

Contents

Contents	9
1 Introduction	21
2 Historic Developments of Safety Systems and Standards	23
3 Standards and guidelines	27
3.1 Standard committees	27
3.2 Standards.....	31
3.2.1 DIN V 19250	32
3.2.2 DIN V VDE 0801	33
3.2.3 IEC 61508.....	36
3.2.4 IEC 61511.....	39
3.2.5 IEC 61131.....	42
3.2.6 ISA TR 84.02	44
3.2.7 RTCA DO 178B	45
3.3 Definitions around the term of safety	47
3.4 State of the Art.....	53
3.4.1 Automobile area	53
3.4.2 Aviation	54
3.4.3 Automation technology	54
4 Faults, Fault Causes and Failures	55
4.1 Failure rates	55
4.2 Fault-Failure-Deviations	60
4.3 Failure sources	62
4.4 Failure tolerance	62
4.5 Common cause failures.....	63
5 Parameter of Risk- and Reliability Analysis	65
5.1 Reliability Parameters	66
5.2 Probability of failure.....	68
5.3 Average Lifetime	68
5.4 Average Repair-Time	70
5.5 Average Duration of Usefulness.....	70
5.6 Availability	71
5.7 Failure Rate.....	71
5.8 SFF.....	73
5.9 DC.....	73
5.9.1 Tests.....	74

5.10 MTTF	75
5.10.1 MTTF – Spurious Trip Rate	75
5.11 PFD	75
6 Measures for a Risk Analysis	79
6.1 Basic concepts	79
6.2 Methods of Danger Analysis.....	80
6.2.1 Forward- and Backward-Search	80
6.2.2 Top-Down and Bottom-Up Search	81
6.3 Probability Analysis	82
6.3.1 Statistical Analysis.....	82
6.3.2 Fault Propagation Model	83
7 Risk Matrix.....	85
8 Risk Graph	89
8.1 Risk Graph according to DIN V 19250	89
8.1.1 Correlation between Risk, Acceptable Risk, Residual Risk and the Risk Reduction.....	90
8.1.2 Risk Parameter	91
8.1.3 Further Risk Parameters.....	94
8.1.4 Risk Graph	94
8.1.5 Requirement Classes.....	96
8.2 Risk Graph according to IEC 61508-5 and IEC 61511-3	97
8.3 Risk Graph according to DIN EN 954-1.....	99
9 Fault tree analysis	103
9.1 Field of application and purpose Fault Tree Analysis.....	103
9.2 Terms	104
9.3 Graphical representation	105
9.4 Analysis procedure.....	107
9.4.1 Analysis steps	107
9.4.2 System analysis.....	107
9.4.3 Undesirable event and failure criteria.....	108
9.4.4 Relevant reliability parameters and time intervals.....	109
9.4.5 Component failure modes	109
9.4.6 Fault tree creation	109
9.4.7 Evaluation of the fault tree.....	113
9.5 Fault tree analyse	120
10 Event tree analysis	121
10.1 Components Event Tree Analysis	122
11 LOPA	127
11.1 Layers of Protection	128
11.2 LOPA Valuation	131
11.3 Typical Protection Levels	132
11.3.1 Basic Process Control System	133
11.3.2 Physical equipment.....	134
11.3.3 External systems to reduce the risk.....	135

11.4 Several actuating events.....	135
12 Reliability Block Diagram Analysis	137
12.1 Reliability models	143
12.1.1 Systems without Redundancy.....	143
12.1.2 Systems with Redundancy	145
12.1.3 Mixed systems	149
12.2 Redundant Systems with Different Failure Rates	161
12.3 Substitution of Redundant System Components through Single System Components	165
13 Markov-Model	169
13.1 Introduction.....	169
13.2 Possibilities with Markov models	170
13.3 Theoretical Principals of the Markov Models.....	170
13.4 Time dependent Markov Models	175
13.5 Implementation of a Markov Calculation for a Safety Related System.....	175
13.5.1 Transition Matrix P for System Model.....	178
14 Lifecycle Analysis of a Safety System.....	185
14.1 Hazard and Risk Analysis.....	185
14.2 Execution of a Risk Evaluation Analysis.....	185
14.3 Life Cycle Phases.....	187
14.3.1 Development of asafety-instrumented function.....	187
14.3.2 Failure models and PFD calculation.....	189
14.3.3 System Architecture	191
14.4 Overall Planning	195
14.5 Realization of a SIS	195
14.6 Installation, Startup and Validation	197
14.7 Operation, Maintenance and Repair	197
14.8 Modification and Retrofit	198
14.9 Summary	199
15 Common Cause Failure.....	201
15.1 General.....	201
15.2 Common cause failures.....	202
15.2.1 Analysis of Common Cause Failures	203
15.3 Common Mode Failure	207
15.4 Examples for Failures through a Common Cause	208
15.5 Technologies for the Evaluation of SIS Designs for CCF.....	208
15.5.1 Industrial Standards	209
15.5.2 Technical organization-specific Guidelines and Standards	209
15.5.3 Qualitative hazard identification methods	209
15.5.4 Qualitative Valuation.....	210
15.5.5 Checklists	210
15.6 Quantitative Evaluation of Common Cause Failures.....	211
15.6.1 Explicit Methods	211
15.6.2 Implicit Methods of Common Cause Failures.....	219
15.6.2.1 Basic-Parameter-Model.....	220

15.6.2.2 Beta-Factor-Model.....	220
15.6.2.3 Multy Greek Letter Model.....	221
15.6.2.4 α -Factor Model	221
15.6.2.5 Binomial Failure Rate Model (BFR)	222
15.7 β -Factor.....	223
15.7.1 The Effect of the β -factor on safety	225
15.7.2 Assessment of the β -factor.....	226
15.8 1oo2 System.....	229
15.8.1 Probability of Failure with Common Cause Failures.....	229
15.9 Measures against Failures through Common Cause	231
16 Proof Test.....	233
16.1 Monitoring and Conducting of Proof Tests	233
16.2 Types of Proof Tests	234
16.3 Reliability Function and MTTF	235
16.3.1 Failure Probability	235
16.3.2 Probability of Failure on Demand.....	236
16.3.3 Proof Test Interval T_1	236
16.4 Definition of the Proof Test according to IEC/EN 61508.....	237
16.5 Consequences of an Insufficient Proof Test.....	237
16.6 Differences between Diagnostic Test and Proof Test	238
16.6.1 Definition of Diagnostic and Proof Test.....	238
16.6.2 Performance Indicators	239
16.6.3 Results of Calculations with or without Diagnosis.....	240
16.6.4 PFD-Calculation with Variable Proof Test Coverage.....	241
16.7 Influence of Proof Test Interval on PFD_{avg} -Value	242
16.8 Risk Reduction	244
16.8.1 Risk Rate and Average Failure Probability.....	245
16.8.2 Proof Test Frequency.....	246
16.8.3 Proof Test Expansion Factor.....	248
17 Hardware of Safety-Related Systems	251
17.1 Normative Architectural Specifications	251
17.1.1 Quality in Safety for Users of Safety-Critical Systems	251
17.1.2 Implementing Safety for Manufacturers of Safety-Critical Systems	252
17.2 Hardware Safety Life Cycle.....	253
17.2.1 Safety Requirements Specification	253
17.2.2 Safety Validation Planning	255
17.2.3 Design and Development of the E/E/PES.....	255
17.3 Hardware Fault Tolerance.....	255
17.4 Constraints	257
17.4.1 Architectural Constraints	257
17.4.2 General Concepts of Risk Reduction.....	258
17.5 1oo1 System.....	260
17.5.1 PFD-Fault Tree in 1oo1-Architecture	261
17.5.2 Markov Model of 1oo1-Architecture.....	262
17.5.3 Calculation of the MTTF-Value of a 1oo1-Architecture.....	263
17.6 Additional Architectures	266

18 Software requirements for a system with functional safety	283
18.1 Software in systems with functional safety	283
18.1.1 Software requirements	287
18.1.2 Non-functional requirements	287
18.1.2.1 Goal setting	288
18.1.2.2 Goal control	288
18.1.3 Categories of non-functional requirements	289
18.2 Software development	290
18.2.1 Models of software development	292
18.2.1.1 Waterfall model	293
18.2.1.2 Spiral model	294
18.2.1.3 V-Model	294
18.2.1.4 Project planning	295
18.2.2 Specification of requirements	295
18.2.2.1 Characteristics of a specification	296
18.2.2.2 Description of requirements	297
18.2.2.3 Formality of requirements	298
18.2.2.4 Customer requirement specifications	299
18.2.3 Software architecture	299
18.2.3.1 Breakdown into components	300
18.2.3.2 Intersections	301
18.2.3.3 Communication within the system	301
18.2.3.4 Ability to test components	301
18.2.3.5 Additional quality characteristics	301
18.2.3.6 Resources	302
18.2.3.7 Quality of the solution	303
18.2.4 Possible architectural styles	303
18.2.4.1 Functional orientation	303
18.2.4.2 Object orientation	304
18.2.5 Reusable architectural structures	304
18.2.5.1 Design patterns	304
18.2.5.2 Frames	305
18.2.5.3 Architectural design	305
18.2.6 Programming convention	305
18.2.6.1 Documentation and appearance of source text	306
18.2.6.2 Naming convention	306
18.2.7 Software development with UML	307
18.2.7.1 Object-oriented analysis	307
18.2.8 Object-oriented design	309
18.2.8.1 Architecture	309
18.2.8.2 Assigning procedural structures	310
18.2.8.3 Developing design classes	310
18.2.8.4 Describing component intersections	310
18.2.8.5 Specializing status models	311
18.2.8.6 Object flow of activity models	311
18.2.8.7 Modeling interaction models	311
18.2.8.8 Developing tests	311

18.2.8.9 Specifying attributes	312
18.2.9 The use of CASE tools.....	312
18.2.9.1 Round trip engineeringwith CASE tools	312
18.2.9.2 MDA	313
18.2.9.3 Comparison of UML CASE tools.....	314
18.2.10 Software quality	314
18.2.10.1 Quality plan	316
18.2.11 Software reliability	317
18.2.11.1 Measurements of reliability	318
18.2.11.2 Differences between hardware and software reliability.....	318
18.2.11.3 Increase in reliability by verification and validation.....	320
18.2.11.4 Validation of reliability.....	322
18.2.11.5 Proof of reliability.....	323
18.2.12 Measuring software quality	323
18.2.12.1 Lines of code (LoC).....	325
18.2.12.2 McCabe measure.....	325
18.2.12.3 Halstead measures.....	326
18.2.12.4 Usefulness of formulas	327
18.2.13 Failures in software systems	327
18.2.14 Testing procedure	329
18.2.14.1 Testing procedure	330
18.2.14.2 Black box test methods.....	331
18.2.14.3 White box test methods.....	332
18.2.14.4 Intuitive test case determination	333
18.2.15 Testing in practice.....	333
18.2.16 Integration.....	333
18.2.16.1 Top-down integration	334
18.2.16.2 Bottom-up integration.....	334
18.2.16.3 Outside-in integration	335
18.2.17 System and certification test	335
19 Application examples.....	337
19.1 Practical Implementation of the IEC 61508 Safety Standard.....	337
19.1.1 IEC 61508 Norm.....	338
19.1.1.1 Functional Safety Management	340
19.1.1.2 Pipe to Pipe Approach	341
19.1.1.3 Quantitative Safety Evaluation	342
19.2 Determining the SIL of a Processor Based System.....	343
19.2.1 SIL Requirements	344
19.2.2 Determining the SIL of a Processor Unit with Processor Periphery.....	345
19.2.3 DC-Measures for a Processor Unit with Processor Periphery	346
19.2.3.1 Processor Units	346
19.2.3.2 Read-Only Memory	346
19.2.3.3 Alterable Memory.....	347
19.3 Determining the SIL of a Safety Function	349
19.3.1 Determining the SIL of a Safety Function.....	350
19.3.2 Modification of the Architecture of a Safety Function.....	351
19.3.3 Determination of the SIL of a Modified Safety Function	353

19.3.4 Modification of the Safety Function.....	355
19.3.5 Determining the SIL of a Safety Function with Diagnosis.....	356
19.4 Determining the SIL of a Safety Loop.....	358
19.4.1 Determining the SIL of the Safety Loop	360
19.5 Examples of Reliability Analyses	363
19.5.1 Example 1 (Chemical Installation)	363
19.5.1.1 Risk Graph.....	364
19.5.1.2 Event Tree	365
19.5.1.3 Error Tree Analysis	366
19.5.1.4 Reliability Block Diagram.....	366
19.5.2.1 Risk graph.....	368
19.5.2.2 Event Tree	369
19.5.2.3 Error tree analysis.....	370
19.5.2.4 Reliability block diagram	371
19.5.3 Example 3 (Airplane)	372
19.5.3.1 Risk Graph.....	372
19.5.3.2 Event Tree	374
19.5.3.3 Fault Tree Analysis.....	374
19.5.4 Example 4 (Pipeline)	376
19.5.4.1 Risk Graph.....	377
19.5.4.2 Event Tree	378
19.5.4.3 Error tree analysis.....	378
19.5.5 Example 5 (Coliseum)	379
19.5.5.1 Risk graph.....	380
19.5.5.2 Event tree.....	381
19.5.5.3 Error tree analysis.....	382
20 IEC/EN 61508.....	383
20.1 IEC/EN 61508-1	384
20.1.1 Outline and Field of Application	384
20.1.2 Compliance with this Standard.....	386
20.1.3 Documentation	386
20.1.4 Safety Management	386
20.1.5 The Complete Safety Lifecycle	387
20.1.6 Verification.....	389
20.1.7 Evaluation of Functional Safety	390
20.2 IEC/EN 61508-2	390
20.2.1 Field of Application.....	390
20.2.2 The E/E/PES Safety Lifecycle.....	390
20.2.3 Techniques and Measures for Control of Failures during Operation	392
20.2.4 Methods for Avoiding Systematic Errors During Different Phases of the Lifecycle.....	393
20.3 IEC/EN61508-3	393
20.3.1 Field of Application.....	393
20.3.2 Quality Management System of Software	393
20.3.3 Software Safety Lifecycle	393
20.3.4 Evaluation of Functional Safety	395
20.3.5 Appendix A Guidelines for the Selection of Techniques and Methods	395

20.4 IEC/EN 61508-4	395
20.4.1 Terms Regarding Safety	395
20.4.2 Terms relating to Devices and Equipment.....	396
20.4.3 System Terms	396
20.4.4 Terms relating to Safety Functions and Safety Integrity	398
20.4.5 Terms relating to Errors, Failure, and Deviation	399
20.4.6 Terms relating to Lifecycle.....	399
20.4.7 Terms relating to Verification of Safety Measures	399
20.5 IEC/EN 61508-5	400
20.5.1 Field of Application.....	400
20.5.2 Appendix A – Underlying Concepts.....	400
20.5.3 Appendix B - ALARP and the Concept of Tolerable Risk.....	400
20.5.4 Appendix C- Quantitative Methods for Determining the Safety Integrity Level.....	402
20.5.5 Appendix D – Qualitative Methods for Determining the Safety Integrity Level (Risk Graph).....	403
20.5.6 Appendix E – Specification of the Safety Integrity Level A Qualitative Procedure – Matrix of the Extent of a Dangerous Event.....	404
20.6 IEC/EN 61508-6	405
20.6.1 Field of Application.....	405
20.6.2 Appendix A – Application of IEC/EN 61508-2 and -3	406
20.6.3 Appendix B – Exemplary Procedure for Determining Hardware Failures.....	406
20.6.4 Appendix D – Methods for Quantifying the Consequences of Hardware Failures due to the Same Cause in E/E/PES	411
20.7 IEC/EN 61508-7	411
20.7.1 Field of Application.....	411
20.7.2 Appendix A – Overview of Procedures and Measures for E/E/PES: Control of Accidental Hardware Failures.....	411
20.7.3 Appendix B – Overview of Techniques and Measures for Prevention of Systematic Failures.....	413
20.7.4 Appendix C – Overview of Techniques and Measures for Achieving Safety Integrity of Software.....	414
21 IEC 61511	417
21.1 Scope of Application.....	417
21.2 Subdivision of Standard 61511	419
21.3 Terms and Abbreviations	422
21.3.1 Abbreviations.....	422
21.3.2 Terms	423
21.4 Management of Functional Safety	434
21.4.1 Goal.....	434
21.4.2 Requirements	434
21.4.3 Evaluation, Auditing, and Revisions	434
21.4.4 SIS Configuration Management	435
21.5 Safety Lifecycle Requirements	435
21.6 Verification	438
21.6.1 Goal.....	438
21.6.2 Requirements	438

21.7 Hazard Analysis and Risk Evaluation.....	438
21.7.1 Goal	438
21.7.2 Requirements	439
21.8 Allocation of Safety Functions to Protection Layers	439
21.8.1 Goal	439
21.8.2 Allocation Requirements	439
21.8.3 Safety Integrity Level 4 Requirements	440
21.8.4 Demands on Factory Devices Used as Protective Layers.....	440
21.8.5 Requirements for Failure Avoidance.....	441
21.9 Safety Specification of the SIS	441
21.9.1 Goal	441
21.9.2 SIS Safety Requirements	441
21.10 SIS Design and Planning	441
21.10.1 Goal	441
21.10.2 General Requirements	441
21.10.3 Demands on Safety Behavior upon Error Detection	442
21.10.4 Demands on Hardware Error Tolerance.....	442
21.10.5 Demands on the Selection of Components and Subsystems	443
21.10.6 Field Devices	443
21.10.7 Interfaces	443
21.10.8 Maintenance and Test Device Requirements.....	444
21.10.9 Failure Probability of Safety-technical Functions	444
21.11 Application Software Requirements	444
21.11.1 Demands on the Safety Lifecycle of Application Software.....	445
21.11.2 Specification of Application Software Safety Requirements	449
21.11.3 Validation Planning for Application Software Safety	450
21.11.4 Design and Construction of Application Software.....	450
21.11.5 Integration of the Application Software into the SIS Subsystem	451
21.11.6 Procedure for Modification of Application Software.....	452
21.11.7 Verification of Application Software	452
21.12 Final Inspection	452
21.12.1 Goals.....	452
21.12.2 Recommendations	452
21.13 SIS Assembly and Implementation.....	452
21.14 SIS Safety Validation.....	453
21.15 Operation and Maintenance of the SIS	453
21.15.1 Goals.....	453
21.15.2 Requirements	453
21.15.3 Re-examination and Inspection	454
21.16 SIS Modifications	454
21.16.1 Goals.....	454
21.16.2 Requirements	454
21.17 Decommissioning of the SIS	455
21.18 Documentation Requirements.....	455
21.18.1 Goal	455
21.18.2 Requirements.....	455

22 Terms and Definitions	457
22.1 Safety Systems	457
22.1.1 Risk	457
22.1.2 Partial Risk.....	457
22.1.3 Risk Limit	457
22.1.4 Risk Parameters	457
22.1.5 Requirement Class	458
22.1.6 Measures	458
22.1.7 Protection.....	458
22.1.8 Measurement and Control Protection Measures	458
22.1.9 MSR Protection Installation.....	458
22.1.10 Undesired Event.....	458
22.1.11 Error.....	458
22.1.12 Redundancy	459
22.1.13 Diverse Redundancy	459
22.1.14 Failsafe.....	459
22.2. Dependability	459
22.2.1 Reliability.....	460
22.2.2 Availability	461
22.2.3 Safety	462
22.2.4 Maintainability	462
22.3 Documentation of Failure Behavior.....	462
22.3.1 Density Function resp. Failure Density $f(t)$	463
22.3.2 Failure Probability, resp. Distribution Function $F(t)$	466
22.3.3 Reliability, resp., Survival Probability $R(t)$	469
22.3.4 Failure rate $\lambda(t)$	471
22.3.5 Description of Failure Behavior by Examples	473
22.3.6 Boolean Theory	477
22.4 Time Factor	478
22.4.1 MTTF.....	479
22.4.2 $MTTF_{\text{spurious}}$	479
22.4.3 MTBF	480
22.4.4 MTTR	480
22.4.5 Example for Calculation of MTTF	480
22.4.6 Continuous Availability.....	480
22.4.7 Downtime DT	482
22.4.8 Uptime UT	483
22.4.9 Mean Down Time MDT	483
22.5 General Thoughts About Terms and Standards	484
22.5.1 Degree of Diagnostic Coverage DC	486
22.5.2 Common Cause Failure CCF.....	486
22.5.3 Probability of Failure on Demand PFD	487
22.5.4 Failure Rates	488
22.5.5 Risk, Damage, and Danger	491
22.5.6 Hazard Rate	492
22.5.7 Safety Integrity Level SIL	492

22.6 Process Control Technique PLT	496
22.7 Performance Level PL	497
Literature	499
Index	531