# Contents

Introduction . . . . . . . . . . xi

Chapter 1. System, Equipment and Software . . . . . . . . . . 1

1.1. Introduction . . . . . . . . . . 1
1.2. Impact on dependability . . . . . . . . . . 1
1.3. Command and control system . . . . . . . . . . 3
1.4. System . . . . . . . . . . 6
1.5. Development process . . . . . . . . . . 10
1.6. Safety: from system to software . . . . . . . . . . 13
1.7. Software application . . . . . . . . . . 16
1.7.1. What is software? . . . . . . . . . . 16
1.7.2. Generic, specific or dedicated . . . . . . . . . . 16
1.7.3. Various types of software . . . . . . . . . . 16
1.7.4. Various types of uses . . . . . . . . . . 17
1.8. Conclusion . . . . . . . . . . 17
1.9. Glossary . . . . . . . . . . 18

Chapter 2. Software Application . . . . . . . . . . 21

2.1. Introduction . . . . . . . . . . 21
2.2. Software versus software applications . . . . . . . . . . 21
2.3. Software application in its context . . . . . . . . . . 24
2.3.1. General framework . . . . . . . . . . 24
2.3.2. Reusability, maintainability and continuous service . . . . . . . . . . 25
2.3.3. Modular architecture . . . . . . . . . . 27
2.4. Generic software and parameterized software . . . . . . . . . . 29

2.5. Module and component . . . . . . . . . . 32
2.6. Reused component and COTS . . . . . . . . . . 37
2.7. Product line. . . . . . . . . . 38
2.8. Conclusion . . . . . . . . . . 40
2.9. Glossary . . . . . . . . . . 41

**Chapter 3. Principle of Dependability** . . . . . . . . . . 43

3.1. Introduction . . . . . . . . . . 43
3.2. Dependability . . . . . . . . . . 44
3.2.1. Basic concepts. . . . . . . . . . 44
3.2.2. Dependability constraints . . . . . . . . . . 45
3.2.3. Methods . . . . . . . . . . 49
3.2.4. Example of a constraint . . . . . . . . . . 50
3.2.5. Classification of faults . . . . . . . . . . 53
3.2.6. Adaptation to software applications . . . . . . . . . . 54
3.3. Description of software errors . . . . . . . . . . 57
3.4. Safety critical software . . . . . . . . . . 60
3.4.1. Prevention of faults . . . . . . . . . . 60
3.4.2. Elimination of faults . . . . . . . . . . 61
3.4.3. Tolerance to faults . . . . . . . . . . 61
3.4.4. Prediction of faults . . . . . . . . . . 62
3.4.5. Review . . . . . . . . . . 63
3.5. Conclusion . . . . . . . . . . 63
3.6. Glossary . . . . . . . . . . 64

**Chapter 4. Safety Management of a Software Application** . . . . . . . . . . 65

4.1. Introduction . . . . . . . . . . 65
4.2. General approach . . . . . . . . . . 66
4.3. Danger, undesirable events, accidents, risks. . . . . . . . . . 67
4.3.1. Definitions. . . . . . . . . . 67
4.4. System safety. . . . . . . . . . 72
4.4.1. Definition . . . . . . . . . . 72
4.4.2. Safety management . . . . . . . . . . 75
4.4.3. Safety integrity . . . . . . . . . . 82
4.4.4. SIL management . . . . . . . . . . 84
4.4.5. Safety integrity level . . . . . . . . . . 86
4.4.6. Overall safety cycle. . . . . . . . . . 89
4.5. Safety Assurance Plan. . . . . . . . . . 94
4.6. Safety case . . . . . . . . . . 94
4.6.1. Structure of the safety case. . . . . . . . . . 94

4.6.2. Exported constraints . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 95
4.6.3. Product. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 96
4.7. Reliability, availability and maintainability . . . . . . . . . . . . . . . . . . . . 97
4.7.1. Requirement . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 97
4.7.2. Problems specific to using off-the-shelf components . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 98
4.7.3. FDM plan . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99
4.8. Critical systems . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99
4.9. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 99
4.10. Appendix 1 – Safety Assurance Plan (SAP) . . . . . . . . . . . . . . . . . . 99
4.11. Glossary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 100

**Chapter 5. Safety of a Software Application** . . . . . . . . . . . . . . . . . . . 103

5.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 103
5.2. General approach . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 105
5.2.1. Software reliability . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 105
5.2.2. Availability . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 107
5.2.3. Maintenance . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 107
5.2.4. Safety . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 108
5.2.5. Impact of the software . . . . . . . . . . . . . . . . . . . . . . . . . . . 110
5.3. Safety level . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 110
5.4. Safety demonstration activity of a software application . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 111
5.4.1. Safety analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 111
5.4.2. Code analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 117
5.4.3. Compliance with safety requirements . . . . . . . . . . . . . . . . . . . . 119
5.4.4. Fault analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 119
5.5. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120
5.6. SSAP template . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 121
5.7. Glossary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 122

**Chapter 6. Technique to Manage Software Safety** . . . . . . . . . . . . . . . 125

6.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 125
6.2. Techniques for software safety . . . . . . . . . . . . . . . . . . . . . . . . . 126
6.2.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 126
6.2.2. Error management . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 126
6.2.3. Error recovery . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 129
6.2.4. Defensive programming . . . . . . . . . . . . . . . . . . . . . . . . . . . 135
6.2.5. Double execution of a software application . . . . . . . . . . . . . . . . 142
6.2.6. Data redundancy . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 150
6.3. Other diversities . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 153
6.3.1. Temporal diversity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 154

6.3.2. Memory allocation diversity . . . . . . . . . . . . . . . . . . . . . . . . . 154
6.4. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 154
6.5. Glossary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 155

Chapter 7. Assessment and Certification. . . . . . . . . . . . . . . . . . . . . . 157

7.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 157
7.2. Product . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 158
7.3. Assessment. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 158
7.4. Certification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 161
7.4.1. Product certification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 161
7.4.2. Assessment and software certification . . . . . . . . . . . . . . . . . . . . 163
7.4.3. Cross-acceptance . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 165
7.4.4. Change management . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 166
7.4.5. Tests . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 167
7.5. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 169
7.6. Glossary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 169

Chapter 8. Different Sectors and Various Normative Referentials . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171

8.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171
8.2. E/E/PE system . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171
8.2.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 171
8.2.2. Certification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 173
8.2.3. Safety levels . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 173
8.2.4. Sub-standards . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 174
8.2.5. Software safety . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 175
8.3. Railway sector . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 175
8.3.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 176
8.3.2. Certification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 179
8.3.3. Safety versus availability. . . . . . . . . . . . . . . . . . . . . . . . . . . . 179
8.3.4. Software safety . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 180
8.3.5. IRIS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 183
8.4. Aeronautics. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 184
8.4.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 184
8.4.2. Software safety level . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 186
8.4.3. Certification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 186
8.5. Space sector . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 186
8.6. Nuclear sector . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 187
8.7. Automobile sector . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 188
8.7.1. ISO 26262 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 188
8.7.2. Safety demonstration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 189
8.7.3. Software safety . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 190

8.7.4. Certification . . . . . 190
8.8. A few constraints . . . . . 190
8.9. Safety level . . . . . 190
8.10. Conclusion . . . . . 191
8.11. Glossary . . . . . 191

Chapter 9. Quality Management . . . . . 195

9.1. Introduction . . . . . 195
9.2. Continuous improvement . . . . . 196
9.3. Quality management as well as quality control . . . . . 197
9.4. Quality management. . . . . . 197
9.4.1. Introduction . . . . . 197
9.4.2. ISO 9000. . . . . . 197
9.4.3. ISO 9001. . . . . . 198
9.4.4. Others . . . . . 200
9.4.5. Quality Assurance Manual . . . . . 205
9.4.6. Project quality . . . . . 206
9.5. What is quality of a software application? . . . . . 207
9.6. Development of a software application . . . . . 208
9.7. Software quality . . . . . 208
9.7.1. Characteristics of a software application . . . . . 209
9.7.2. Quality objective . . . . . 210
9.8. Measurement of complexity of a software application . . . . . 213
9.9. Development cycle . . . . . 213
9.9.1. Introduction . . . . . 213
9.9.2. Various lifecycles . . . . . 214
9.9.3. V cycle . . . . . 216
9.9.4. Verification and validation . . . . . 218
9.10. Vocabulary and mode of expression . . . . . 219
9.11. Organization . . . . . 220
9.11.1. Introduction . . . . . 220
9.11.2. Organization type . . . . . 220
9.11.3. Skills management . . . . . 222
9.12. Configuration management . . . . . 225
9.13. Safety assurance management. . . . . . 227
9.14. Software Quality Assurance Plan . . . . . 229
9.15. Defect management . . . . . 231
9.16. Maintenance of a software application . . . . . 233
9.17. Conclusion . . . . . 234
9.18. Appendix A – Structure of an SQAP . . . . . 235
9.19. Glossary . . . . . 236

**Chapter 10. Requirement Management** . . . . . . . . . . . . . . . . . . . . . . 239

10.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 239
10.2. Requirement acquisition phase . . . . . . . . . . . . . . . . . . . . . . . . . 240
10.2.1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 240
10.2.2. Elicitation of requirements . . . . . . . . . . . . . . . . . . . . . . . . . 241
10.2.3. Analysis process and documentation . . . . . . . . . . . . . . . . . . . . 249
10.2.4. Verification and validation of requirements . . . . . . . . . . . . . . . . . 256
10.3. Specification of requirements . . . . . . . . . . . . . . . . . . . . . . . . . . 258
10.3.1. Characterization of requirements . . . . . . . . . . . . . . . . . . . . . . 258
10.3.2. Characterization of requirements specification . . . . . . . . . . . . . . 264
10.3.3. Expression of requirements . . . . . . . . . . . . . . . . . . . . . . . . . 264
10.3.4. Validation of requirements . . . . . . . . . . . . . . . . . . . . . . . . . 269
10.4. Implementation of requirements . . . . . . . . . . . . . . . . . . . . . . . . . 269
10.4.1. Processes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 269
10.4.2. Verification . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 269
10.4.3. Traceability . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 271
10.4.4. Change management . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 275
10.5. Requirement management . . . . . . . . . . . . . . . . . . . . . . . . . . . . 278
10.5.1. Activities . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 278
10.5.2. Two approaches to requirement management . . . . . . . . . . . . . . . . 279
10.5.3. Implementation of tools . . . . . . . . . . . . . . . . . . . . . . . . . . . 279
10.6. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 281
10.7. Glossary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 281

**Conclusion** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 283

**Bibliography** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 285

**Index** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 295