

CONTENTS

Preface	xii
Acknowledgments	xvii
1 Introduction	1
1.1 Introduction	1
1.2 Objectives and Scope	10
1.3 Functional Safety Standards	13
1.4 The Main Elements of a SIS	17
1.5 A Brief History	21
1.6 Structure of the Book	22
1.7 Additional Reading	24
2 Concepts and Requirements	25
2.1 Introduction	25
2.2 System Hardware Aspects	25
2.3 Safety-Instrumented Functions	29
	vii

2.4	Modes of Operation	29
2.5	Safe State	31
2.6	Demands and Demand Rate	31
2.7	Testing of Safety-Instrumented Functions	32
2.8	Safety Integrity Levels (SILs)	33
2.9	Safety Life Cycle	39
2.10	Reliability of Safety-Instrumented Systems	47
2.11	Functional Safety Certificates	48
2.12	Safety Analysis Report	48
2.13	Functional Safety Assessment	49
2.14	Reliability and Decision-Making	50
2.15	Additional Reading	51
3	Failures and Failure Analysis	53
3.1	Introduction	53
3.2	Failures and Failure Modes	53
3.3	Failure Causes and Mechanisms	58
3.4	Failure Effects	58
3.5	Failure/Fault Classification	59
3.6	FMECA	71
3.7	FMEDA	75
3.8	Additional Reading	75
4	Testing and Maintenance	77
4.1	Introduction	77
4.2	Testing	78
4.3	Maintenance	87
4.4	Additional Reading	89
5	Reliability Quantification	91
5.1	Introduction	91
5.2	Reliability Block Diagrams	92
5.3	Fault Tree Analysis	105
5.4	The Beta-Factor Model	119
5.5	Markov Approach	120
5.6	Petri Net Approach	146
5.7	Additional Reading	164

6	Reliability Data Sources	165
6.1	Introduction	165
6.2	Types of Data	165
6.3	Failure Modes	167
6.4	Generic Failure Rate Sources	167
6.5	Plant-Specific Reliability Data	170
6.6	Data Dossier	172
6.7	Additional Reading	174
7	Demand Modes and Performance Measures	175
7.1	Introduction	175
7.2	Mode of Operation According to the IEC Standards	175
7.3	Functional Categories	177
7.4	Operational Strategies	179
7.5	Reliability Measures	181
7.6	$PF_{D_{avg}}$ versus PFH	186
7.7	Placement of the SIF	187
7.8	Analytical Methods	188
7.9	Assumptions and Input Data	188
7.10	Additional Reading	190
8	Average Probability of Failure on Demand	191
8.1	Introduction	191
8.2	Reliability Block Diagrams	195
8.3	Simplified Formulas	196
8.4	The IEC 61508 Formulas	223
8.5	The PDS Method	233
8.6	Fault Tree Approach	241
8.7	Markov Approach	248
8.8	Petri Net Approach	265
8.9	Additional Reading	272
9	Average Frequency of Dangerous Failures	273
9.1	Introduction	273
9.2	Frequency of Failures	274
9.3	Average Frequency of Dangerous Failures (PFH)	280
9.4	Simplified PFH Formulas	285
9.5	The IEC 61508 Formulas	295

9.6	Alternative IEC Formulas	301
9.7	The PDS Method	302
9.8	Fault Tree Approach	302
9.9	Markov Approach	304
9.10	Petri Net Approach	307
9.11	PFD_{avg} or PFH?	308
9.12	Additional Reading	308
10	Common-Cause Failures	309
10.1	Introduction	309
10.2	Causes of CCF	312
10.3	Defenses Against CCF	314
10.4	Explicit Versus Implicit Modeling	315
10.5	The Beta-Factor Model	317
10.6	The Binomial Failure Rate Model	330
10.7	Multiplicity of Faults	333
10.8	The Multiple Beta-Factor Model	335
10.9	CCF Modeling with Petri Nets	340
10.10	CCFs Between Groups and Subsystems	340
10.11	Additional Reading	341
11	Imperfect Proof-Testing	343
11.1	Introduction	343
11.2	Proof Test Coverage	344
11.3	Splitting the Failure Rate	345
11.4	Adding a Constant PFD_{avg}	353
11.5	Nonconstant Failure Rates	354
11.6	Markov Models	355
11.7	Additional Reading	358
12	Spurious Activation	359
12.1	Introduction	359
12.2	Main Concepts	362
12.3	Causes of Spurious Activation	365
12.4	Reliability Data for Spurious Operations	368
12.5	Quantitative Analysis	368
12.6	Additional Reading	379

13	Uncertainty Assessment	381
13.1	Introduction	381
13.2	What Is Uncertainty?	382
13.3	Completeness Uncertainty	383
13.4	Model Uncertainty	386
13.5	Parameter Uncertainty	387
13.6	Concluding Remarks	390
13.7	Additional Reading	391
14	Closure	393
14.1	Introduction	393
14.2	Which Approach Should Be Used?	394
14.3	Remaining Issues	395
14.4	A Final Word	397
Appendix A	Elements of Probability Theory	399
A.1	Introduction	399
A.2	Probability	401
A.3	Discrete Distributions	406
A.4	Life Distributions	410
A.5	Repairable Items	418
	Acronyms	423
	Symbols	427
	Bibliography	431
	Index	443