

# Contents

<i>Foreword</i> . . . . .	v
<i>Acknowledgements</i> . . . . .	vi
<i>Introduction</i> . . . . .	xiii

## CHAPTER 1 A GUIDELINE FOR THE DOCUMENTATION OF CRITICAL COMPUTER SYSTEMS

### **Part 1 About this Guideline**

1.1 Scope . . . . .	4
1.2 Intended Audience . . . . .	4
1.3 Main Topics . . . . .	4
1.4 Tailoring . . . . .	4
1.5 Relationship of this Guideline to Other Documents . . . . .	5
1.6 References . . . . .	6
1.7 Principles Determining the Documentation Set . . . . .	6
1.8 Structure and Content of the Guideline . . . . .	7

### **Part 2 Documentation Guideline**

Topic 1: Management Documentation . . . . .	9
1.1 Documentation structure . . . . .	10
1.2 Documentation standards . . . . .	10
1.3 Documentation maintenance . . . . .	11
Topic 2: System Requirements Specification (SRS) . . . . .	13
Topic 3: System Description . . . . .	13
3.1 The system . . . . .	14
3.2 Hardware . . . . .	19
3.3 Software . . . . .	23
3.4 System operation and user aspects . . . . .	32

Topic 4: Technical Support Documentation . . . . .	35
4.1 Verification, validation and test plans . . . . .	36
4.2 Record of verification activities . . . . .	36
4.3 Project development report . . . . .	44
Topic 5: Project Management Documentation . . . . .	45
5.1 End-product specification . . . . .	46
5.2 Technical approach document . . . . .	46
5.3 Activity descriptions . . . . .	47
5.4 Risks and fallback documents . . . . .	47
5.5 Dependency diagrams/network . . . . .	48
5.6 Bar charts . . . . .	48
5.7 Budgets . . . . .	49
5.8 Project management and quality plans (PMQP) . . . . .	49
Topic 6: Maintenance Documentation . . . . .	54
6.1 Introduction . . . . .	54
6.2 Maintenance organisation . . . . .	55
6.3 Maintenance procedures . . . . .	57
6.4 Maintenance provisions . . . . .	60
6.5 Maintenance equipment . . . . .	60
Topic 7: Operational Documentation . . . . .	61
7.1 System overview . . . . .	61
7.2 Operator interfaces . . . . .	61
7.3 Tasks and procedures . . . . .	62
7.4 Operator responsibilities and demands . . . . .	63
Topic 8: Additional Equipment and Software Documentation . . . . .	63
8.1 Introduction . . . . .	64
8.2 Management tools . . . . .	64
8.3 Development documentation tools . . . . .	65
8.4 Verification and validation tools . . . . .	65
8.5 Operation tools . . . . .	66
8.6 Interfaces with other systems and external constraints . . . . .	67
8.7 Additional documentation . . . . .	68

## CHAPTER 2 A GUIDELINE FOR THE PRODUCTION OF SYSTEM REQUIREMENTS SPECIFICATIONS

### Part 1 About this Guideline

1.1 Scope . . . . .	72
1.2 Intended Audience . . . . .	72
1.3 Main Topics . . . . .	72
1.4 Tailoring . . . . .	72
1.5 Terms and Definitions . . . . .	73
1.6 Existing Requirements Specification Practice . . . . .	74
1.7 Structure of an SRS . . . . .	75
1.8 Relationship of this Document to Other Standards . . . . .	75
1.9 References . . . . .	75

**Part 2 About System Requirements Specifications (SRSs)**

2.1	Importance of SRSs . . . . .	76
2.2	Purpose . . . . .	77
2.3	Form . . . . .	77
2.4	Areas Subject to Customer Requirements . . . . .	77
2.5	Stability . . . . .	77
2.6	Quality—What is a Good SRS . . . . .	78
2.7	Standard SRS Outline . . . . .	81
2.8	Life-Cycle of an SRS . . . . .	81

**Part 3 The Form of a System Requirements Specification**

3.0	Title . . . . .	82
3.1	Contents . . . . .	82
3.2	Introduction . . . . .	84
3.3	About this Document . . . . .	84
3.4	Definitions of Terms Used in this Document . . . . .	87
3.5	Target System in Context . . . . .	87
3.6	Target System Requirements . . . . .	88
3.7	Target System Environment Requirements . . . . .	101
3.8	Development Project Requirements . . . . .	105
3.9	Development Project Environment Requirements . . . . .	108
3.10	Acceptance Test Plans and Criteria . . . . .	109
3.11	References . . . . .	110
3.12	Appendices . . . . .	111

**CHAPTER 3 A GUIDELINE FOR THE DEVELOPMENT OF CRITICAL SOFTWARE****Part 1 About this Guideline**

1.1	Scope . . . . .	114
1.2	Intended Audience . . . . .	114
1.3	Main Topics . . . . .	115
1.4	Tailoring . . . . .	115
1.5	Structure of the Guideline . . . . .	115

**Part 2 About the Development of Critical Software**

2.1	Guideline Approach . . . . .	116
2.2	Approach to Software Design . . . . .	117
2.3	The Development Process . . . . .	118
2.4	Appropriate Programming Language and Compiler . . . . .	118
2.5	Verification of Criteria Compliance . . . . .	119

**Part 3 Detailed Guideline for the Design and Construction of Critical Software**

3.1	Design and Construction Procedures . . . . .	121
3.2	Structuring of Software . . . . .	128

3.3	Program Self Checks . . . . .	138
3.4	Detailed Design and Coding . . . . .	142
3.5	Language-Dependent Considerations . . . . .	149

#### **Part 4 Language, Translator and Linkage Editor**

4.1	General . . . . .	153
4.2	Error Handling . . . . .	154
4.3	Data and Variable Handling . . . . .	154
4.4	Timing Aspects . . . . .	154

## **CHAPTER 4 A GUIDELINE FOR THE DESIGN AND PRODUCTION OF HARDWARE FOR SAFETY-RELATED COMPUTER SYSTEMS**

### **Part 1 About this Guideline**

1.1	Introduction . . . . .	157
1.2	Scope . . . . .	158
1.3	Intended Audience . . . . .	158
1.4	Main Topics . . . . .	158
1.5	Existing Practice . . . . .	159
1.6	Relationship of this Document to other Standards . . . . .	159
1.7	References . . . . .	159
1.8	List of Abbreviations . . . . .	160

### **Part 2 Safe Hardware**

2.1	Aim . . . . .	161
2.2	Methods . . . . .	162
2.3	Types of Failures . . . . .	164
2.4	Possibilities for Fail-Safe Systems, Including Computers . . . . .	166
2.5	A Qualitative Safety Investigation on the Influence of and Protective Measures against Failures . . . . .	173
2.6	A Quantitative Safety Investigation on the Influence of Failure-Detection Time and Failure-Detection Completeness . . . . .	182
2.7	Special Programs for Failure Detection . . . . .	214
2.8	Verification of the Checking Programs . . . . .	222
2.9	Comparative Discussion of the Various Systems from a Fail-Safe Point of View . . . . .	228
2.10	New Developments . . . . .	231

## **CHAPTER 5 A GUIDELINE FOR THE VERIFICATION AND VALIDATION OF CRITICAL COMPUTER SYSTEMS**

### **Part 1 About this Guideline**

1.1	Scope . . . . .	233
1.2	Intended Audience . . . . .	234

1.3	Assumptions . . . . .	234
1.4	The Verification and Validation Process . . . . .	235
1.5	The Verification and Validation Plan . . . . .	236
<b>Part 2 The Verification and Validation Activities</b>		
2.1	Design Verification . . . . .	237
2.2	Design Verification Report . . . . .	241
2.3	Code Verification . . . . .	242
2.4	Code Verification Report . . . . .	245
2.5	Hardware/Software Integration Verification . . . . .	245
2.6	Integration Verification Report . . . . .	247
2.7	Computer System Validation . . . . .	247
2.8	System Validation Report . . . . .	248
2.9	Post-Certification Software—Change Verification and Validation . . . . .	249
2.10	Related Standards and Guidelines . . . . .	249
 <b>CHAPTER 6 TECHNIQUES FOR THE VERIFICATION AND VALIDATION OF CRITICAL SOFTWARE</b>		
<b>Part 1 About this Guideline</b>		
1.1	Scope . . . . .	252
1.2	Intended Audience . . . . .	252
1.3	Classification . . . . .	253
1.4	Format of the Survey . . . . .	253
<b>Part 2 A Survey of Software Verification and Validation Techniques</b>		
2.1	Method Class 1: Analysis Techniques . . . . .	254
2.2	Method Class 2: Testing Techniques . . . . .	260
2.3	Method Class 3: Reliability Assessment . . . . .	267
2.4	Method Class 4: Tests of Databases . . . . .	271
2.5	References . . . . .	277
 <b>Glossary . . . . . 279</b>		
 <b>Appendix 1 EWICS TC7 Members who Assisted in the Production of these Guidelines. . . . . 283</b>		
 <b>Appendix 2 Companies of the EWICS TC7 Members . . . . . 285</b>		
 <b>Index . . . . . 287</b>		