

Josef Böresök

# **Funktionale Sicherheit**

**Grundzüge  
sicherheitstechnischer Systeme**

2., überarbeitete Auflage



# Inhaltsverzeichnis

<b>1 Einleitung</b> .....	23
<b>2 Historische Entwicklung von Sicherheitssystemen und Normen</b> .....	25
<b>3 Normen und Richtlinien</b> .....	29
3.1 Normengremien .....	29
3.2 Normen .....	33
3.2.1 DIN V 19250 .....	34
3.2.2 DIN V VDE 0801 .....	35
3.2.3 IEC 61508.....	38
3.2.4 IEC 61511.....	41
3.2.5 IEC 61131.....	44
3.2.6 ISA TR 84.0.02 .....	46
3.2.7 RTCA DO 178B .....	47
3.3 Definitionen rund um den Begriff der Sicherheit .....	49
3.4 Stand der Technik .....	55
3.4.1 Automobilbereich .....	55
3.4.2 Luftfahrt.....	56
3.4.3 Automatisierungstechnik .....	56
<b>4 Fehler, Fehlerursachen und Ausfälle</b> .....	59
4.1 Fehlerraten .....	59
4.2 Fehler-Ausfall-Abweichung .....	62
4.3 Fehlerquellen .....	64
4.4 Fehlertoleranz .....	65
4.5 Fehler gemeinsamer Ursache.....	65
<b>5 Kenngrößen der Risiko- und Zuverlässigkeitsanalyse</b> .....	67
5.1 Kenngrößen der Zuverlässigkeit .....	68
5.2 Ausfallwahrscheinlichkeit .....	70
5.3 Mittlere Lebensdauer .....	70
5.4 Mittlere Instandsetzungszeit .....	72
5.5 Mittlere Brauchbarkeitsdauer.....	72
5.6 Verfügbarkeit .....	73
5.7 Ausfallraten.....	73
5.8 SFF.....	75
5.9 DC.....	75
5.9.1 Tests.....	76
5.10 MTTF.....	77
5.10.1 MTTF – Spurious Trip Rate .....	77

5.11 PFD .....	78
<b>6 Maßnahmen zur Risikobestimmung</b> .....	<b>83</b>
6.1 Grundsätzliche Konzepte .....	83
6.2 Methoden der Gefahrenanalyse.....	84
6.2.1 Vorwärts- und Rückwärts-Suche .....	84
6.2.2 Top-Down und Bottom-Up Suche .....	85
6.3 Wahrscheinlichkeitsanalyse .....	86
6.3.1 Statistische Analyse .....	86
6.3.2 Fehlerausbreitungsmodell.....	87
<b>7 Risikomatrix</b> .....	<b>89</b>
<b>8 Risikograph</b> .....	<b>93</b>
8.1 Risikograph nach DIN V 19250.....	93
8.1.1 Zusammenhang zwischen Risiko, Grenzkrisiko, Restrisiko und Risikoreduzierung.....	94
8.1.2 Risikoparameter .....	95
8.1.3 Weitere Risikoparameter .....	98
8.1.4 Risikograph.....	98
8.1.5 Anforderungsklassen .....	100
8.2 Risikograph nach IEC 61508-5 und IEC 61511-3 .....	101
8.3 Risikograph nach DIN EN 954-1 .....	102
<b>9 Fehlerbaumanalyse</b> .....	<b>105</b>
9.1 Anwendungsbereich und Zweck der Fehlerbaumanalyse.....	105
9.2 Begriffe .....	106
9.3 Bildzeichen.....	107
9.4 Vorgehen bei der Analyse.....	109
9.4.1 Schritte der Analyse.....	109
9.4.2 Systemanalyse.....	110
9.4.3 Unerwünschtes Ereignis und Ausfallkriterien .....	111
9.4.4 Relevante Zuverlässigkeitskenngröße und Zeitintervall.....	111
9.4.5 Ausfallarten der Komponenten .....	111
9.4.6 Aufstellen des Fehlerbaumes .....	111
9.4.7 Auswerten des Fehlerbaums .....	115
9.5 Fehlerbaum-Analyse .....	122
<b>10 Ereignisbaumanalyse</b> .....	<b>125</b>
10.1 Bestandteile eines Ereignisbaumes .....	126
<b>11 LOPA</b> .....	<b>131</b>
11.1 Schutzebenen .....	132
11.2 LOPA-Bewertung .....	135
11.3 Typische Schutzebenen.....	136
11.3.1 Basis-Prozess-Kontroll-System .....	137
11.3.2 Physikalische Einrichtungen.....	138
11.3.3 Externe Anlagen zur Risikoreduzierung.....	139
11.4 Mehrere auslösende Ereignisse.....	140

<b>12 Zuverlässigkeitsblockanalyse</b> .....	141
12.1 Zuverlässigkeitsmodelle .....	147
12.1.1 Systeme ohne Redundanz .....	147
12.1.2 Systeme mit Redundanz .....	149
12.1.3 Gemischte Systeme.....	153
12.2 Redundante Systeme mit unterschiedlicher Ausfallrate.....	166
12.3 Ersatz von redundanten Systemkomponenten durch Einzelsystemkomponenten ...	171
<b>13 Markov-Modell</b> .....	173
13.1 Einleitung.....	173
13.2 Möglichkeiten des Markov-Modells.....	174
13.3 Theoretische Grundlagen der Markov-Modelle.....	175
13.4 Zeitabhängiges Markov-Modell.....	179
13.5 Durchführung einer Markov-Berechnung für ein sicherheitsgerichtetes System ....	180
13.5.1 Übergangsmatrix $P$ für System-Modell .....	183
<b>14 Lebenszyklusbetrachtung eines Sicherheitssystems</b> .....	189
14.1 Gefahr- und Risikoanalyse.....	189
14.2 Durchführung einer Risikobewertungsanalyse .....	189
14.3 Lebenszyklusphasen .....	191
14.3.1 Entwicklung einer sicherheitsgerichteten Funktion.....	192
14.3.2 Fehlermodelle und PFD Berechnung .....	193
14.3.3 Systemarchitektur .....	196
14.4 Gesamte Planung .....	200
14.5 Realisierung einer SIS .....	201
14.6 Installation, Inbetriebnahme und Validierung .....	203
14.7 Betrieb, Wartung und Reparatur.....	203
14.8 Verändern und Aufrüsten .....	204
14.9 Zusammenfassung .....	205
<b>15 Common Cause Failure</b> .....	207
15.1 Allgemeines .....	207
15.2 Ausfälle gemeinsamer Ursache.....	208
15.2.1 Analyse von Ausfällen mit gemeinsamer Ursache .....	209
15.3 Common Mode Ausfälle.....	213
15.4 Beispiele für den Ausfall durch gemeinsame Ursache .....	214
15.5 Techniken zur Bewertung von SIS Entwürfen für CCF .....	215
15.5.1 Industrielle Standards .....	215
15.5.2 Technische unternehmensspezifische Richtlinien und Standards.....	216
15.5.3 Qualitative Methoden zur Gefahrenidentifikation .....	216
15.5.4 Qualitative Bewertung.....	216
15.5.5 Checklisten .....	217
15.6 Quantitative Bewertung von Ausfällen mit gemeinsamer Ursache .....	218
15.6.1 Explizite Methoden.....	218
15.6.2 Implizite Methoden bei einer gemeinsamen Fehlerursache.....	226
15.6.2.1 Basic-Parameter-Modell .....	227
15.6.2.2 Beta-Faktor-Modell .....	227
15.6.2.3 Mehrfache Griechische Buchstaben Modell.....	228
15.6.2.4 $\alpha$ -Faktor Modell.....	228

15.6.2.5 Binomial-Ausfallraten Modell (BFR).....	229
15.7 Beta-Faktor.....	230
15.7.1 Auswirkungen des $\beta$ -Faktors auf die Sicherheit.....	232
15.7.2 Einschätzung des $\beta$ -Faktors .....	234
15.8 1oo2-System.....	236
15.8.1 Ausfallwahrscheinlichkeit bei Common Cause Fehlern .....	237
15.9 Maßnahmen gegen Ausfälle durch gemeinsame Ursache.....	238
<b>16 Proof-Test .....</b>	<b>241</b>
16.1 Überwachung und Durchführung von Proof-Tests .....	241
16.2 Arten von Proof-Tests .....	242
16.3 Zuverlässigkeitsfunktion und MTTF .....	243
16.3.1 Ausfallwahrscheinlichkeit .....	243
16.3.2 Probability of Failure on Demand.....	245
16.3.3 Proof-Test-Intervall $T_1$ .....	245
16.4 Definition des Proof-Tests nach IEC/EN 61508 .....	245
16.5 Auswirkungen eines nicht ausreichenden Proof-Tests.....	246
16.6 Unterschiede zwischen Diagnose-Test und Proof-Test .....	247
16.6.1 Definition von Diagnose- und Proof-Test .....	247
16.6.2 Performance-Indikatoren .....	248
16.6.3 Berechnungsergebnisse mit und ohne Diagnose.....	248
16.6.4 PFD-Berechnung mit variablen Proof-Test-Abdeckung.....	250
16.7 Einfluss des Proof-Test-Intervalls auf den PFD <sub>avg</sub> -Wert.....	251
16.8 Risikoreduzierung .....	253
16.8.1 Risikorate und durchschnittliche Ausfallwahrscheinlichkeit.....	254
16.8.2 Proof-Test-Häufigkeit .....	256
16.8.3 Proof-Test Erweiterungsfaktor .....	257
<b>17 Hardware sicherheitsgerichteter Systeme .....</b>	<b>259</b>
17.1 Normative Architekturvorschriften .....	259
17.1.1 Qualitätssicherheit für Nutzer sicherheitskritischen Systeme .....	259
17.1.2 Realisierungssicherheit für Hersteller sicherheitskritischer Systeme .....	260
17.2 Hardware-Sicherheitslebenszyklus .....	261
17.2.1 Spezifikation der Sicherheitsanforderungen .....	261
17.2.2 Planung der Sicherheitsvalidation.....	263
17.2.3 Entwurf und Entwicklung des E/E/PES.....	263
17.3 Hardware Fehlertoleranz.....	264
17.4 Constraints .....	265
17.4.1 Architectural constraints .....	265
17.4.2 Allgemeine Konzepte zur Risikoreduzierung .....	266
17.5 1oo1-System.....	268
17.5.1 PFD-Fehlerbaum der 1oo1-Architektur .....	269
17.5.2 Markov-Modell für die 1oo1-Architektur .....	271
17.5.3 Berechnung des MTTF-Wertes einer 1oo1-Architektur .....	272
17.6 Weitere Architekturen.....	275
<b>18 Softwareanforderungen an ein System mit funktionaler Sicherheit .....</b>	<b>293</b>
18.1 Software in Systemen mit funktionaler Sicherheit.....	293
18.1.1 Anforderungen an die Software .....	297

18.1.2 Nicht-funktionale Anforderungen .....	297
18.1.2.1 Zielsetzung .....	298
18.1.2.2 Zielkontrolle .....	299
18.1.3 Kategorien von nicht-funktionalen Anforderungen .....	299
18.2 Softwareentwicklung .....	301
18.2.1 Modelle der Software-Entwicklung .....	303
18.2.1.1 Wasserfallmodell .....	303
18.2.1.2 Spiralmodell .....	304
18.2.1.3 V-Modell .....	305
18.2.1.4 Projektplanung .....	306
18.2.2 Anforderungsspezifikation .....	306
18.2.2.1 Merkmale einer Spezifikation .....	307
18.2.2.2 Darstellung von Anforderungen .....	308
18.2.2.3 Formalität der Anforderungen .....	310
18.2.2.4 Pflichtenheft .....	310
18.2.3 Software-Architektur .....	310
18.2.3.1 Aufteilung in Komponenten .....	311
18.2.3.2 Schnittstellen .....	312
18.2.3.3 Kommunikation innerhalb des Systems .....	312
18.2.3.4 Testbarkeit von Komponenten .....	313
18.2.3.5 Zusätzliche Qualitätsmerkmale .....	313
18.2.3.6 Ressourcen .....	313
18.2.3.7 Qualität der Lösung .....	314
18.2.4 Mögliche Architekturstile .....	314
18.2.4.1 Funktionsorientierung .....	314
18.2.4.2 Objektorientierung .....	315
18.2.5 Wiederverwendbare Architekturstrukturen .....	316
18.2.5.1 Entwurfsmuster .....	316
18.2.5.2 Rahmen .....	317
18.2.5.3 Architekturmuster .....	317
18.2.6 Programmierkonventionen .....	317
18.2.6.1 Dokumentation und Aussehen des Quelltextes .....	317
18.2.6.2 Namenskonventionen .....	318
18.2.7 Softwareentwicklung mit UML .....	319
18.2.7.1 Objektorientierte Analyse .....	319
18.2.8 Objektorientiertes Design .....	321
18.2.8.1 Architektur .....	321
18.2.8.2 Ablaufstrukturen zuordnen .....	322
18.2.8.3 Design-Klassen entwickeln .....	322
18.2.8.4 Komponentenschnittstellen beschreiben .....	323
18.2.8.5 Zustandsmodelle spezialisieren .....	323
18.2.8.6 Objektfluss der Aktivitätsmodelle .....	323
18.2.8.7 Interaktionsmodelle modellieren .....	323
18.2.8.8 Tests entwickeln .....	323
18.2.8.9 Attribute festlegen .....	324
18.2.9 Verwendung von CASE-Tools .....	324
18.2.9.1 Roundtrip-Engineering mit CASE-Tools .....	325

18.2.9.2 MDA (Model Driven Architecture).....	325
18.2.9.3 Vergleich von UML-CASE-Tools.....	326
18.2.10 Softwarequalität.....	326
18.2.10.1 Qualitätsplan.....	328
18.2.11 Software-Zuverlässigkeit.....	329
18.2.11.1 Zuverlässigkeitskenngrößen.....	330
18.2.11.2 Unterschiede zwischen Hardware- und Softwarezuverlässigkeit.....	331
18.2.11.3 Erhöhung der Zuverlässigkeit durch Verifikation und Validierung....	333
18.2.11.4 Validierung der Zuverlässigkeit.....	335
18.2.11.5 Nachweis der Zuverlässigkeit.....	336
18.2.12 Messen von Software-Qualität.....	336
18.2.12.1 Lines of Code (LoC).....	338
18.2.12.2 McCabe-Maß.....	338
18.2.12.3 Maße von Halstead.....	339
18.2.12.4 Nutzen von Maßen.....	340
18.2.13 Fehler in Software-Systemen.....	340
18.2.13.1 Fehlertoleranz und Fehlervermeidung.....	342
18.2.14 Testverfahren.....	343
18.2.14.1 Testablauf.....	343
18.2.14.2 Black-Box-Testmethoden.....	344
18.2.14.3 White-Box-Testmethoden.....	345
18.2.14.4 Intuitive Testfallermittlung.....	346
18.2.15 Testen in der Praxis.....	346
18.2.16 Integration.....	347
18.2.16.1 Top-Down-Integration.....	347
18.2.16.2 Bottom-Up-Integration.....	348
18.2.16.3 Outside-In-Integration.....	348
18.2.17 System- und Abnahmetest.....	348
<b>19 Anwendungsbeispiele.....</b>	<b>351</b>
19.1 Praktische Implementierung des IEC 61508 Sicherheitsstandards.....	351
19.1.1 IEC 61508 Norm.....	352
19.1.1.1 Funktionales Sicherheitsmanagement.....	354
19.1.1.2 Pipe to Pipe Ansatz.....	356
19.1.1.3 Quantitative Sicherheitseinschätzung.....	357
19.2 Bestimmung des SIL eines Prozessorsystems.....	357
19.2.1 SIL-Anforderung.....	358
19.2.2 Bestimmung des SIL einer Prozessor-Einheit mit Prozessor-Peripherie..	359
19.2.3 DC-Maßnahmen für eine Prozessor-Einheit mit Prozessor-Peripherie....	360
19.2.3.1 Prozessor-Einheiten.....	360
19.2.3.2 Festspeicher.....	361
19.2.3.3 Veränderlicher Speicher.....	361
19.3 Bestimmung des SIL einer Sicherheitsfunktion.....	364
19.3.1 Bestimmung des SIL einer Sicherheitsfunktion.....	365
19.3.2 Modifikation der Architektur der Sicherheitsfunktion.....	366
19.3.3 Bestimmung des SIL der modifizierten Sicherheitsfunktion.....	368
19.3.4 Modifikation der Sicherheitsfunktion.....	370
19.3.5 Bestimmung des SIL der Sicherheitsfunktion mit Diagnose.....	371

19.4 Bestimmung des SIL eines Sicherheitsloops .....	373
19.4.1 Bestimmung des SIL des Sicherheitsloops .....	375
19.5 Beispiele zu Zuverlässigkeitsanalysen .....	378
19.5.1 Beispiel 1 (Chemische Anlage) .....	378
19.5.1.1 Risikograph .....	379
19.5.1.2 Ereignisbaum .....	380
19.5.1.3 Fehlerbaumanalyse .....	381
19.5.1.4 Zuverlässigkeitsblockdiagramm .....	382
19.5.2. Beispiel 2 (Fahrer-Airbag) .....	383
19.5.2.1 Risikograph .....	384
19.5.2.2 Ereignisbaum .....	385
19.5.2.3 Fehlerbaumanalyse .....	386
19.5.2.4 Zuverlässigkeitsblockdiagramm .....	386
19.5.3 Beispiel 3 (Flugzeug) .....	387
19.5.3.1 Risikograph .....	388
19.5.3.2 Ereignisbaum .....	390
19.5.3.3 Fehlerbaumanalyse .....	390
19.5.4 Beispiel 4 (Pipeline) .....	392
19.5.4.1 Risikograph .....	393
19.5.4.2 Ereignisbaum .....	394
19.5.4.3 Fehlerbaumanalyse .....	394
19.5.5 Beispiel 5 (Sporthalle) .....	395
19.5.5.1 Risikograph .....	397
19.5.5.2 Ereignisbaum .....	397
19.5.5.3 Fehlerbaumanalyse .....	398
<b>20 IEC/EN 61508</b> .....	<b>401</b>
20.1 IEC/EN 61508-1 .....	402
20.1.1 Übersicht und Anwendungsbereich .....	402
20.1.2 Übereinstimmung mit dieser Norm .....	404
20.1.3 Dokumentation .....	404
20.1.4 Sicherheitsmanagement .....	404
20.1.5 Sicherheitslebenszyklus .....	406
20.1.6 Verifikation .....	408
20.1.7 Beurteilung der funktionalen Sicherheit .....	408
20.2 IEC/EN 61508-2 .....	409
20.2.1 Anwendungsbereich .....	409
20.2.2 E/E/PES-Sicherheits-Lebenszyklus .....	409
20.2.3 Techniken und Maßnahmen zur Beherrschung von Ausfällen während des Betriebs .....	411
20.2.4 Methoden zur Vermeidung von systematischen Fehlern während der verschiedenen Phasen des Lebenszyklusses .....	411
20.3 IEC/EN 61508-3 .....	411
20.3.1 Anwendungsbereich .....	411
20.3.2 Qualitätsmanagementsystem der Software .....	412
20.3.3 Software- Sicherheitslebenszyklus .....	412
20.3.4 Beurteilung der funktionalen Sicherheit .....	413
20.3.5 Anhang A Richtlinien zur Auswahl von Techniken und Maßnahmen .....	413

20.4 IEC/EN 61508-4 .....	414
20.4.1 Begriffe zu Sicherheit .....	414
20.4.2 Begriffe zu Einrichtungen und Geräten .....	414
20.4.3 Begriffe zu Systemen .....	414
20.4.5 Begriffe zu Sicherheitsfunktionen und Sicherheits-Integrität .....	416
20.4.6 Begriffe zu Fehler, Ausfall und Abweichung .....	417
20.4.7 Begriffe zu Lebenszyklus .....	418
20.4.8 Begriffe zu Bestätigung von Sicherheitsmaßnahmen .....	418
20.5 IEC/EN 61508-5 .....	419
20.5.1 Anwendungsbereich .....	419
20.5.2 Anhang A – Grundlegende Konzepte .....	419
20.5.3 Anhang B – ALARP und das Konzept des tolerierbaren Risikos .....	419
20.5.4 Anhang C – quantitative Methode zur Bestimmung der Sicherheits- Integritätslevel .....	421
20.5.5 Anhang D – qualitative Methode zur Bestimmung der Sicherheits- Integritätslevel (Risiko-Graph) .....	422
20.5.6 Anhang E – Festlegung der Sicherheits- Integritätslevel Eine qualitative Vorgehensweise – Matrix des Ausmaßes des gefährlichen Vorfalls .....	422
20.6 IEC/EN 61508-6 .....	423
20.6.1 Anwendungsbereich .....	423
20.6.2 Anhang A – Anwendung von IEC/EN 61508-2 und –3 .....	424
20.6.3 Anhang B – Beispielhafte Vorgehensweise zur Bestimmung von Hardware- Ausfällen .....	424
20.6.4 Anhang D – Methodik zur Quantifizierung der Auswirkungen von Hardware-Ausfällen mit gemeinsamer Ursache in E/E/PES .....	429
20.7 IEC/EN 61508-7 .....	429
20.7.1 Anwendungsbereich .....	429
20.7.2 Anhang A – Überblick über Verfahren und Maßnahmen für E/E/PES: Beherrschung von zufälligen Hardwareausfällen .....	429
20.7.3 Anhang B – Übersicht über Techniken und Maßnahmen zur Vermeidung systematischer Ausfälle .....	431
20.7.4 Anhang C – Übersicht über Techniken und Maßnahmen, um die Sicherheits-Integrität der Software zu erreichen .....	432
<b>21 IEC 61511</b> .....	435
21.1 Anwendungsbereich .....	435
21.2 Aufteilung der Norm 61511 .....	437
21.3 Begriffe und Abkürzungen .....	440
21.3.1 Abkürzungen .....	440
21.3.2 Begriffe .....	441
21.4 Management der funktionalen Sicherheit .....	453
21.4.1 Ziel .....	453
21.4.2 Anforderungen .....	453
21.4.3 Beurteilung, Auditierung und Revisionen .....	454
21.4.4 Management der SIS-Konfiguration .....	454
21.5 Anforderungen an den Sicherheitslebenszyklus .....	454
21.6 Verifikation .....	458
21.6.1 Ziel .....	458

21.6.2 Anforderungen.....	458
21.7 Gefährdungsanalyse und Risikobewertung.....	458
21.7.1 Ziel.....	458
21.7.2 Anforderungen.....	458
21.8 Zuordnung von Sicherheitsfunktionen zu Schutzebenen.....	458
21.8.1 Ziel.....	458
21.8.2 Anforderungen für die Zuordnung .....	459
21.8.3 Anforderungen für Sicherheits-Integritätslevel 4 .....	459
21.8.4 Anforderungen an Betriebseinrichtungen, die als Schutzebene eingesetzt werden .....	459
21.8.5 Anforderungen zur Vermeidung von Ausfällen .....	460
21.9 Sicherheitsspezifikation des SIS .....	461
21.9.1 Ziel.....	461
21.9.2 Sicherheitsanforderungen an das SIS .....	461
21.10 SIS-Entwurf und Planung .....	461
21.10.1 Ziel.....	461
21.10.2 Allgemeine Anforderungen .....	461
21.10.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers ..	462
21.10.4 Anforderungen an die Fehlertoleranz der Hardware .....	462
21.10.5 Anforderungen an die Auswahl von Komponenten und Teilsystemen ..	463
21.10.6 Feldgeräte .....	463
21.10.7 Schnittstellen .....	463
21.10.8 Anforderungen an Instandhaltungs- oder Prüfeinrichtungen .....	464
21.10.9 Ausfallwahrscheinlichkeit sicherheitstechnischer Funktionen .....	464
21.11 Anforderungen an Anwendungssoftware .....	465
21.11.1 Anforderungen an den Sicherheitslebenszyklus der Anwendungssoftware .....	465
21.11.2 Spezifikation der Sicherheitsanforderungen an die Anwendungssoftware .....	470
21.11.3 Validierungsplanung für die Sicherheit der Anwendungssoftware .....	470
21.11.4 Entwurf und Erstellung der Anwendungssoftware.....	471
21.11.5 Integration der Anwendungssoftware in das SIS-Teilsystem.....	472
21.11.6 Vorgehen bei Modifikation der Anwendungssoftware.....	472
21.11.7 Verifikation der Anwendungssoftware.....	472
21.12 Werksendprüfungen.....	473
21.12.1 Ziele .....	473
21.12.2 Empfehlungen.....	473
21.13 SIS-Montage und Inbetriebnahme .....	473
21.14 SIS-Sicherheits-Validierung .....	474
21.15 Betrieb und Instandhaltung des SIS .....	474
21.15.1 Ziele .....	474
21.15.2 Anforderungen.....	474
21.15.3 Wiederholungsprüfung und Inspektion .....	475
21.16 Modifikationen am SIS .....	475
21.16.1 Ziele .....	475
21.16.2 Anforderungen.....	475
21.17 Außerbetriebnahme des SIS.....	476

21.18 Anforderungen an die Dokumentation.....	476
21.18.1 Ziel.....	476
21.18.2 Anforderungen.....	476
<b>22 Begriffe und Definitionen .....</b>	<b>477</b>
22.1 Sicherheitssysteme .....	477
22.1.1 Risiko.....	477
22.1.2 Teilrisiko.....	477
22.1.3 Grenzzisiko .....	477
22.1.4 Risikoparameter.....	477
22.1.5 Anforderungsklasse .....	478
22.1.6 Maßnahmen .....	478
22.1.7 Schutz .....	478
22.1.8 MSR-Schutzmaßnahmen .....	478
22.1.9 MSR-Schutzeinrichtung.....	478
22.1.10 Unerwünschtes Ereignis .....	478
22.1.11 Fehler .....	478
22.1.12 Redundanz .....	479
22.1.13 Diversitäre Redundanz.....	479
22.1.14 Fail-safe .....	479
22.2. Verlässlichkeit (Dependability) .....	479
22.2.1 Zuverlässigkeit.....	480
22.2.2 Verfügbarkeit.....	482
22.2.3 Sicherheit .....	482
22.2.4 Wartbarkeit.....	483
22.3 Darstellung des Ausfallverhaltens.....	483
22.3.1 Dichtefunktion bzw. Ausfalldichte $f(t)$ .....	483
22.3.2 Ausfallwahrscheinlichkeit bzw. Verteilungsfunktion $F(t)$ .....	487
22.3.3 Zuverlässigkeit bzw. Überlebenswahrscheinlichkeit $R(t)$ .....	490
22.3.4 Ausfallrate $\lambda(t)$ .....	492
22.3.5 Beschreibung des Ausfallsverhalten durch Beispiele .....	496
22.3.6 Boolsche Theorie .....	499
22.4 Zeit-Faktor .....	501
22.4.1 MTTF.....	502
22.4.2 MTTF <sub>spurious</sub> .....	502
22.4.3 MTBF .....	502
22.4.4 MTTR .....	502
22.4.5 Beispiel zur Berechnung von MTTF .....	502
22.4.6 Dauerverfügbarkeit.....	503
22.4.7 Downtime DT .....	505
22.4.8 Uptime UT .....	506
22.4.9 Mean Down Time MDT .....	506
22.5 Allgemeines zu den Begrifflichkeiten und Normen.....	506
22.5.1 Diagnoseabdeckungsgrad DC.....	508
22.5.2 Common Cause Failure CCF .....	509
22.5.3 Probability of Failure on Demand PFD .....	510
22.5.4 Ausfallraten.....	511
22.5.5 Risiko, Schaden und Gefahr .....	514

---

22.5.6 Hazard Rate .....	515
22.5.7 Safety Integrity Level SIL .....	516
22.6 Prozessleittechnik PLT .....	520
22.7 Performance Level PL .....	520
<b>Literaturverzeichnis .....</b>	<b>521</b>
<b>Stichwortverzeichnis.....</b>	<b>553</b>