

D Acknowledgements

Most of the text of this book has been derived from project reports or from material specially supplied by project members. The following list identifies the main source of each section.

In many cases the full report is available - for details see the indicated reference on the project page in Appendix A.

2 Are your systems critical?

- | | | |
|-----|---------------------------------------|--|
| 2.1 | Legal liability for defective systems | Based on [FRESCO <i>ref</i> 6/1] updated by Eversheds, December 1996 |
| 2.2 | Emerging software safety standards | Para 6 onwards based on [SADLI <i>ref</i> 9] |
| 2.3 | IEC 1508 | Based on text supplied by Mr R Bell, HSE ¹ |

3 Hazard Analysis

- | | | |
|-----|---|---|
| 3.1 | Software hazard analysis | Based on [CONTESSE <i>ref</i> B10] |
| 3.2 | Integrating software hazard analysis with the development process | Based on [MORSE <i>refs</i> D27, D36 and D35] |
| 3.3 | HAZOP throughout the lifecycle | Based on [SADLI <i>ref</i> 9] |
| 3.3 | A case study of Fault Tree Analysis | Based on [SADLI <i>ref</i> 10] |
| 3.4 | Mobile robots | Based on text supplied by the project |
| 3.5 | A method for hazard assessment in programmable systems | Based on text supplied by the project |

4 Making the Case that it's Safe

- | | | |
|-----|----------------------------|---|
| 4.1 | A method for safety cases | Closely based on text supplied by the project |
| 4.2 | A designer's assistant | Based on text supplied by the project |
| 4.3 | Combining diverse evidence | Based on text supplied by the project |

5 Assessment

- | | | |
|-----|----------------------------|----------------------------------|
| 5.1 | A Framework for Assessment | Based on [FRESCO <i>ref</i> 9/3] |
| 5.2 | Guidelines for assessment | Based on [MORSE <i>ref</i> D39] |

6 Managing Risk and Safety

- | | | |
|-----|----------------------------|---|
| 6.1 | Managing risk | Based on text supplied by the project |
| 6.2 | Safety policies and models | Based on SPAM report D6 (not published) |

7 The Interface with the Operator

- | | | |
|-----|--------------------------------------|---------------------------------------|
| 7.1 | Supporting team operation | Based on [LIFETRACK <i>ref</i> 6] |
| 7.2 | Analysing human error | Based on text supplied by the project |
| 7.3 | Hazard analysis of human interaction | Based on [SADLI <i>ref</i> 11] |

¹ Extracts from the draft standard IEC 1508 : Part 1 are reproduced with permission. Complete editions of the draft standard can be obtained by post from BSI Customer Services, 389 Chiswick High Road, London W4 4AL, or through national standards bodies.

8 Guidelines for Best Practice

- | | | |
|-----|---|---------------------------------------|
| 8.1 | Automotive industry | Based on [MISRA refs 1, 2 and 10] |
| 8.2 | Management guidelines for developing safety-critical software | Refers to [MORSE ref D39] |
| 8.3 | A methodology for safe advanced robots | Based on [ROBUST ref 1] |
| 8.4 | A code of practice for the human dimension | Based on text supplied by the project |
| 8.5 | Guidelines for programmable logic controllers | Text supplied by the project |

9 Getting the Process Right

- | | | |
|-----|---|---|
| 9.1 | The safety-critical systems engineering process | Based on project Final Report (not published) |
| 9.2 | The problem of changing requirements | Based on [PROTEUS ref 1] |
| 9.3 | The legal lifecycle | Based on unpublished report MS/WP/620/2 |
| 9.4 | Modelling the process using AI techniques | Based on text supplied by the project |
| 9.5 | Communication in engineering design | Based on text supplied by the project |

10 Tools and Languages for Critical Systems

- | | | |
|------|--|---------------------------------------|
| 10.1 | Tools for railway signalling | Based on text supplied by the project |
| 10.2 | Reverse engineering safety-critical systems | Based on text supplied by the project |
| 10.3 | Design patterns and frameworks | Based on text supplied by the project |
| 10.4 | Assessing the impact of object technology in the safety-critical domain. | Based on text supplied by the project |

11 The Human Element in the Development Process

- | | | |
|------|--|---|
| 11.1 | Predicting fault rates during software development | Based on [FASGEP refs 6 and 9] |
| 11.2 | Avoiding human error in design | Based on text supplied by the project |
| 11.3 | A systems approach to human error | Closely based on text supplied by the project |
| 11.4 | Designers' practices | Refers to [DATUM refs 19, 20 and 22] |

12 Testing

- | | | |
|------|---|---------------------------------------|
| 12.1 | Environment simulation | Based on [CONTESSE ref B10] |
| 12.2 | The contribution of testing to safety cases | ditto |
| 12.3 | Case studies | ditto |
| 12.4 | How much testing do I need to do? | Refers to [DATUM ref 21] |
| 12.5 | Measuring the testability of a system | Based on text supplied by the project |

13 Formal Methods

- | | | |
|------|---|--|
| 13.1 | Formal Methods for cost-effective procurement of high integrity systems | Based on [SAFE-FM <i>ref</i> D22] |
| 13.2 | Case studies with RAISE in avionics, plant control and laboratory information | Based on [MORSE <i>refs</i> D34, D35, D36] |
| 13.3 | Reverse engineering by formal transformations | Based on text supplied by the project |
| 14.4 | Using natural language processing tools | Based on [MORSE <i>ref</i> D40] |

14 New Approaches to Critical Systems

- | | | |
|------|---|--|
| 14.1 | Knowledge-based systems and safety-critical decisions | Based on [RED <i>ref</i> 12] |
| 14.2 | Functional programming languages for complex systems | Based on report [SADLI <i>ref</i> 9] |
| 14.3 | Neural computing | Based on text supplied by the project |
| 14.4 | Using natural language processing tools | Based on report [MORSE <i>ref</i> D40] |

15 System Architectures

- | | | |
|------|--|--|
| 15.1 | Supporting re-use | Based on reports [MORSE <i>refs</i> D23, D25, D32 and D37] |
| 15.2 | An architecture for mobile robots | Based on text supplied by the project |
| 15.3 | The multiversion approach to ultra-reliability | Based on text supplied by the project |

16 Safety-Related Engineering Design

- | | | |
|------|--------------------------|--|
| 16.1 | Safe structural analysis | Closely based on sections 1 and 2 of [SAFESA <i>ref</i> 3] |
| 16.2 | Safe design of networks | Based on text supplied by the project.. |

In addition, Bob Malcolm made many helpful contributions to the introductions to chapters.