

Josef Börcsök

Elektronische Sicherheitssysteme

Hardwarekonzepte, Modelle und Berechnung

f

2., überarbeitete Auflage



Hüthig Verlag Heidelberg

Inhaltsverzeichnis

1 Einleitung.....	1
1.1 Gründlegende Forderungen.....	4
2 Grundlagen der Sicherheitstechnik in Rechnersystemen.....	11
2.1 Risikodefinition und Risikoanalyse.....	13
2.2 Risiko und Folgen der Fehlfunktion.....	15
2.3 Risikobewertung.....	18
2.4 Risikograph.....	21
2.5 Anforderungsklassen.....	23
2.6 Akzeptanz eines Risikos.....	24
2.7 Normative Institutionen und die Rolle von Normen und Standards.....	31
3 Allgemeines zur Entwicklung sicherheitskritischer Rechner.....	37
3.1 Allgemeine abstrakte Systembeschreibung.....	38
3.1.1 Deskription.....	39
3.1.2 Korrektheits- und Versagenswahrscheinlichkeit eines Systems.....	39
4 Fehler^ Fehlerquellen - Fehlerauswirkung.....	43
4.1 Grundlagen.....	43
4.2 Ausfälle und Fehler.....	45
4.3 Fehlerquellen.....	45
4.3.1 Interne Fehlerquellen.....	46
4.3.2 Externe Fehlerquellen.....	46
4.4 Bedeutung von Fehlerquellen.....	48
4.5 Fehlerauswirkungen.....	48
5 Entwicklungsaspekte für sichere Hardware.....	49
5.1 Fehlerannahmen eingesetzter Hardwarekomponenten in sicheren Rechnersystemen.....	52
6 Entwicklungsmodelle für Software in sicherheitsgerichteten Systemen.....	57
6.1 Wasserfall-Modell.....	59
6.2 Spiral-Modell.....	59
6.3 Rapid Prototyping.....	60
6.4 V-Modell.....	60
6.5 Softwareentwicklung für sicherheitsgerichtete Systeme.....	60
6.5.1 Festlegen der Sicherheitsanforderungen.....	61
6.6 Vorgehen bei der Implementierung.....	61
6.6.1 Strukturiertes Programmieren.....	62
6.6.2 Modularisierung.....	62

6.6.3	Objektorientierung.....	63
6.6.4	Kodierungsregeln.....	64
6.7	Nachweis der Zuverlässigkeit.....	65
6.7.1	Inspektion.....	65
6.7.2	Review.....	65
6.7.3	Walkthrough.....	66
6.7.4	Statische Analyse.....	66
6.7.5	Programmkorrektheitsbeweis.....	67
6.7.6	Test.....	67
7	Maßnahmen zur Fehlervermeidung und Fehlerrückmeldung in Softwaresystemen	71
7.1	Software-Diversität.....	71
7.2	Programmlaufüberwachung.....	73
7.2.1	Zeitliche Überwachung.....	74
7.2.2	Logische Überwachung.....	75
7.2.2.1	Buserweiterung.....	75
7.2.2.2	Überwachung durch Zählverfahren.....	76
7.2.2.3	Überwachung mit Rücksprungkontrolle.....	76
/	7.2.3 Fehlerauffindungsgrad einer Programmablaufüberwachung.....	76
'/	7.3 Reale Überwachungsmaßnahme.....	78
'{.''''	8 Verifikation, Validation und Sicherheitsplan.....	81
8.1	Planung für Verifikation und Validation.....	81
8.1.1	Sicherheitsplan.....	83
9	Methoden zur Fehlererkennung.....	88
9.1	Fehlerbaumanalyse.....	88
9.2	Ereignis-Baum-Analyse.....	89
9.3	FMEA.....	90
9.3.1	Entwicklung und Anwendung der FMEA.....	91
9.3.2	Definitionen und Grundbegriffe.....	92
*	9.3.2.1 Abweichung/Ausfall/Fehler/Irrtum.....	92
	9.3.2.2 Verfügbarkeit.....	92
	9.3.2.3 Zuverlässigkeit.....	92
	9.3.3 Hauptarten der FMEA.....	92
	9.3.4 Erstellen einer FMEA - Allgemein.....	92
	9.3.4.1 Stufe I: Systembeschreibung.....	10
	9.3.4.2 Stufe II: Fehleranalyse.....	10
	9.3.4.3 Stufe III: Risikobeurteilung.....	11
	9.3.4.4 Stufe IV: Aktivitäten Qualitätsverbesserung.....	11
	9.3.4.5 Stufe V: Ergebnisbeurteilung/Einführung der Verbesserungsmaßnahmen.....	11
	9.3.5 Durchführung einer FMEA.....	11
	9.3.6 Unterschiede zwischen einer allgemeinen FMEA und einer speziellen FMEA.....	11
	9.3.6.1 Möglichkeiten der Verbesserung.....	11
	9.3.7 Kurzbeschreibung einer Muster-FMEA.....	11
	9.3.8 Ausfallratensammlung.....	11

10 Mathematische und statistische Grundlagen	121
10.1 Kombinatorik; Kombination, Variation, Permutation	121
10.1.1. Permutation	121
10.1.2. Variation	122
10.1.3 Kombination	123
10.2 Fehlerkombinationsbetrachtung sicherheitsgerichteter Rechnerarchitekturen	124
10.3 Fehlerkombinationsmöglichkeiten des Ioo2-Systems	125
10.3.1 Interne Strangbetrachtung des Ioo2-Systems	125
10.3.2 Ausfall eines Elementes im Strang	126
10.3.3 Ausfall beider Elemente im Strang	126
10.3.4 Ausfall eines Stranges	127
10.3.5 Tabellarische Fehlerkombinationen der Ioo2-Architektur	128
10.4 Fehlerkombinationsmöglichkeiten eines Ioo3-Systems	128
10.4.1 Interne Strangbetrachtung des Ioo3-Systems	129
10.4.1.1 Ausfall eines Elementes im Strang	129
10.4.1.2 Ausfall beider Elemente im Strang	129
10.4.2 Strangbetrachtung im Ioo3-System	130
10.4.2.1 Ausfall eines Stranges	130
10.4.2.2 Ausfall von zwei Strängen	130
10.4.2.3 Minimum zwei Fehlfunktionen in zwei Strängen	131
10.4.2.4 Drei Fehlfunktionen in zwei Strängen	131
10.4.2.5 Maximum vier Fehlfunktionen in zwei Strängen	132
10.4.2.6 Gesamtheit der möglichen Fehlerkombinationen für ein Ioo3-System	132
10.4.2.7 Tabellarische Fehlerkombinationen	133
10.5 Fehlerkombinationsmöglichkeiten in einem 2oo3-System mit zwei Elementen	134
10.5.1 Interne Strangbetrachtung des 2oo3-Systems	134
10.5.1.1 Ausfall eines Elementes im Strang	134
10.5.1.2 Ausfall beider Elemente im Strang	135
10.5.1.3 Tabellarische Fehlerkombinationen	137
10.6 Fehlerkombinationsmöglichkeiten eines 2oo3-Systems mit drei Elementen	138
10.6.1 Interne Strangbetrachtung des 2oo3-Systems	138
10.6.1.1 Ausfall eines Elementes im Strang	138
10.6.1.2 Ausfall von zwei Elementen im Strang	139
10.6.1.3 Dreifacher Fehler in einem Strang	140
10.6.2 Strangbetrachtung im 2oo3-System	140
10.6.2.1 Ausfall eines Stranges	140
10.7 Fehlerkombinationsmöglichkeiten eines 2oo4-Systems	140
10.7.1 Interne Strangbetrachtung des 2oo4-Systems	141
10.7.1.1 Ausfall eines Elementes im Strang	141
10.7.1.2 Ausfall beider Elemente im Strang	142
10.7.2 Strangbetrachtung im 2oo4-System	142
10.7.2.1 Ausfall eines Stranges	142
10.7.2.2 Ausfall von zwei Strängen	143
10.7.2.3 Minimum zwei Fehlfunktionen in zwei Strängen	143
10.7.2.4 Drei Fehlfunktionen in zwei Strängen	143
10.7.2.5 Maximum vier Fehlfunktionen in zwei Strängen	144
10.7.3 Gesamtheit der möglichen Fehlerkombinationen für ein 2oo4-System	144

10.8 Fehlerkombinationsmöglichkeiten eines 2oo4-Systems mit drei Elementen	14
10.8.1 Interne Strangbetrachtung des 2oo4-Systems	14
10.8.1.1 Ausfall eines Elementes im Strang	14
10.8.1.2 Ausfall von zwei Elementen im Strang	14
10.8.1.3 Dreifach-Fehler in einem Strang	14
10.8.2 Strangbetrachtung im 2oo4-System mit drei Elementen	14
10.8.2.1 Ausfall eines Stranges	14
10.8.2.2 Ausfall von zwei Strängen	14
10.8.2.3 Minimum zwei Fehlfunktionen in zwei Strängen	14
10.8.2.4 Drei Fehlfunktionen in zwei Strängen	14
10.8.2.5 Vier Fehlfunktionen in zwei Strängen	14
10.8.2.6 Zwei Doppelfehler	14
10.8.2.7 Drei Fehler in einem Strang und einer in dem zweiten Strang	14
10.8.2.8 Fünf Fehlfunktionen in zwei Strängen	15
10.8.2.9 Sechs Fehlfunktionen in zwei Strängen	15
10.8.3 Gesamtheit der möglichen Fehlerkombinationen	15
10.9 Wahrscheinlichkeiten	15
10.9.1 Begriff der Wahrscheinlichkeit	
10.9.2 Berechnungsregeln der Wahrscheinlichkeit	
10.9.3 Addition von Wahrscheinlichkeiten	
10.9.4 Multiplikation von Wahrscheinlichkeiten	
10.9.5 Totale Wahrscheinlichkeiten	
11 Wahrscheinlichkeitsverteilungen	1
11.1 Diskrete Wahrscheinlichkeitsverteilungen	1
11.2 Stetige Wahrscheinlichkeitsverteilungen	1
11.3 Lage- und Formparameter diskreter und stetiger Verteilungsfunktionen	1
11.4 Exponentialverteilung	1
11.5 Rechteckverteilung oder Gleichverteilung	1
11.6 Binomialverteilung	1
» 11.7 Weibull-Verteilung	1
11.8 Lognormal-Verteilung	1
11.9 χ^2 -Verteilung	1
11.10 Student-Verteilung	1
11.11 Grenzwertsatz	1
11.12 Konfidenzintervall	1
11.12.1 Konfidenzintervall für den Erwartungswert mit Hilfe der χ^2 -Verteilung, 1	
11.12.2 Konfidenzintervall für den Erwartungswert mit Hilfe der t-Verteilung, 1	
12 Schaltungsmaßnahmen zur Zuverlässigkeitserhöhung.	
12.1 Kenngrößen der Zuverlässigkeit	
12.2 Ausfallwahrscheinlichkeit	
12.3 Mittlere Lebensdauer	
12.4 Mittlere Instandsetzungszeit	
12.5 Mittlere Brauchbarkeitsdauer	
12.6 Verfügbarkeit	
12.7 Ausfallrate $\dot{A}(t)$	
12.8 Zuverlässigkeitsmodelle für Gerätesysteme	

12.8.1 Systeme ohne Redundanz.....	192
12.8.2 Systeme mit Redundanz.....	194
12.8.3 Gemischte Systeme.....	198
12.9 Redundante Systeme mit unterschiedlicher Ausfallrate.....	210
12.10 Ersatz von redundanten Systemkomponenten durch Einzelsystemkomponenten ..	215
13 PFD-, /?-Faktor und Diagnoseabdeckung.....	219
13.1 Grundlagen.....	219
13.2 Herleitung der /"FD^-Gleichungen für Systemarchitekturen.....	225
13.2.1 Allgemeine Betrachtungen.....	225
13.2.2 Ioo1-System.....	232
13.2.3 Ioo2-System.....	234
13.2.3.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern ..	235
13.2.3.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern	236
13.2.4 2oo2-System.....	240
13.2.5 Ioo3-System.....	241
13.2.5.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern ..	242
13.2.5.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern	242
13.2.6 2oo3-System.....	252
13.2.6.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern ..	253
13.2.6.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern	254
13.2.7 2oo4-System.....	255
13.2.7.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern ..	256
13.2.7.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern	256
13.2.8 Ioo2D-System.....	258
13.2.8.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern ..	258
13.2.8.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern	259
13.2.9 2oo4D-System.....	261
13.2.9.1 Berechnung der Ausfallwahrscheinlichkeit bei common-cause-Fehlern ..	262
13.2.9.2 Berechnung der Ausfallwahrscheinlichkeit bei einfachen Fehlern	262
13.2.10 Berechnung des PFD_{avg} -Wertes für eine Reihenarchitektur.....	265
13.2.11 Berechnung des PFD_{avg} -Wertes für eine Reihen-Parallelarchitektur.....	266
13.3 Berechnung des /^-Faktors.....	267
13.3.1 Berechnung des PFD_{avg} -Wertes für ein mehrkanaliges System.....	273
14 Markov-Modell.....	279
14.1 Einleitung.....	279
14.2 Möglichkeiten des Markov-Modells.....	280
14.3 Theoretische Grundlagen der Markov-Modelle.....	281
14.4 Zeitabhängiges Markov-Modell.....	286
14.5 Markov-Modell-Berechnung für ein sicherheitsgerichtetes System.....	286
14.5.1 Übergangsmatrix P für ein System-Modell.....	289
14.5.2 Baumdiagramm des redundanten System-Modells.....	295
14.5.3 Berechnung der Grenzwert-Zustandswahrscheinlichkeiten unabhängig vom Ausgangszustand mit der Matrixmultiplikation.....	300
14.5.4 Berechnung der Grenzwert-Zustandswahrscheinlichkeiten in Abhängigkeit vom Anfangszustand.....	306
14.5.4.1 Start im Zustand Z_0	307

14.5.4.3 Start im Zustand Z_2	316
14.5.4.4 Start im Zustand Z_3	321
14.5.4.5 Start im Zustand Z_4	325
14.5.4.6 Start im Zustand Z_5	330
14.5.4.7 Start im Zustand Z_6	335
14.5.5 Berechnung der zeitabhängigen Verfügbarkeit	336
14.5.6 Berechnung der zeitabhängigen Zuverlässigkeit	339
14.5.7 Vergleich von Verfügbarkeit und Zuverlässigkeit	340
15 Grundlagen und Erläuterungen der Systeme (Verfahren und Modelle)	341
15.1 Einleitung	341
15.1.1 Überwachungskonstruktionen	342
15.2 Systemkonfiguration und Voraussetzungen	342
15.3 Iool-System	343
15.3.1 PFD-Fehlerbaum der Iool-Architektur	343
15.3.2 Markov-Modell für die Iool-Architektur	345
15.3.3 Berechnung des MTRF-Wertes	347
15.4 Ioo2-System	349
15.4.1 PFD-Fehlerbaum der Ioo2-Architektur	350
15.4.2 Markov-Modell für die Ioo2-Architektur	355
15.4.3 Berechnung des MTTF-Wertes	357
15.5 2oo2-System	360
15.5.1 PFD-Fehlerbaum der 2oo2-Architektur	360
15.5.2 Markov-Modell der 2oo2-Architektur	362
15.5.3 Berechnung des MTTF-Wertes	364
15.6 Ioo3-System	366
15.6.1 PFD-Fehlerbaum der Ioo3-Architektur	367
15.6.2 Markov-Modell für die Ioo3-Architektur	371
15.6.3 Berechnung des MTTF-Wertes	375
15.7 2oo3-System	378
15.7.1 PFD-Fehlerbaum der 2oo3-Architektur	378
15.7.2 Markov-Modell der 2oo3-Architektur	382
15.7.3 Berechnung des MTTF-Wertes	386
15.8 2oo4-Systeme	396
15.8.1 PFD-Fehlerbaum des 2oo4-Systems	391
15.8.2 Markov-Modell der 2oo4-Architektur	391
15.8.3 Berechnung des MTTF-Wertes	391
15.9 Ioo2D-System	400
15.9.1 PFD-Fehlerbaum der Ioo2D-Architektur	401
15.9.2 Markov-Modell der Ioo2D-Architektur	41
15.9.3 Berechnung des MTTF-Wertes	41
15.10 2oo4D-System	41
15.10.1 PFD-Fehlerbaum der 2oo4D-Architektur	41
15.10.2 Markov-Modell der 2oo4D-Architektur	42
15.10.3 Berechnung des MTTF-Wertes	43
15.11 Berechnung des MTTF-Wertes verschiedener Architekturen	45
15.11.1 MTTF-Wert für Eingangselemente	45

15.11.2 A/7TF-Werte für Rechnerelemente.....	453
15.11.3 MT7F-Werte für Ausgangselemente.....	456
16 MTTF-Bestimmung durch eine Monte-Carlo-Simulation.....	459
16.1 Einführung.....	459
16.1.1 Erläuterungen zur Monte-Carlo-Simulation.....	459
16.2 Mathematische Grundlagen.....	460
16.2.1 Zufallszahlen.....	464
16.3 Monte-Carlo ¹ Algorithmus.....	466
16.3.1 Rechenalgorithmus zur Berechnung des <i>MTTF</i> mit der Monte-Carlo-Simulation.....	468
16.4 Anwendung auf verschiedene Systemarchitekturen.....	477
16.4.1 lool-System.....	478
16.4.2 Ioo2-System.....	497
16.4.3 loo2-Systemmit/?-Faktor.....	514
16.4.4 2oo3-System.....	518
16.4.5 2oo4-System.....	530
16.4.6 loo2D-Systemmit/?-Faktor..j.....	552
16.5 Vergleich der <i>MTTF</i> -Werte berechnet mit Markov und MCS für ein SIS.....	557
Literaturverzeichnis.....ly&.....	561
Abkürzungsverzeichnis.....oi-.....	583
Stichwortverzeichnis.....	593