

Inhaltsverzeichnis

1	Das Lebenszyklusmodell	1
1.1	Grundsätzliche Überlegungen	2
1.1.1	Sicherheitsklassifizierung	2
1.1.2	Gefahrenanalyse	3
1.1.3	Einhaltung der Normen	5
1.1.4	Fehlervermeidung	6
1.1.5	Fehlererkennung und Fehlerbeherrschung	7
1.2	Die Phasen des Lebenszyklus	8
1.3	Risikoanalyse	9
1.3.1	Risikograf	9
1.3.2	Risikobeurteilung	14
1.4	FMEA	18
1.5	SRS (Safety Requirement Specification)	23
2	Organisation und Dokumentation	25
2.1	Projektdokumente	28
2.1.1	Funktionale Spezifikation	30
2.1.2	Spezifikation der Sicherheitsanforderungen (Safety Requirement Specification, SRS)	30
2.1.3	Validation- und Verifikationsplan (V&V Plan)	33
3	Kenngößen für die Sicherheitsbewertung	35
3.1	Zusammenhang der Kenngößen	35
3.1.1	Fehlerausschlüsse	37
3.1.2	Funktionstests	38
3.2	Sicherheitsarchitekturen	40
3.2.1	1oo1-Struktur, HFT	41
3.2.2	1oo2- und 1oo2D-Struktur	41
3.2.3	Fail-Safe-Logik	43
3.2.4	2oo3-Struktur	44
3.2.5	Fehlerbaum mehrkanaliger Strukturen	45
3.2.6	Ausfallraten	46
3.2.7	Verteilungsfunktion und Ausfallhäufigkeit	47
3.2.8	λ -Wert, Zuverlässigkeitsfunktion und MTBF-Bestimmung	49
3.2.9	Ausfallwahrscheinlichkeit, PFD-Werte	51
3.2.10	Aufteilung der λ -Werte im System, SFF	52
3.3	Diagnosedeckungsgrad, Testintervall	58
3.3.1	DC und SFF	58
3.3.2	Testintervall	59
3.3.3	Zyklische Tests	61
3.3.4	Wiederholdauer zyklischer Tests	63

3.4	Fehler gemeinsamer Ursache	63
3.4.1	Versorgungseinheiten	64
3.4.2	Zweikanalige Abschaltung	65
3.4.3	Abschätzung des β -Wertes	67
3.5	PFD- und PFH-Wert	69
3.6	Anforderungen aus den Normen	71
3.6.1	EN 954-1	71
3.6.2	IEC 61508	71
3.6.3	EN 62061 und DIN EN ISO 13849	72
3.7	Rechenbeispiele	73
3.7.1	SFF und DC für eine elektronische Eingangsschaltung	73
3.7.2	Einkanalgiges System für SIL 2	75
3.7.3	Sporadischer Ausfall bei einem zweikanaligen System	76
4	Architekturen	79
4.1	Erfassung von Messgrößen, Sensoren und Eingangsschaltungen	79
4.1.1	Einkanalgige Sensorstruktur	79
4.1.2	Einkanalgiger Sensor mit zweikanaliger Eingangsschaltung	80
4.1.3	Sensoren mit zweikanaliger Eingangsschaltung	81
4.1.4	Diversitäre Sensoren mit zweikanaliger Eingangsschaltung	82
4.1.5	Test von kontaktbehafteten Sensoren	84
4.1.6	Geschlossener Testkreis	85
4.1.7	Testbare Eingangsstufe	86
4.2	Ausgangsschaltungen	86
4.2.1	Serienschaltung von Relais	87
4.2.2	Zweikanalige Ausgabe mit Halbleitern	88
4.2.3	Kombination von High-Side- und Low-Side-Switch	90
4.2.4	Fail-Safe-Einheit	91
4.2.5	Kombinierte Ein-/Ausgabe-Einheiten (Zuhaltungen)	92
4.3	Logikeinheiten	93
4.3.1	Standardsicherheitsfunktionen von Logikeinheiten	93
4.3.2	Zentralprozessor mit Watchdog	94
4.3.3	Pfadkontrolle durch diversitäre Einheit	95
4.3.4	Einkanalgige Struktur mit Softwarediversität	96
4.3.5	Sicherheitsüberwachung	97
4.3.6	Zweikanaligkeit mit homogener Redundanz	100
4.3.7	Zweikanaligkeit mit diversitärer Redundanz	100
4.3.8	Mehrkanaligkeit	102
4.4	Kombination von Einheiten zu einem Gesamtsystem	103
4.4.1	Gesamtsysteme	103
4.4.2	Gesamtmaschinen und Anlagen	105
4.5	Übersicht und Bewertung	106

4.6	Wechselwirkung zwischen Standardeinheiten und Sicherheitssystemen	110
4.7	Online-Tests und Offline-Tests	112
5	Bussysteme	114
5.1	Entwicklung sicherer Netzwerke	114
5.2	Vergleich zum Standard	115
5.3	Wirkungsbereich	115
5.4	Systematische Fehler	116
5.5	Maßnahmen zur Erkennung systematischer Fehler	118
5.6	Sporadische Fehler	121
5.7	Typische sichere Datenformate	126
5.8	Nachweis der Sicherheit	128
5.9	Integration des sicheren Netzwerkes in die Automatisierungsstruktur	131
5.10	PROFIsafe	132
5.10.1	Verwendung des „Black Channels“	132
5.10.2	Referenz zum ISO/OSI-Modell	133
5.10.3	Maßnahmen gegen Übertragungsfehler	134
5.10.4	Sicherheitsgerichtete Datenstruktur	134
5.11	Interbus-Safety	135
5.11.1	Summenrahmenprotokoll	135
5.11.2	Sicherheits-Layer	136
5.12	Ethernet-Powerlink-Safety	137
5.12.1	Kommunikationsbeziehungen	138
5.12.2	Eigenschaften	138
5.12.3	Nachrichtenformat für höchste Sicherheitsanforderungen	138
5.12.4	Zeitsynchronisation	139
5.12.5	Datenformat	139
5.13	CANopen-Safety	140
5.13.1	Der CAN-Bus als Basis	140
5.13.2	CANopen als höheres Protokoll	141
5.13.3	CANopen-Safety als Protokollerweiterung	141
5.13.4	Übertragungsspezifische Hardwarestruktur der Busteilnehmer	142
5.13.5	Sicherheitsgerichtete Telegrammstruktur	143
5.13.6	Qualitative Maßnahmen gegen Übertragungsfehler	143
5.13.7	Fehlerrestwahrscheinlichkeit	145
5.14	AS-i Safety	145
5.14.1	Standard-System	145
5.14.2	Sicherer Datenverkehr	146
5.14.3	Sicherheitsgerichtete Telegrammstruktur	148
5.15	Vergleich einiger sicherheitsrelevanter Netzwerke	149

6	Antriebstechnik	150
6.1	Sicherheitsfunktionen	150
6.1.1	Arbeitssicherheit einer Maschine	150
6.1.2	Sicheres Stillsetzen	151
6.1.3	Schutz gegen unerwarteten Anlauf	151
6.1.4	Sicher reduzierte Geschwindigkeit	155
6.1.5	Sicher begrenzter Weg	155
6.1.6	Sicher begrenzte Kraft	156
6.1.7	Sichere Tipp-Schaltung	156
6.2	Technische Realisierung sicherer Antriebsfunktionen	157
6.2.1	Abschaltung über elektromechanische Elemente	157
6.2.2	Elektronische Abschalttechniken	159
6.2.3	Zweikanalige Lösungen	162
6.3	Versagen der Leistungshalbleiter	164
6.4	Betrieb gekoppelter Antriebe	165
7	Software	168
7.1	V-Modell	168
7.2	Fehlerverteilung auf den Lebenszyklus	170
7.3	Ursachen der Fehlerentstehung	171
7.3.1	Erfahrungen	172
7.3.2	Umweltbedingungen der Software	172
7.3.3	Sicherheitsanforderungsspezifikation (SRS)	173
7.3.4	Werkzeuge (Toolchain)	173
7.3.5	Validierung und Verifizierung	174
7.4	Reviews	175
7.4.1	Fagan-Inspektion	176
7.4.2	Walkthroughs	176
7.5	Softwaretest	177
7.5.1	White Box Test	177
7.5.2	Black Box Test	177
7.5.3	Testabdeckungen	178
7.5.4	Softwaremetriken	181
7.5.5	Software Zuverlässigkeits-Modelle	182
7.5.6	Von Metriken zu Modellen	184
7.5.7	Einbindung der Testabdeckung in die Zuverlässigkeitsrechnung	188
7.5.8	Softwarealterung	189
7.6	Sichere Applikationsprogrammierung und Parametrierung	190
7.6.1	Parametrierung	191
7.6.2	Sichere Programmierung von Applikationssoftware	193
7.6.3	Softwareerstellung	197

8	Test von elektronischen Komponenten und Systemen	203
8.1	Speichertests	203
8.1.1	Test variabler Speicher	203
8.1.2	Test invarianter Speicher	212
8.2	CPU-Test	215
8.2.1	Fehlermodell ein Prozessors	216
8.2.2	Implementierungshinweise	225
9	Statistische Tests	226
9.1	Stichprobenauswertung	226
9.1.1	Häufigkeit und Mittelwert	226
9.1.2	Streuung und Varianz	227
9.1.3	Normalverteilung, Gaußverteilung	228
9.1.4	Binomialverteilung	229
9.1.5	Poisson-Verteilung	230
9.2	Lebensdauerbestimmung, MTBF-Werte	231
9.2.1	Weibull-Verteilung	231
9.2.2	MTBF- und λ -Bestimmung	233
10	Mechanische Komponenten in Sicherheitssystemen	235
10.1	Lebensdauer und statistische Größen	235
10.2	Konstruktive Maßnahmen	236
10.3	Sicherheitsarchitekturen und Kenngrößen	237
10.4	Anforderungen an mechanische Komponenten (Beispiel Hydraulikventil)	239
10.4.1	Auslegung der Rückstellfeder	239
10.4.2	Verschmutzung	240
10.4.3	Lebensdauerbestimmung	240
11	Unfallursachen	242
12	Applikationen	245
12.1	Etikettiermaschine	245
12.2	Fluchtwege für den Brandfall	251
12.3	Sicherheitsfunktionen im Fertigungsprozess	254
12.3.1	Not-Aus bei Transportbändern	255
12.3.2	Verwendung von Lichtgittern	256
12.3.3	Zweihandbedienung	257
12.4	Personentransport, Automotive, Avionik	259
12.5	Arbeiten mit Service-Robotern	262
12.6	Umrüstung von Altmaschinen	265

13 Normen und Standards	270
13.1 Historie	271
13.1.1 Gefahren- und Risikoanalyse	272
13.1.2 DIN 31000, DIN V 19250 und DIN V 19251	272
13.1.3 Maschinensicherheit	273
13.1.4 DIN V VDE 0801	274
13.1.5 Europäische Maschinen-Richtlinie (MRL)	274
13.1.6 IEC 61508 und IEC 61511	275
13.1.7 EN 62061 und DIN EN ISO 13849	275
13.2 Die Sicherheitsnorm IEC 61508	276
13.2.1 Lebenszyklusmodell innerhalb der Norm	277
13.2.2 Harmonisierung mit EN 954-1	279
13.2.3 FMEA und Qualitätssicherung	280
13.3 Übersicht der wichtigsten Normen	281
13.3.1 Klima- und Umweltaanforderungen	281
13.3.2 EMV	285
13.3.3 Kerntechnik	288
13.3.4 Messen, Steuern, Regeln	288
13.3.5 Speicherprogrammierbare Steuerungen	289
13.3.6 Explosionsschutz	290
Begriffe der Sicherheitstechnik	291
Die CD-ROM zu diesem Buch	307
Programmierung und Simulation	307
Literaturangaben und Hinweise	309
Abbildungsverzeichnis und Hinweise	315
Stichwortregister	323