

Contents

Contents9

1 Introduction21

2 Historic Developments of Safety Systems and Standards.....23

3 Standards and guidelines27

3.1 Standard committees.....27

3.2 Standards30

3.2.1 DIN V 1925032

3.2.2 DIN V VDE 080132

3.2.3 IEC 61508.....35

3.2.4 IEC 61511.....38

3.2.5 EN ISO 1384941

3.2.6 IEC 61131.....43

3.2.7 ISA TR 84.02.....44

3.2.8 RTCA DO 178B45

3.3 Definitions around the term of safety47

3.4 State of the Art.....50

3.4.1 Automobile area – ISO 2626250

3.4.2 Aviation55

3.4.3 Automation technology55

4 Faults, Fault Causes and Failures57

4.1 Failure rates57

4.2 Fault-Failure-Deviations.....62

4.3 Failure sources.....63

4.4 Failure tolerance64

4.5 Common cause failures65

5 Parameter of Risk- and Reliability Analysis67

5.1 Reliability Parameters.....68

5.2 Probability of failure.....70

5.3 Average Lifetime70

5.4	Average Repair-Time	71
5.5	Average Duration of Usefulness.....	71
5.6	Availability	72
5.7	Failure Rate.....	72
5.8	SFF.....	74
5.9	DC.....	74
	5.9.1 Tests.....	75
5.10	MTTF.....	76
	5.10.1 MTTF – Spurious Trip Rate	76
5.11	PFD.....	76
6	Measures for a Risk Analysis.....	81
6.1	Basic Concepts.....	81
6.2	Methods of Danger Analysis	82
	6.2.1 Forward- and Backward-Search	82
	6.2.2 Top-Down and Bottom-Up Search	83
6.3	Probability Analysis.....	83
	6.3.1 Statistical Analysis.....	83
	6.3.2 Fault Propagation Model	84
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	98
9	Fault tree analysis	103
9.1	Field of application and purpose Fault Tree Analysis	103
9.2	Terms	104
9.3	Graphical representation	106
9.4	Analysis procedure	107
	9.4.1 Analysis steps	107
	9.4.2 System analysis	108
	9.4.3 Undesirable event and failure criteria	109
	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 analysis	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	142
12.1.1	Systems without Redundancy	142
12.1.2	Systems with Redundancy	144
12.1.3	Mixed systems	148
12.2	Redundant Systems with Different Failure Rates	159
12.3	Substitution of Redundant System Components through Single System Components	164
13	Markov Model	167
13.1	Introduction	167
13.2	Possibilities with Markov Models	168
13.3	Theoretical Principals of the Markov Models	168
13.4	Time dependent Markov Models	173
13.5	Implementation of a Markov Calculation for a Safety Related System	173
13.5.1	Transition Matrix P for System Model	176
14	Lifecycle Analysis of a Safety System	183
14.1	Hazard and Risk Analysis	183
14.2	Execution of a Risk Evaluation Analysis	183
14.3	Life Cycle Phases	185
14.3.1	Development of a safety-instrumented function	185
14.3.2	Failure models and PFD calculation	187
14.3.3	System Architecture	189
14.4	Overall Planning	193
14.5	Realization of a SIS	193

14.6	Installation, Startup and Validation	195
14.7	Operation, Maintenance and Repair	195
14.8	Modification and Retrofit	196
14.9	Summary	196
15	Common Cause Failure.....	199
15.1	General.....	199
15.2	Common cause failures.....	200
15.2.1	Analysis of Common Cause Failures.....	201
15.3	Common Mode Failure	204
15.4	Examples for Failures through a Common Cause	205
15.5	Technologies for the Evaluation of SIS Designs for CCF	206
15.5.1	Industrial Standards	206
15.5.2	Technical organization-specific Guidelines and Standards	206
15.5.3	Qualitative hazard identification methods	207
15.5.4	Qualitative Valuation.....	207
15.5.5	Checklists.....	208
15.6	Quantitative Evaluation of Common Cause Failures.....	208
15.6.1	Explicit Methods.....	209
15.6.2	Implicit Methods of Common Cause Failures	216
15.6.2.1	Basic-Parameter-Model	217
15.6.2.2	Beta-Factor-Model.....	217
15.6.2.3	Multy Greek Letter Model	218
15.6.2.4	α -Factor Model	218
15.6.2.5	Binomial Failure Rate Model (BFR)	219
15.7	β -Factor.....	220
15.7.1	The Effect of the β -factor on safety	221
15.7.2	Assessment of the β -factor.....	223
15.8	1oo2 System.....	225
15.8.1	Probability of Failure with Common Cause Failures.....	225
15.9	Measures against Failures through Common Cause	227
16	Proof Test	229
16.1	Monitoring and Conducting of Proof Tests	229
16.2	Types of Proof Tests	230
16.3	Reliability Function and MTTF	231
16.3.1	Failure Probability	231
16.3.2	Probability of Failure on Demand.....	232
16.3.3	Proof Test Interval T_1	232
16.4	Definition of the Proof Test according to IEC/EN 61508	233
16.5	Consequences of an Insufficient Proof Test	233
16.6	Differences between Diagnostic Test and Proof Test.....	234
16.6.1	Definition of Diagnostic and Proof Test.....	234

16.6.2	Performance Indicators.....	235
16.6.3	Results of Calculations with or without Diagnosis.....	236
16.6.4	PFD-Calculation with Variable Proof Test Coverage	237
16.7	Influence of Proof Test Interval on PFD_{avg} -Value.....	238
16.8	Risk Reduction	240
16.8.1	Risk Rate and Average Failure Probability	241
16.8.2	Proof Test Frequency	242
16.8.3	Proof Test Expansion Factor	244
17	Hardware of Safety-Related Systems	247
17.1	Normative Architectural Specifications.....	247
17.1.1	Quality in Safety for Users of Safety-Critical Systems	247
17.1.2	Implementing Safety for Manufacturers of Safety-Critical Systems.....	248
17.2	Hardware Safety Life Cycle	249
17.2.1	Safety Requirements Specification.....	249
17.2.2	Safety Validation Planning.....	251
17.2.3	Design and Development of the E/E/PES	251
17.3	Hardware Fault Tolerance	251
17.4	Constraints.....	253
17.4.1	Architectural Constraints.....	253
17.4.2	General Concepts of Risk Reduction.....	253
17.5	1001 System	256
17.5.1	PFD -Fault Tree in 1001-Architecture	256
17.5.2	Markov Model of 1001-Architecture	258
17.5.3	Calculation of the MTTF-Value of a 1001-Architecture.....	259
17.6	Additional Architectures.....	261
18	Software requirements for a system with functional safety.....	277
18.1	Software in systems with functional safety	277
18.1.1	Software requirements.....	281
18.1.2	Non-functional requirements.....	281
18.1.2.1	Goal setting.....	281
18.1.2.2	Goal control	282
18.1.3	Categories of non-functional requirements	282
18.2	Software development	284
18.2.1	Models of software development.....	286
18.2.1.1	Waterfall model	286
18.2.1.2	Spiral model.....	287
18.2.1.3	V-Model	288
18.2.1.4	Project planning.....	289
18.2.2	Specification of requirements	289
18.2.2.1	Characteristics of a specification	290
18.2.2.2	Description of requirements	291
18.2.2.3	Formality of requirements	291
18.2.2.4	Customer requirement specifications.....	292

- 18.2.3 Software architecture 292
 - 18.2.3.1 Breakdown into components 293
 - 18.2.3.2 Intersections 293
 - 18.2.3.3 Communication within the system..... 294
 - 18.2.3.4 Ability to test components 294
 - 18.2.3.5 Additional quality characteristics..... 294
 - 18.2.3.6 Resources 295
 - 18.2.3.7 Quality of the solution 295
- 18.2.4. Possible architectural styles 296
 - 18.2.4.1 Functional orientation 296
 - 18.2.4.2 Object orientation 297
- 18.2.5 Reusable architectural structures 297
 - 18.2.5.1 Design patterns 297
 - 18.2.5.2 Frames..... 298
 - 18.2.5.3 Architectural design..... 298
- 18.2.6 Programming convention..... 298
 - 18.2.6.1 Documentation and appearance of source text 298
 - 18.2.6.2 Naming convention..... 299
- 18.2.7 Software development with UML 300
 - 18.2.7.1 Object-oriented analysis 300
- 18.2.8 Object-oriented design 301
 - 18.2.8.1 Architecture 302
 - 18.2.8.2 Assigning procedural structures..... 302
 - 18.2.8.3 Developing design classes 303
 - 18.2.8.4 Describing component intersections 303
 - 18.2.8.5 Specializing status models 303
 - 18.2.8.6 Object flow of activity models..... 303
 - 18.2.8.7 Modeling interaction models 303
 - 18.2.8.8 Developing tests..... 304
 - 18.2.8.9 Specifying attributes 304
- 18.2.9 The use of CASE tools..... 304
 - 18.2.9.1 Round trip engineering with CASE tools 305
 - 18.2.9.2 MDA 306
 - 18.2.9.3 Comparison of UML CASE tools..... 306
- 18.2.10 Software quality 307
 - 18.2.10.1 Quality plan..... 309
- 18.2.11 Software reliability 310
 - 18.2.11.1 Measurements of reliability 310
 - 18.2.11.2 Differences between hardware and software reliability..... 311
 - 18.2.11.3 Increase in reliability by verification and validation..... 313
 - 18.2.11.4 Validation of reliability..... 314
 - 18.2.11.5 Proof of reliability..... 315
- 18.2.12 Measuring software quality..... 315
 - 18.2.12.1 Lines of code (LoC)..... 317
 - 18.2.12.2 McCabe measure..... 317
 - 18.2.12.3 Halstead measures..... 318
 - 18.2.12.4 Usefulness of formulas 319

- 18.2.13 Failures in software systems319
- 18.2.14 Testing procedure321
 - 18.2.14.1 Testing procedure321
 - 18.2.14.2 Black box test methods.....322
 - 18.2.14.3 White box test methods323
 - 18.2.14.4 Intuitive test case determination324
- 18.2.15 Testing in practice325
- 18.2.16 Integration.....325
 - 18.2.16.1 Top-down integration325
 - 18.2.16.2 Bottom-up integration.....326
 - 18.2.16.3 Outside-in integration326
- 18.2.17 System and certification test.....327
- 19 Application examples329**
 - 19.1 Practical Implementation of the IEC 61508 Safety Standard329
 - 19.1.1 IEC 61508 Norm330
 - 19.1.1.1 Functional Safety Management332
 - 19.1.1.2 Pipe to Pipe Approach334
 - 19.1.1.3 Quantitative Safety Evaluation335
 - 19.2 Determining the SIL of a Processor Based System335
 - 19.2.1 SIL Requirements336
 - 19.2.2 Determining the SIL of a Processor Unit with Processor Periphery337
 - 19.2.3 DC-Measures for a Processor Unit with Processor Periphery337
 - 19.2.3.1 Processor Units337
 - 19.2.3.2 Read-Only Memory338
 - 19.2.3.3 Alterable Memory339
 - 19.3 Determining the SIL of a Safety Function.....340
 - 19.3.1 Determining the SIL of a Safety Function.....341
 - 19.3.2 Modification of the Architecture of a Safety Function.....342
 - 19.3.3 Determination of the SIL of a Modified Safety Function.....344
 - 19.3.4 Modification of the Safety Function.....345
 - 19.3.5 Determining the SIL of a Safety Function with Diagnosis.....347
 - 19.4 Determining the SIL of a Safety Loop348
 - 19.4.1 Determining the SIL of the Safety Loop350
 - 19.5 Examples of Reliability Analysis353
 - 19.5.1 Example 1 (Chemical Installation)353
 - 19.5.1.1 Risk Graph.....353
 - 19.5.1.2 Event Tree355
 - 19.5.1.3 Error Tree Analysis356
 - 19.5.1.4 Reliability Block Diagram357
 - 19.5.2 Example 2 (Driver-Side Airbag)358
 - 19.5.2.1 Risk graph.....358
 - 19.5.2.2 Event Tree360
 - 19.5.2.3 Error Tree Analysis360
 - 19.5.2.4 Reliability Block Diagram361
 - 19.5.3 Example 3 (Airplane)362

19.5.3.1 Risk Graph	362
19.5.3.2 Event Tree.....	364
19.5.3.3 Fault Tree Analysis.....	364
19.5.4 Example 4 (Pipeline)	367
19.5.4.1 Risk Graph	367
19.5.4.2 Event Tree.....	368
19.5.4.3 Error Tree Analysis.....	369
19.5.5 Example 5 (Coliseum)	370
19.5.5.1 Risk Graph	371
19.5.5.2 Event Tree.....	371
19.5.5.3 Error Tree Analysis.....	372
20 IEC/EN 61508.....	373
20.1 IEC/EN 61508-1	374
20.1.1 Outline and Field of Application	374
20.1.2 Compliance with this Standard	376
20.1.3 Documentation.....	376
20.1.4 Safety Management	376
20.1.5 The Complete Safety Lifecycle.....	378
20.1.6 Verification	380
20.1.7 Evaluation of Functional Safety.....	380
20.2 IEC/EN 61508-2	380
20.2.1 Field of Application.....	380
20.2.2 The E/E/PES Safety Lifecycle	381
20.2.3 Techniques and Measures for Control of Failures during Operation.....	383
20.2.4 Methods for Avoiding Systematic Errors during Different Phases of the Lifecycle	383
20.3 IEC/EN 61508-3	383
20.3.1 Field of Application.....	383
20.3.2 Quality Management System of Software	383
20.3.3 Software Safety Lifecycle.....	383
20.3.4 Evaluation of Functional Safety.....	385
20.3.5 Appendix A – Guidelines for the Selection of Techniques and Methods.	385
20.4 IEC/EN 61508-4	385
20.4.1 Terms Regarding Safety	385
20.4.2 Terms relating to Devices and Equipment.....	386
20.4.3 System Terms.....	386
20.4.4 Terms relating to Safety Functions and Safety Integrity	388
20.4.5 Terms relating to Errors, Failure, and Deviation	389
20.4.6 Terms relating to Lifecycle	389
20.4.7 Terms relating to Verification of Safety Measures	389
20.5 IEC/EN 61508-5	390
20.5.1 Field of Application.....	390
20.5.2 Appendix A – Underlying Concepts.....	390
20.5.3 Appendix B – ALARP and the Concept of Tolerable Risk	391

20.5.4 Appendix C – Quantitative Methods for Determining the Safety Integrity Level.....393

20.5.5 Appendix D – Qualitative Methods for Determining the Safety Integrity Level (Risk Graph).....394

20.5.6 Appendix E – Specification of the Safety Integrity Level A Qualitative Procedure – Matrix of the Extent of a Dangerous Event.....395

20.6 IEC/EN 61508-6.....396

20.6.1 Field of Application.....396

20.6.2 Appendix A – Application of IEC/EN 61508-2 and -3396

20.6.3 Appendix B – Exemplary Procedure for Determining Hardware Failures 396

20.6.4 Appendix D – Methods for Quantifying the Consequences of Hardware Failures due to the Same Cause in E/E/PES401

20.7 IEC/EN 61508-7.....401

20.7.1 Field of Application.....401

20.7.2 Appendix A – Overview of Procedures and Measures for E/E/PES: Control of Accidental Hardware Failures.....401

20.7.3 Appendix B – Overview of Techniques and Measures for Prevention of Systematic Failures403

20.7.4 Appendix C – Overview of Techniques and Measures for Achieving Safety Integrity of Software.....404

21 IEC 61511.....405

21.1 Scope of Application405

21.2 Subdivision of Standard IEC 61511407

21.3 Terms and Abbreviations.....410

21.3.1 Abbreviations410

21.3.2 Terms411

21.4 Management of Functional Safety.....422

21.4.1 Goal422

21.4.2 Requirements422

21.4.3 Evaluation, Auditing, and Revisions422

21.4.4 SIS Configuration Management423

21.5 Safety Lifecycle Requirements.....423

21.6 Verification.....426

21.6.1 Goal426

21.6.2 Requirements426

21.7 Hazard Analysis and Risk Evaluation426

21.7.1 Goal426

21.7.2 Requirements426

21.8 Allocation of Safety Functions to Protection Layers.....427

21.8.1 Goal427

21.8.2 Allocation Requirements427

21.8.3 Safety Integrity Level 4 Requirements427

21.8.4 Demands on Factory Devices Used as Protective Layers.....428

21.8.5 Requirements for Failure Avoidance.....428

21.9	Safety Specification of the SIS	429
21.9.1	Goal.....	429
21.9.2	SIS Safety Requirements	429
21.10	SIS Design and Planning	429
21.10.1	Goal.....	429
21.10.2	General Requirements.....	429
21.10.3	Demands on Safety Behavior upon Error Detection.....	430
21.10.4	Demands on Hardware Error Tolerance	430
21.10.5	Demands on the Selection of Components and Subsystems.....	431
21.10.6	Field Devices	431
21.10.7	Interfaces.....	431
21.10.8	Maintenance and Test Device Requirements.....	432
21.10.9	Failure Probability of Safety-technical Functions	432
21.11	Application Software Requirements	432
21.11.1	Demands on the Safety Lifecycle of Application Software.....	433
21.11.2	Specification of Application Software Safety Requirements.....	437
21.11.3	Validation Planning for Application Software Safety	438
21.11.4	Design and Construction of Application Software	438
21.11.5	Integration of the Application Software into the SIS Subsystem	439
21.11.6	Procedure for Modification of Application Software	440
21.11.7	Verification of Application Software.....	440
21.12	Final Inspection	440
21.12.1	Goals.....	440
21.12.2	Recommendations.....	440
21.13	SIS Assembly and Implementation.....	440
21.14	SIS Safety Validation.....	441
21.15	Operation and Maintenance of the SIS	441
21.15.1	Goals.....	441
21.15.2	Requirements	441
21.15.3	Re-examination and Inspection.....	442
21.16	SIS Modifications	442
21.16.1	Goals.....	442
21.16.2	Requirements	442
21.17	Decommissioning of the SIS	442
21.18	Documentation Requirements.....	443
21.18.1	Goal.....	443
21.18.2	Requirements	443
22	Terms and Definitions	445
22.1	Safety Systems.....	445
22.1.1	Risk.....	445
22.1.2	Partial Risk.....	445
22.1.3	Risk Limit	445
22.1.4	Risk Parameters	445
22.1.5	Requirement Class	445

22.1.6 Measures.....	446
22.1.7 Protection.....	446
22.1.8 Measurement and Control Protection Measures.....	446
22.1.9 MSR Protection Installation	446
22.1.10 Undesired Event	446
22.1.11 Error.....	446
22.1.12 Redundancy	446
22.1.13 Diverse Redundancy.....	446
22.1.14 Failsafe	447
22.2. Dependability	447
22.2.1 Reliability	448
22.2.2 Availability	449
22.2.3 Safety	450
22.2.4 Maintainability.....	450
22.3 Documentation of Failure Behavior	450
22.3.1 Density Function, resp. Failure Density $f(t)$	450
22.3.2 Failure Probability, resp. Distribution Function $F(t)$	453
22.3.3 Reliability, resp. Survival Probability $R(t)$	456
22.3.4 Failure rate $\lambda(t)$	458
22.3.5 Description of Failure Behavior by Examples.....	460
22.3.6 Boolean Theory	464
22.4 Time Factor	465
22.4.1 MTTF	466
22.4.2 MTTF _{spurious}	466
22.4.3 MTBF	466
22.4.4 MTTR	467
22.4.5 Example for Calculation of MTTF	467
22.4.6 Continuous Availability.....	467
22.4.7 Downtime DT	469
22.4.8 Uptime UT	470
22.4.9 Mean Down Time MDT	470
22.5 General Thoughts About Terms and Standards.....	470
22.5.1 Degree of Diagnostic Coverage DC	472
22.5.2 Common Cause Failure CCF	473
22.5.3 Probability of Failure on Demand PFD	474
22.5.4 Failure Rates	475
22.5.5 Risk, Damage, and Danger	478
22.5.6 Hazard Rate	479
22.5.7 Safety Integrity Level SIL	479
22.6 Process Control Technique PLT.....	482
22.7 Performance Level PL	483
Literature.....	485
Index	517