# Inhaltsverzeichnis


**1 Einleitung ..... 19**
1.1 Grundlegende Forderungen ..... 22

**2 Grundlagen der Sicherheitstechnik in Rechnersystemen ..... 29**
2.1 Risikodefinition und Risikoanalyse ..... 31
2.2 Risiko und Folgen der Fehlfunktion ..... 32
2.3 Risikobewertung ..... 36
2.4 Risikograph ..... 39
2.5 Anforderungsklassen ..... 41
2.6 Akzeptanz eines Risikos ..... 42
2.7 Normative Institutionen und die Rolle von Normen und Standards ..... 49

**3 Allgemeines zur Entwicklung sicherheitskritischer Rechner ..... 55**
3.1 Allgemeine abstrakte Systembeschreibung ..... 56
3.1.1 Deskription ..... 57
3.1.2 Korrektheits- und Versagenswahrscheinlichkeit eines Systems ..... 57

**4 Fehler – Fehlerquellen – Fehlerauswirkung ..... 61**
4.1 Grundlagen ..... 61
4.2 Ausfälle und Fehler ..... 63
4.3 Fehlerquellen ..... 63
4.3.1 Interne Fehlerquellen ..... 64
4.3.2 Externe Fehlerquellen ..... 64
4.4 Bedeutung von Fehlerquellen ..... 65
4.5 Fehlerauswirkungen ..... 66

**5 Entwicklungsaspekte für sichere Hardware ..... 67**
5.1 Fehlerannahmen eingesetzter Hardwarekomponenten in sicheren Rechnersystemen ..... 70

**6 Entwicklungsmodelle für Software in sicherheitsgerichteten Systemen ..... 75**
6.1 Wasserfall-Modell ..... 77
6.2 Spiral-Modell ..... 77
6.3 Rapid Prototyping ..... 78
6.4 V-Modell ..... 78
6.5 Softwareentwicklung für sicherheitsgerichtete Systeme ..... 78
6.5.1 Festlegen der Sicherheitsanforderungen ..... 79
6.6 Vorgehen bei der Implementierung ..... 80
6.6.1 Strukturiertes Programmieren ..... 80

6.6.2 Modularisierung ... 80
6.6.3 Objektorientierung ... 81
6.6.4 Kodierungsregeln ... 82
6.7 Nachweis der Zuverlässigkeit ... 83
6.7.1 Inspektion ... 83
6.7.2 Review ... 84
6.7.3 Walkthrough ... 84
6.7.4 Statische Analyse ... 84
6.7.5 Programmkorrektheitsbeweis ... 85
6.7.6 Test ... 85

**7 Maßnahmen zur Fehlervermeidung und Fehleraufdeckung in Softwaresystemen ... 89**
7.1 Software-Diversität ... 89
7.2 Programmlaufüberwachung ... 91
7.2.1 Zeitliche Überwachung ... 92
7.2.2 Logische Überwachung ... 93
7.2.2.1 Buserweiterung ... 93
7.2.2.2 Überwachung durch Zählverfahren ... 94
7.2.2.3 Überwachung mit Rücksprungkontrolle ... 94
7.2.3 Fehleraufdeckungsgrad einer Programmablaufüberwachung ... 94
7.3 Reale Überwachungsmaßnahme ... 96

**8 Verifikation, Validation und Sicherheitsplan ... 99**
8.1 Planung für Verifikation und Validation ... 99
8.1.1 Sicherheitsplan ... 101

**9 Methoden zur Fehlererkennung ... 105**
9.1 Fehlerbaumanalyse ... 106
9.2 Ereignis-Baum-Analyse ... 107
9.3 FMEA ... 108
9.3.1 Entwicklung und Anwendung der FMEA ... 109
9.3.2 Definitionen und Grundbegriffe ... 110
9.3.2.1 Abweichung/Ausfall/Fehler/Irrtum ... 110
9.3.2.2 Verfügbarkeit ... 113
9.3.2.3 Zuverlässigkeit ... 114
9.3.3 Hauptarten der FMEA ... 115
9.3.4 Erstellen einer FMEA - Allgemein ... 117
9.3.4.1 Stufe I: Systembeschreibung ... 118
9.3.4.2 Stufe II: Fehleranalyse ... 118
9.3.4.3 Stufe III: Risikobeurteilung ... 128
9.3.4.4 Stufe IV: Aktivitäten/Qualitätsverbesserung ... 129
9.3.4.5 Stufe V: Ergebnisbeurteilung/Einführung der Verbesserungsmaßnahmen. 130
9.3.5 Durchführung einer FMEA ... 130
9.3.6 Unterschiede zwischen einer allgemeinen FMEA und einer speziellen FMEA ... 131
9.3.6.1 Möglichkeiten der Verbesserung ... 131
9.3.7 Kurzbeschreibung einer Muster-FMEA ... 132
9.3.8 Ausfallratensammlung ... 137

**10 Mathematische und statistische Grundlagen ....139**
10.1 Kombinatorik; Kombination, Variation, Permutation ....139
10.1.1 Permutation....139
10.1.2 Variation....141
10.1.3 Kombination....141
10.2 Fehlerkombinationsbetrachtung sicherheitsgerichteter Rechnerarchitekturen ....143
10.3 Fehlerkombinationsmöglichkeiten des 1oo2-Systems....143
10.3.1 Interne Strangbetrachtung des 1oo2-Systems....144
10.3.2 Ausfall eines Elements im Strang....144
10.3.3 Ausfall beider Elemente im Strang....145
10.3.4 Ausfall eines Strangs....145
10.3.5 Tabellarische Fehlerkombinationen der 1oo2-Architektur....146
10.4 Fehlerkombinationsmöglichkeiten eines 1oo3-Systems....146
10.4.1 Interne Strangbetrachtung des 1oo3-Systems....147
10.4.1.1 Ausfall eines Elements im Strang....147
10.4.1.2 Ausfall beider Elemente im Strang....148
10.4.2 Strangbetrachtung im 1oo3-System....148
10.4.2.1 Ausfall eines Strangs....148
10.4.2.2 Ausfall von zwei Strängen....149
10.4.2.3 Minimum zwei Fehlfunktionen in zwei Strängen....149
10.4.2.4 Drei Fehlfunktionen in zwei Strängen....150
10.4.2.5 Maximum vier Fehlfunktionen in zwei Strängen....150
10.4.2.6 Gesamtheit der möglichen Fehlerkombinationen für ein 1oo3-System....150
10.4.2.7 Tabellarische Fehlerkombinationen....151
10.5 Fehlerkombinationsmöglichkeiten in einem 2oo3-System mit zwei Elementen....152
10.5.1 Interne Strangbetrachtung des 2oo3-Systems....152
10.5.1.1 Ausfall eines Elements im Strang....152
10.5.1.2 Ausfall beider Elemente im Strang....153
10.5.1.3 Tabellarische Fehlerkombinationen....155
10.6 Fehlerkombinationsmöglichkeiten eines 2oo3-Systems mit drei Elementen ....156
10.6.1 Interne Strangbetrachtung des 2oo3-Systems....156
10.6.1.1 Ausfall eines Elements im Strang....156
10.6.1.2 Ausfall von zwei Elementen im Strang....157
10.6.1.3 Dreifacher Fehler in einem Strang....158
10.6.2 Strangbetrachtung im 2oo3-System....158
10.6.2.1 Ausfall eines Strangs....158
10.7 Fehlerkombinationsmöglichkeiten eines 2oo4-Systems....159
10.7.1 Interne Strangbetrachtung des 2oo4-Systems....159
10.7.1.1Ausfall eines Elements im Strang....159
10.7.1.2 Ausfall beider Elemente im Strang....160
10.7.2 Strangbetrachtung im 2oo4-System....161
10.7.2.1 Ausfall eines Strangs....161
10.7.2.2 Ausfall von zwei Strängen....161
10.7.2.3 Minimum zwei Fehlfunktionen in zwei Strängen....161
10.7.2.4 Drei Fehlfunktionen in zwei Strängen....162
10.7.2.5 Maximum vier Fehlfunktionen in zwei Strängen....162
10.7.3 Gesamtheit der möglichen Fehlerkombinationen für ein 2oo4-System....163

10.8 Fehlerkombinationsmöglichkeiten eines 2oo4-Systems mit drei Elementen ..... 163
10.8.1 Interne Strangbetrachtung des 2oo4-Systems ..... 163
10.8.1.1 Ausfall eines Elements im Strang ..... 164
10.8.1.2 Ausfall von zwei Elementen im Strang ..... 164
10.8.1.3 Dreifach-Fehler in einem Strang ..... 165
10.8.2 Strangbetrachtung im 2oo4-System mit drei Elementen ..... 165
10.8.2.1 Ausfall eines Strangs ..... 165
10.8.2.2 Ausfall von zwei Strängen ..... 165
10.8.2.3 Minimum zwei Fehlfunktionen in zwei Strängen ..... 166
10.8.2.4 Drei Fehlfunktionen in zwei Strängen ..... 166
10.8.2.5 Vier Fehlfunktionen in zwei Strängen ..... 167
10.8.2.6 Zwei Doppelfehler ..... 167
10.8.2.7 Drei Fehler in einem Strang und einer in dem zweiten Strang ..... 168
10.8.2.8 Fünf Fehlfunktionen in zwei Strängen ..... 168
10.8.2.9 Sechs Fehlfunktionen in zwei Strängen ..... 169
10.8.3 Gesamtheit der möglichen Fehlerkombinationen ..... 169
10.9 Wahrscheinlichkeiten ..... 169
10.9.1 Begriff der Wahrscheinlichkeit ..... 169
10.9.2 Berechnungsregeln der Wahrscheinlichkeit ..... 174
10.9.3 Addition von Wahrscheinlichkeiten ..... 174
10.9.4 Multiplikation von Wahrscheinlichkeiten ..... 175
10.9.5 Totale Wahrscheinlichkeiten ..... 177

**11 Wahrscheinlichkeitsverteilungen ..... 179**
11.1 Diskrete Wahrscheinlichkeitsverteilungen ..... 181
11.2 Stetige Wahrscheinlichkeitsverteilungen ..... 183
11.3 Lage- und Formparameter diskreter und stetiger Verteilungsfunktionen ..... 185
11.4 Exponentialverteilung ..... 186
11.5 Rechteckverteilung oder Gleichverteilung ..... 187
11.6 Binomialverteilung ..... 188
11.7 Weibull-Verteilung ..... 189
11.8 Lognormal-Verteilung ..... 191
11.9 $\chi^2$ -Verteilung ..... 192
11.10 Student-Verteilung ..... 194
11.11 Grenzwertsatz ..... 195
11.12 Konfidenzintervall ..... 197
11.12.1 Konfidenzintervall für den Erwartungswert mit Hilfe der $\chi^2$-Verteilung ..... 197
11.12.2 Konfidenzintervall für den Erwartungswert mit Hilfe der t-Verteilung ..... 199

**12 Schaltungsmaßnahmen zur Zuverlässigkeitserhöhung ..... 201**
12.1 Kenngrößen der Zuverlässigkeit ..... 202
12.2 Ausfallwahrscheinlichkeit ..... 204
12.3 Mittlere Lebensdauer ..... 205
12.4 Mittlere Instandsetzungszeit ..... 206
12.5 Mittlere Brauchbarkeitsdauer ..... 207
12.6 Verfügbarkeit ..... 207
12.7 Ausfallrate $\lambda(t)$ ..... 207
12.8 Zuverlässigkeitsmodelle für Gerätesysteme ..... 210
12.8.1 Systeme ohne Redundanz ..... 210

12.8.2 Systeme mit Redundanz ....213
12.8.3 Gemischte Systeme....216
12.9 Redundante Systeme mit unterschiedlicher Ausfallrate ....229
12.10 Ersatz von redundanten Systemkomponenten durch Einzelsystemkomponenten..234

**13 PFD-Berechnung, $\beta$-Faktor und Diagnoseabdeckung....237**
13.1 Grundlagen ....237
13.2 Herleitung der $PFD_{avg}$-Gleichungen für Systemarchitekturen....242
13.2.1 Allgemeine Betrachtungen ....242
13.2.2 1oo1-System ....250
13.2.3 1oo2-System ....252
13.2.3.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern...253
13.2.3.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern....254
13.2.4 2oo2-System ....258
13.2.5 1oo3-System ....259
13.2.5.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern...260
13.2.5.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern....261
13.2.6 2oo3-System ....271
13.2.6.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern...272
13.2.6.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern....273
13.2.7 2oo4-System ....274
13.2.7.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern...275
13.2.7.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern....275
13.2.8 1oo2D-System ....277
13.2.8.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern...277
13.2.8.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern....278
13.2.9 2oo4D-System ....280
13.2.9.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern...281
13.2.9.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern....281
13.2.10 Berechnung des $PFD_{avg}$-Werts für eine Reihenarchitektur....284
13.2.11 Berechnung des $PFD_{avg}$-Werts für eine Reihen-Parallelarchitektur ....285
13.3 Berechnung des $\beta$-Faktors ....286
13.3.1 Berechnung des $PFD_{avg}$-Werts für ein mehrkanaliges System ....292

**14 Markov-Modell....297**
14.1 Einleitung ....297
14.2 Möglichkeiten des Markov-Modells ....298
14.3 Theoretische Grundlagen der Markov-Modelle ....299
14.4 Zeitabhängiges Markov-Modell ....304
14.5 Markov-Modell-Berechnung für ein sicherheitsgerichtetes System....304
14.5.1 Übergangsmatrix P für ein System-Modell ....307
14.5.2 Baumdiagramm des redundanten System-Modells ....313
14.5.3 Berechnung der Grenzwert-Zustandswahrscheinlichkeiten unabhängig vom Ausgangszustand mit der Matrixmultiplikation ....318
14.5.4 Berechnung der Grenzwert-Zustandswahrscheinlichkeiten in Abhängigkeit vom Anfangszustand ....324
14.5.4.1 Start im Zustand $Z_0$....324
14.5.4.2 Start im Zustand $Z_1$ ....329
14.5.4.3 Start im Zustand $Z_2$ ....334

14.5.4.4 Start im Zustand $Z_3$ ..... 339
14.5.4.5 Start im Zustand $Z_4$ ..... 343
14.5.4.6 Start im Zustand $Z_5$ ..... 348
14.5.4.7 Start im Zustand $Z_6$ ..... 353
14.5.5 Berechnung der zeitabhängigen Verfügbarkeit ..... 354
14.5.6 Berechnung der zeitabhängigen Zuverlässigkeit ..... 357
14.5.7 Vergleich von Verfügbarkeit und Zuverlässigkeit ..... 358

**15 Grundlagen und Erläuterungen der Systeme (Verfahren und Modelle) ..... 359**
15.1 Einleitung ..... 359
15.1.1 Überwachungskonstruktionen ..... 360
15.2 Systemkonfiguration und Voraussetzungen ..... 360
15.3 1oo1-System ..... 361
15.3.1 PFD-Fehlerbaum der 1oo1-Architektur ..... 361
15.3.2 Markov-Modell für die 1oo1-Architektur ..... 363
15.3.3 Berechnung des *MTTF*-Werts ..... 365
15.4 1oo2-System ..... 367
15.4.1 PFD-Fehlerbaum der 1oo2-Architektur ..... 368
15.4.2 Markov-Modell für die 1oo2-Architektur ..... 372
15.4.3 Berechnung des *MTTF*-Werts ..... 375
15.5 2oo2-System ..... 377
15.5.1 PFD-Fehlerbaum der 2oo2-Architektur ..... 378
15.5.2 Markov-Modell der 2oo2-Architektur ..... 379
15.5.3 Berechnung des *MTTF*-Werts ..... 382
15.6 1oo3-System ..... 384
15.6.1 PFD-Fehlerbaum der 1oo3-Architektur ..... 385
15.6.2 Markov-Modell für die 1oo3-Architektur ..... 389
15.6.3 Berechnung des *MTTF*-Werts ..... 393
15.7 2oo3-System ..... 396
15.7.1 PFD-Fehlerbaum der 2oo3-Architektur ..... 398
15.7.2 Markov-Modell der 2oo3-Architektur ..... 401
15.7.3 Berechnung des *MTTF*-Werts ..... 404
15.8 2oo4-Systeme ..... 408
15.8.1 PFD-Fehlerbaum des 2oo4-Systems ..... 409
15.8.2 Markov-Modell der 2oo4-Architektur ..... 412
15.8.3 Berechnung des *MTTF*-Werts ..... 417
15.9 1oo2D-System ..... 425
15.9.1. PFD-Fehlerbaum der 1oo2D-Architektur ..... 426
15.9.2 Markov-Modell der 1oo2D-Architektur ..... 429
15.9.3 Berechnung des *MTTF*-Werts ..... 433
15.10 2oo4D-System ..... 435
15.10.1 PFD-Fehlerbaum der 2oo4D-Architektur ..... 437
15.10.2 Markov-Modell der 2oo4D-Architektur ..... 442
15.10.3 Berechnung des MTTF-Werts ..... 449
15.11 Berechnung des *MTTF*-Werts verschiedener Architekturen ..... 470
15.11.1 *MTTF*-Werte für Eingangselemente ..... 470
15.11.2 *MTTF*-Werte für Rechnerelemente ..... 472
15.11.3 *MTTF*-Werte für Ausgangselemente ..... 474

**16 MTTF-Bestimmung durch eine Monte-Carlo-Simulation ..... 477**
16.1 Einführung ..... 477
16.1.1 Erläuterungen zur Monte-Carlo-Simulation ..... 477
16.2 Mathematische Grundlagen ..... 478
16.2.1 Zufallszahlen ..... 482
16.3 Monte-Carlo-Algorithmus ..... 484
16.3.1 Rechenalgorithmus zur Berechnung des *MTTF* mit der Monte-Carlo-Simulation ..... 486
16.4 Anwendung auf verschiedene Systemarchitekturen ..... 495
16.4.1 1oo1-System ..... 496
16.4.2 1oo2-System ..... 515
16.4.3 1oo2-System mit $\beta$-Faktor ..... 531
16.4.4 2oo3-System ..... 535
16.4.5 2oo4-System ..... 547
16.4.6 1oo2D-System mit $\beta$-Faktor ..... 567
16.5 Vergleich der *MTTF*-Werte berechnet mit Markov und MCS für ein SIS ..... 571

**Literaturverzeichnis ..... 575**

**Abkürzungsverzeichnis ..... 597**

**Stichwortverzeichnis ..... 607**