 136
6.10 Safety integrity level (SIL) 143
6.11 Summary 143
6.12 References 144

7 Inherently unsafe: safety issues in planning a new facility 145
7.1 Introduction 145
7.2 Site location 145
7.3 Scope considerations 147
7.4 Design for safety 149
7.5 Hazardous area classification 149
7.6 Fire prevention 150
7.7 Design to ensure safety 157
7.8 Design for reliability 160
8 Product risk: managing risk in the design and development process

8.1 Introduction
8.2 Product risk assessment
8.3 Reliability testing
8.4 Life characteristics
8.5 Reliability target
8.6 Statistical data
8.7 Data enhancement
8.8 Test data processing
8.9 Test data analysis
8.10 Warranty analysis
8.11 Summary
8.12 References

9 Asset integrity: learning about the cause and symptoms of age and decay and the need for maintenance to avoid catastrophic failures

9.1 Introduction
9.2 Maintenance strategies
9.3 Failure due to service deterioration
9.4 Failures due to corrosion
9.5 Pressure systems failures
9.6 Risk-based inspection (RBI)
9.7 Maintenance resources
9.8 Summary
9.9 References

10 Coping with risk: how to ensure the health and safety of people at work

10.1 Introduction
10.2 The cost of safety and reliability
10.3 The occupational safety and health management system
10.4 Education and training
10.5 Supervision
10.6 Control
10.7 Monitoring performance
10.8 Emergency planning and management
10.9 Plant modification: change procedures
10.10 Auditing safety 248
10.11 Security 251
10.12 Summary 251
10.13 References 252

11 Management disasters: the lessons to be learnt from three major disasters 253
11.1 Introduction 253
11.2 Bhopal 254
11.3 Piper Alpha 258
11.4 Nimrod 268
11.5 Summary 272
11.6 References 273

Appendix 1: List of abbreviations and acronyms 275

Appendix 2: Bibliography 279

Appendix 3: Directory of bodies associated with risk management and safety 281

Index 287