

Inhaltsverzeichnis

1 Einleitung.....	25
2 Historische Entwicklung von Sicherheitssystemen und Normen	27
3 Normen und Richtlinien.....	31
3.1 Normengremien	31
3.2 Normen	35
3.2.1 DIN V 19250.....	36
3.2.2 DIN V VDE 0801.....	37
3.2.3 IEC 61508	40
3.2.4 IEC 61511	43
3.2.5 IEC 61131	46
3.2.6 ISA TR 84.0.02	48
3.2.7 RTCA DO 178B.....	49
3.3 Definitionen rund um den Begriff der Sicherheit	52
3.4 Stand der Technik	57
3.4.1 Automobilbereich.....	57
3.4.2 Luftfahrt	58
3.4.3 Automatisierungstechnik.....	58
4 Fehler, Fehlerursachen und Ausfälle	61
4.1 Fehlerraten	61
4.2 Fehler-Ausfall-Abweichung	64
4.3 Fehlerquellen	66
4.4 Fehlertoleranz	67
4.5 Fehler gemeinsamer Ursache	67
5 Kenngrößen der Risiko- und Zuverlässigkeitssanalyse	69
5.1 Kenngrößen der Zuverlässigkeit.....	70
5.2 Ausfallwahrscheinlichkeit	72
5.3 Mittlere Lebensdauer	72
5.4 Mittlere Instandsetzungszeit	74
5.5 Mittlere Brauchbarkeitsdauer.....	74
5.6 Verfügbarkeit.....	75
5.7 Ausfallraten.....	75
5.8 SFF	77
5.9 DC	77
5.9.1 Tests	78
5.10 MTTF	79
5.10.1 MTTF – Spurious Trip Rate	80

5.11 PFD	80
6 Maßnahmen zur Risikobestimmung	85
6.1 Grundsätzliche Konzepte	85
6.2 Methoden der Gefahrenanalyse.....	86
6.2.1 Vorwärts- und Rückwärts-Suche.....	86
6.2.2 Top-down- und Bottom-up-Suche.....	87
6.3 Wahrscheinlichkeitsanalyse	88
6.3.1 Statistische Analyse	88
6.3.2 Fehlerausbreitungsmodell.....	89
7 Risikomatrix	91
8 Risikograph	95
8.1 Risikograph nach DIN V 19250.....	95
8.1.1 Zusammenhang zwischen Risiko, Grenzrisiko, Restrisiko und Risikoreduzierung	96
8.1.2 Risikoparameter	97
8.1.3 Weitere Risikoparameter	100
8.1.4 Risikograph.....	100
8.1.5 Anforderungsklassen	102
8.2 Risikograph nach IEC 61508-5 und IEC 61511-3	103
8.3 Risikograph nach DIN EN 954-1	104
9 Fehlerbaumanalyse	107
9.1 Anwendungsbereich und Zweck der Fehlerbaumanalyse.....	107
9.2 Begriffe	108
9.3 Bildzeichen.....	109
9.4 Vorgehen bei der Analyse.....	111
9.4.1 Schritte der Analyse.....	111
9.4.2 Systemanalyse.....	112
9.4.3 Unerwünschtes Ereignis und Ausfallkriterien	113
9.4.4 Relevante Zuverlässigkeitsskenngröße und Zeitintervall.....	113
9.4.5 Ausfallarten der Komponenten.....	113
9.4.6 Aufstellen des Fehlerbaums.....	113
9.4.7 Auswerten des Fehlerbaums	117
9.5 Fehlerbaum-Analyse	124
10 Ereignisbaumanalyse	127
10.1 Bestandteile eines Ereignisbaums	128
11 LOPA	133
11.1 Schutzebenen	134
11.2 LOPA-Bewertung	137
11.3 Typische Schutzebenen	138
11.3.1 Basis-Prozess-Kontroll-System	139
11.3.2 Physikalische Einrichtungen.....	140
11.3.3 Externe Anlagen zur Risikoreduzierung.....	141
11.4 Mehrere auslösende Ereignisse	142

12 Zuverlässigkeitssblockanalyse.....	143
12.1 Zuverlässigkeitsmodelle	149
12.1.1 Systeme ohne Redundanz.....	149
12.1.2 Systeme mit Redundanz	151
12.1.3 Gemischte Systeme	156
12.2 Redundante Systeme mit unterschiedlicher Ausfallrate.....	168
12.3 Ersatz von redundanten Systemkomponenten durch Einzelsystemkomponenten	173
13 Markov-Modell	175
13.1 Einleitung.....	175
13.2 Möglichkeiten des Markov-Modells	176
13.3 Theoretische Grundlagen der Markov-Modelle.....	176
13.4 Zeitabhängiges Markov-Modell.....	181
13.5 Durchführung einer Markov-Berechnung für ein sicherheitsgerichtetes System	182
13.5.1 Übergangsmatrix P für System-Modell.....	184
14 Lebenszyklusbetrachtung eines Sicherheitssystems	191
14.1 Gefahr- und Risikoanalyse.....	191
14.2 Durchführung einer Risikobewertungsanalyse	191
14.3 Lebenszyklusphasen	193
14.3.1 Entwicklung einer sicherheitsgerichteten Funktion	194
14.3.2 Fehlermodelle und PFD-Berechnung.....	195
14.3.3 Systemarchitektur	198
14.4 Gesamte Planung	202
14.5 Realisierung einer SIS	203
14.6 Installation, Inbetriebnahme und Validierung	205
14.7 Betrieb, Wartung und Reparatur	205
14.8 Verändern und Aufrüsten	206
14.9 Zusammenfassung	207
15 Common Cause Failure.....	209
15.1 Allgemeines	209
15.2 Ausfälle gemeinsamer Ursache.....	210
15.2.1 Analyse von Ausfällen mit gemeinsamer Ursache	211
15.3 Common-Mode-Ausfälle	215
15.4 Beispiele für den Ausfall durch gemeinsame Ursache	216
15.5 Techniken zur Bewertung von SIS-Entwürfen für CCF	217
15.5.1 Industrielle Standards	217
15.5.2 Technische unternehmensspezifische Richtlinien und Standards	217
15.5.3 Qualitative Methoden zur Gefahrenidentifikation.....	218
15.5.4 Qualitative Bewertung.....	218
15.5.5 Checklisten	219
15.6 Quantitative Bewertung von Ausfällen mit gemeinsamer Ursache	219
15.6.1 Explizite Methoden	220
15.6.2 Implizite Methoden bei einer gemeinsamen Fehlerursache	227
15.6.2.1 Basic-Parameter-Modell.....	228
15.6.2.2 Beta-Faktor-Modell	228
15.6.2.3 Mehrfache-griechische-Buchstaben-Modell	229

15.6.2.4 α -Faktor-Modell	229
15.6.2.5 Binomial-Ausfallraten-Modell (BFR)	230
15.7 Beta-Faktor.....	231
15.7.1 Auswirkungen des β -Faktors auf die Sicherheit.....	233
15.7.2 Einschätzung des β -Faktors.....	235
15.8 1oo2-System.....	237
15.8.1 Ausfallwahrscheinlichkeit bei Common-Cause-Fehlern	238
15.9 Maßnahmen gegen Ausfälle durch gemeinsame Ursache.....	240
16 Proof-Test	241
16.1 Überwachung und Durchführung von Proof-Tests.....	241
16.2 Arten von Proof-Tests	242
16.3 Zuverlässigkeitfunktion und MTTF	243
16.3.1 Ausfallwahrscheinlichkeit	244
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	249
16.6.4 PFD-Berechnung mit variabler Proof-Test-Abdeckung.....	250
16.7 Einfluss des Proof-Test-Intervalls auf den PFD _{avg} -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
17 Hardware sicherheitsgerichteter Systeme	261
17.1 Normative Architekturvorschriften	261
17.1.1 Qualitätssicherheit für Nutzer sicherheitskritischer Systeme	261
17.1.2 Realisierungssicherheit für Hersteller sicherheitskritischer Systeme	262
17.2 Hardware-Sicherheitslebenszyklus	263
17.2.1 Spezifikation der Sicherheitsanforderungen	263
17.2.2 Planung der Sicherheitsvalidation	265
17.2.3 Entwurf und Entwicklung des E/E/PES	265
17.3 Hardware-Fehlertoleranz	265
17.4 Constraints	267
17.4.1 Architectural Constraints	267
17.4.2 Allgemeine Konzepte zur Risikoreduzierung	268
17.5 1oo1-System.....	270
17.5.1 PFD-Fehlerbaum der 1oo1-Architektur.....	271
17.5.2 Markov-Modell für die 1oo1-Architektur	273
17.5.3 Berechnung des MTTF-Werts einer 1oo1-Architektur	274
17.6 Weitere Architekturen	276

18 Softwareanforderungen an ein System mit funktionaler Sicherheit.....	295
18.1 Software in Systemen mit funktionaler Sicherheit.....	295
18.1.1 Anforderungen an die Software	299
18.1.2 Nichtfunktionale Anforderungen	299
18.1.2.1 Zielsetzung	300
18.1.2.2 Zielkontrolle	300
18.1.3 Kategorien von nichtfunktionalen Anforderungen.....	301
18.2 Software-Entwicklung	302
18.2.1 Modelle der Software-Entwicklung	304
18.2.1.1 Wasserfallmodell.....	305
18.2.1.2 Spiralmodell	306
18.2.1.3 V-Modell	307
18.2.1.4 Projektplanung	307
18.2.2 Anforderungsspezifikation	308
18.2.2.1 Merkmale einer Spezifikation	309
18.2.2.2 Darstellung von Anforderungen.....	310
18.2.2.3 Formalität der Anforderungen.....	311
18.2.2.4 Pflichtenheft	311
18.2.3 Software-Architektur.....	311
18.2.3.1 Aufteilung in Komponenten	312
18.2.3.2 Schnittstellen	313
18.2.3.3 Kommunikation innerhalb des Systems	313
18.2.3.4 Testbarkeit von Komponenten	313
18.2.3.5 Zusätzliche Qualitätsmerkmale	314
18.2.3.6 Ressourcen	314
18.2.3.7 Qualität der Lösung	315
18.2.4 Mögliche Architekturstile.....	315
18.2.4.1 Funktionsorientierung	315
18.2.4.2 Objektorientierung	316
18.2.5 Wiederverwendbare Architekturstrukturen.....	317
18.2.5.1 Entwurfsmuster	317
18.2.5.2 Rahmen.....	317
18.2.5.3 Architekturmuster.....	318
18.2.6 Programmierkonventionen	318
18.2.6.1 Dokumentation und Aussehen des Quelltextes	318
18.2.6.2 Namenskonventionen	319
18.2.7 Software-Entwicklung mit UML.....	320
18.2.7.1 Objektorientierte Analyse.....	320
18.2.8 Objektorientiertes Design.....	322
18.2.8.1 Architektur	322
18.2.8.2 Ablaufstrukturen zuordnen.....	323
18.2.8.3 Design-Klassen entwickeln	323
18.2.8.4 Komponentenschnittstellen beschreiben	323
18.2.8.5 Zustandsmodelle spezialisieren.....	324
18.2.8.6 Objektfluss der Aktivitätsmodelle	324
18.2.8.7 Interaktionsmodelle modellieren	324
18.2.8.8 Tests entwickeln	324

18.2.8.9 Attribute festlegen	325
18.2.9 Verwendung von CASE-Tools	325
18.2.9.1 Roundtrip-Engineering mit CASE-Tools	325
18.2.9.2 MDA (Model Driven Architecture)	326
18.2.9.3 Vergleich von UML-CASE-Tools	327
18.2.10 Softwarequalität	327
18.2.10.1 Qualitätsplan	329
18.2.11 Software-Zuverlässigkeit	331
18.2.11.1 Zuverlässigkeitskenngrößen	332
18.2.11.2 Unterschiede zwischen Hardware- und Softwarezuverlässigkeit	333
18.2.11.3 Erhöhung der Zuverlässigkeit durch Verifikation und Validierung	335
18.2.11.4 Validierung der Zuverlässigkeit	336
18.2.11.5 Nachweis der Zuverlässigkeit	337
18.2.12 Messen von Software-Qualität	338
18.2.12.1 Lines of Code (LoC)	339
18.2.12.2 McCabe-Maß	340
18.2.12.3 Maße von Halstead	340
18.2.12.4 Nutzen von Maßen	341
18.2.13 Fehler in Software-Systemen	341
18.2.13.1 Fehlertoleranz und Fehlervermeidung	343
18.2.14 Testverfahren	344
18.2.14.1 Testablauf	344
18.2.14.2 Black-Box-Testmethoden	345
18.2.14.3 White-Box-Testmethoden	346
18.2.14.4 Intuitive Testfallermittlung	347
18.2.15 Testen in der Praxis	347
18.2.16 Integration	347
18.2.16.1 Top-down-Integration	349
18.2.16.2 Bottom-up-Integration	348
18.2.16.3 Outside-in-Integration	349
18.2.17 System- und Abnahmetest	349
19 Anwendungsbeispiele	351
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	363
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.....	369
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 Zuverlässigkeitssanalysen.....	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 Zuverlässigkeitssblockdiagramm.....	382
19.5.2. Beispiel 2 (Fahrer-Airbag)	383
19.5.2.1 Risikograph	384
19.5.2.2 Ereignisbaum.....	386
19.5.2.3 Fehlerbaumanalyse	386
19.5.2.4 Zuverlässigkeitssblockdiagramm.....	387
19.5.3 Beispiel 3 (Flugzeug)	388
19.5.3.1 Risikograph	389
19.5.3.2 Ereignisbaum.....	391
19.5.3.3 Fehlerbaumanalyse	392
19.5.4 Beispiel 4 (Pipeline)	394
19.5.4.1 Risikograph	395
19.5.4.2 Ereignisbaum.....	396
19.5.4.3 Fehlerbaumanalyse	397
19.5.5 Beispiel 5 (Sporthalle).....	398
19.5.5.1 Risikograph	399
19.5.5.2 Ereignisbaum.....	400
19.5.5.3 Fehlerbaumanalyse	401
20 IEC/EN 61508.....	403
20.1 IEC/EN 61508-1	404
20.1.1 Übersicht und Anwendungsbereich.....	404
20.1.2 Übereinstimmung mit dieser Norm	407
20.1.3 Dokumentation	407
20.1.4 Sicherheitsmanagement	407
20.1.5 Sicherheitslebenszyklus	407
20.1.6 Verifikation	410
20.1.7 Beurteilung der funktionalen Sicherheit.....	410
20.2 IEC/EN 61508-2	410
20.2.1 Anwendungsbereich	410
20.2.2 E/E/PES-Sicherheits-Lebenszyklus.....	411
20.2.3 Techniken und Maßnahmen zur Beherrschung von Ausfällen während des Betriebs	413
20.2.4 Methoden zur Vermeidung von systematischen Fehlern während der verschiedenen Phasen des Lebenszyklus	413
20.3 IEC/EN 61508-3	413
20.3.1 Anwendungsbereich	413
20.3.2 Qualitätsmanagementsystem der Software.....	413

20.3.3 Software-Sicherheitslebenszyklus	413
20.3.4 Beurteilung der funktionalen Sicherheit.....	415
20.3.5 Anhang A Richtlinien zur Auswahl von Techniken und Maßnahmen.....	415
20.4 IEC/EN 61508-4	415
20.4.1 Begriffe zu Sicherheit.....	415
20.4.2 Begriffe zu Einrichtungen und Geräten.....	416
20.4.3 Begriffe zu Systemen.....	416
20.4.5 Begriffe zu Sicherheitsfunktionen und Sicherheits-Integrität.....	418
20.4.6 Begriffe zu Fehler, Ausfall und Abweichung.....	419
20.4.7 Begriffe zu Lebenszyklus	419
20.4.8 Begriffe zu Bestätigung von Sicherheitsmaßnahmen	420
20.5 IEC/EN 61508-5	420
20.5.1 Anwendungsbereich	420
20.5.2 Anhang A – Grundlegende Konzepte.....	421
20.5.3 Anhang B – ALARP und das Konzept des tolerierbaren Risikos	422
20.5.4 Anhang C – Quantitative Methode zur Bestimmung der Sicherheits-Integritätslevel	423
20.5.5 Anhang D – Qualitative Methode zur Bestimmung der Sicherheits-Integritätslevel (Risiko-Graph).....	424
20.5.6 Anhang E – Festlegung der Sicherheits-Integritätslevel: Eine qualitative Vorgehensweise – Matrix des Ausmaßes des gefährlichen Vorfalls.....	424
20.6 IEC/EN 61508-6	425
20.6.1 Anwendungsbereich	425
20.6.2 Anhang A – Anwendung von IEC/EN 61508-2 und -3.....	426
20.6.3 Anhang B – Beispielhafte Vorgehensweise zur Bestimmung von Hardware-Ausfällen	426
20.6.4 Anhang D – Methodik zur Quantifizierung der Auswirkungen von Hardware-Ausfällen mit gemeinsamer Ursache in E/E/PES	431
20.7 IEC/EN 61508-7	431
20.7.1 Anwendungsbereich	431
20.7.2 Anhang A – Überblick über Verfahren und Maßnahmen für E/E/PES: Beherrschung von zufälligen Hardwareausfällen.....	431
20.7.3 Anhang B – Übersicht über Techniken und Maßnahmen zur Vermeidung systematischer Ausfälle	433
20.7.4 Anhang C – Übersicht über Techniken und Maßnahmen, um die Sicherheits-Integrität der Software zu erreichen	434
21 IEC 61511	437
21.1 Anwendungsbereich.....	437
21.2 Aufteilung der Norm 61511	439
21.3 Begriffe und Abkürzungen.....	442
21.3.1 Abkürzungen	442
21.3.2 Begriffe.....	443
21.4 Management der funktionalen Sicherheit	455
21.4.1 Ziel	455
21.4.2 Anforderungen.....	455
21.4.3 Beurteilung, Auditierung und Revisionen	455
21.4.4 Management der SIS-Konfiguration.....	456

21.5 Anforderungen an den Sicherheitslebenszyklus	456
21.6 Verifikation.....	460
21.6.1 Ziel	460
21.6.2 Anforderungen	460
21.7 Gefährdungsanalyse und Risikobewertung.....	460
21.7.1 Ziel	460
21.7.2 Anforderungen	460
21.8 Zuordnung von Sicherheitsfunktionen zu Schutzebenen.....	461
21.8.1 Ziel	461
21.8.2 Anforderungen für die Zuordnung	461
21.8.3 Anforderungen für Sicherheits-Integritätslevel 4	461
21.8.4 Anforderungen an Betriebseinrichtungen, die als Schutzebene eingesetzt werden.....	462
21.8.5 Anforderungen zur Vermeidung von Ausfällen.....	463
21.9 Sicherheitsspezifikation des SIS	463
21.9.1 Ziel	463
21.9.2 Sicherheitsanforderungen an das SIS	463
21.10 SIS-Entwurf und -Planung.....	463
21.10.1 Ziel	463
21.10.2 Allgemeine Anforderungen	463
21.10.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers	464
21.10.4 Anforderungen an die Fehlertoleranz der Hardware	464
21.10.5 Anforderungen an die Auswahl von Komponenten und Teilsystemen	465
21.10.6 Feldgeräte	465
21.10.7 Schnittstellen	466
21.10.8 Anforderungen an Instandhaltungs- oder Prüfeinrichtungen	466
21.10.9 Ausfallwahrscheinlichkeit sicherheitstechnischer Funktionen.....	467
21.11 Anforderungen an Anwendungssoftware	467
21.11.1 Anforderungen an den Sicherheitslebenszyklus der Anwendungssoftware	467
21.11.2 Spezifikation der Sicherheitsanforderungen an die Anwendungssoftware	472
21.11.3 Validierungsplanung für die Sicherheit der Anwendungssoftware	472
21.11.4 Entwurf und Erstellung der Anwendungssoftware.....	473
21.11.5 Integration der Anwendungssoftware in das SIS-Teilsystem.....	474
21.11.6 Vorgehen bei Modifikation der Anwendungssoftware	474
21.11.7 Verifikation der Anwendungssoftware	474
21.12 Werksendprüfungen.....	475
21.12.1 Ziele.....	475
21.12.2 Empfehlungen	475
21.13 SIS-Montage und -Inbetriebnahme.....	475
21.14 SIS-Sicherheits-Validierung	476
21.15 Betrieb und Instandhaltung des SIS	476
21.15.1 Ziele.....	476
21.15.2 Anforderungen	476
21.15.3 Wiederholungsprüfung und Inspektion	477
21.16 Modifikationen am SIS	477
21.16.1 Ziele.....	477

21.16.2 Anforderungen.....	477
21.17 Außerbetriebnahme des SIS	478
21.18 Anforderungen an die Dokumentation.....	478
21.18.1 Ziel.....	478
21.18.2 Anforderungen.....	478
22 Begriffe und Definitionen	479
22.1 Sicherheitssysteme	479
22.1.1 Risiko.....	479
22.1.2 Teilrisiko.....	479
22.1.3 Grenzrisiko	479
22.1.4 Risikoparameter.....	479
22.1.5 Anforderungsklasse	479
22.1.6 Maßnahmen	480
22.1.7 Schutz	480
22.1.8 MSR-Schutzmaßnahmen	480
22.1.9 MSR-Schutzeinrichtung	480
22.1.10 Unerwünschtes Ereignis	480
22.1.11 Fehler	480
22.1.12 Redundanz	480
22.1.13 Diversitäre Redundanz	481
22.1.14 Fail-safe	481
22.2 Verlässlichkeit (Dependability)	481
22.2.1 Zuverlässigkeit.....	482
22.2.2 Verfügbarkeit.....	484
22.2.3 Sicherheit	484
22.2.4 Wartbarkeit	485
22.3 Darstellung des Ausfallverhaltens.....	485
22.3.1 Dichtefunktion bzw. Ausfalldichte $f(t)$	485
22.3.2 Ausfallwahrscheinlichkeit bzw. Verteilungsfunktion $F(t)$	489
22.3.3 Zuverlässigkeit bzw. Überlebenswahrscheinlichkeit $R(t)$	492
22.3.4 Ausfallrate $\lambda(t)$	494
22.3.5 Beschreibung des Ausfallverhaltens anhand von Beispielen.....	498
22.3.6 Boolesche Theorie	501
22.4 Zeit-Faktor	503
22.4.1 MTTF	503
22.4.2 MTTF _{spurious}	504
22.4.3 MTBF	504
22.4.4 MTTR	504
22.4.5 Beispiel zur Berechnung von MTTF	504
22.4.6 Dauerverfügbarkeit	505
22.4.7 Downtime DT	507
22.4.8 Uptime UT	508
22.4.9 Mean Down Time MDT	508
22.5 Allgemeines zu den Begrifflichkeiten und Normen.....	508
22.5.1 Diagnoseabdeckungsgrad DC.....	510
22.5.2 Common Cause Failure CCF	511
22.5.3 Probability of Failure on Demand PFD	512

22.5.4 Ausfallraten	513
22.5.5 Risiko, Schaden und Gefahr	516
22.5.6 Hazard Rate	517
22.5.7 Safety Integrity Level SIL	518
22.6 Prozessleittechnik PLT	522
22.7 Performance Level PL	522
Literaturverzeichnis	523
Stichwortverzeichnis.....	553