

Inhaltsverzeichnis

Zu diesem Buch	V
Vorwort	XI
1 Einführung	1
1.1 Historie und Stand der Sicherheitstechnik	1
2 Grundüberlegungen zur Maschinensicherheit	7
2.1 Ermittlung von Risiko und Restrisiko	8
2.2 Auswahl von Schutzmaßnahmen	10
2.2.1 Grundsätzliche Überlegungen	10
2.2.2 Lebenszyklen	12
2.3 Hierarchie der Maßnahmen	13
2.4 Umgehung von Schutzmaßnahmen	15
3 Richtlinien, Gesetze, Normen	17
3.1 Allgemeines zu Richtlinien, Gesetzen, Normen	17
3.1.1 Grundlage der Gesetzgebung in verschiedenen Ländern	17
3.1.2 Gesetze und Richtlinien	17
3.1.3 Normen	18
3.1.3.1 A-Normen	18
3.1.3.2 B-Normen	18
3.1.3.3 Maschinenspezifische C-Normen	21
3.1.4 Maschinenrichtlinie, CE-Kennzeichnung	23
3.1.5 Artikel der Maschinenrichtlinie	24
3.1.5.1 Artikel 1: Anwendungsbereich	25
3.1.5.2 Artikel 2: Begriffsbestimmungen	25
3.1.5.3 Artikel 4: Marktaufsicht	25
3.1.5.4 Artikel 5: Inverkehrbringen	25
3.1.5.5 Artikel 7: Konformitätsvermutung und harmonisierte Normen	26
3.1.5.6 Weitere Artikel	27
3.2 Anhänge der Maschinenrichtlinie	27
4 Risikobeurteilung	29
4.1 Grundsätzliches zur Risikobeurteilung im Maschinenbau	29
4.2 Durchführung der Risikobeurteilung	30
4.2.1 Risikoanalyse	31
4.2.1.1 Gefährdungen	32
4.2.1.2 Lebensphasen	34
4.2.1.3 Risiken	35
4.2.1.4 Maßnahmen	36
4.3 Dokumentation der Risikobeurteilung	38

5	Organisatorische Aspekte	41
6	Beispiel: Konformitätsbewertungsverfahren und Risikobeurteilung	43
6.1	Konformitätsbewertungsverfahren	43
6.2	Risikobeurteilung	47
6.2.1	Grundkonzept der Maschine	48
6.2.2	Ermittlung der Gefährdungen	49
6.2.3	Mechanische Gefährdungen	50
6.2.3.1	Lebensphase Betrieb	51
6.2.3.2	Weitere Lebensphasen	54
6.2.4	Elektrische Gefährdungen	57
6.2.5	Thermische Gefährdungen	58
6.2.6	Gefährdungen durch Lärm	60
6.2.7	Gefährdungen durch Schwingungen	60
6.2.8	Gefährdungen durch Strahlung	61
6.2.9	Gefährdungen durch Materialien und Substanzen	62
6.2.10	Gefährdungen in Zusammenhang mit der Ergonomie	62
6.2.11	Gefährdungen durch die Einsatzumgebung der Maschine	62
6.2.12	Weitere Gefährdungen	63
6.2.13	Veränderungen des Konzepts	64
7	Einstufung des Risikos nach Norm	67
7.1	Das Verfahren der Beurteilung des Risikos mithilfe von Risikografen	67
7.2	Weitere wichtige Risikografen	70
7.2.1	Risikograf nach den Normen IEC 61508 und IEC 61511	70
7.2.2	Risikobeurteilung nach der Norm DIN EN IEC 62061	71
7.2.3	EN 954 und Vergleich der Bewertungen	73
7.2.4	Kategorien innerhalb der Normen EN 954 und DIN EN 13849	74
7.3	Ableitung der notwendigen Maßnahmen aus der Bewertung	76
8	Kenngrößen eines Sicherheitssystems	79
8.1	Quantifizierung der Sicherheit	79
8.2	Quantitative Kenngrößen	81
8.2.1	Die Struktur des Sicherheitssystems	83
8.2.2	Die Ausfallrate oder die Lebensdauer	85
8.2.3	Der Diagnosedeckungsgrad	88
8.2.4	Fehler gemeinsamer Ursache	90
8.3	Aufteilung in Systeme, Einheiten und Komponenten	91
8.4	Darstellung als Block-Diagramm	94
9	Berechnungsmethoden	99
9.1	Sichere Auslegung einer Krananlage	99
9.1.1	Technische Ausführung der Krananlage	99
9.1.2	Die Sicherheitskomponenten der Anlage	100
9.2	Entwurf einer geeigneten Block-Struktur	103
9.3	Beherrschung eines Überlastfehlers	104

9.4	Nachweis der Eignung durch Berechnung	106
9.4.1	Auffinden der Ausfallraten	106
9.4.2	Auffinden der DC-Werte	111
9.4.3	Berechnung im Detail	112
9.4.4	Berechnung mit einer Tabellenkalkulation	113
9.4.5	Verwendung von SISTEMA zur Berechnung	115
9.4.6	Bestimmung des Anteils für Fehler gemeinsamer Ursache	116
9.4.7	Ermittlung weiterer Kenngrößen der Sicherheit	117
9.4.8	Optimierung der Lösung	119
9.5	Abschaltung am Hubwende	121
9.6	Verwendung von Standard-Komponenten	123
9.7	FMEA und FTA	124
10	Hydraulik und Pneumatik	127
10.1	Maschinenfunktion mit pneumatischen Einheiten	127
10.2	Aufbau der Maschine und Druckerzeugung	128
10.3	Realisierte technische Lösung	128
10.4	Nachweis der Eignung nach DIN EN ISO 13849	130
10.4.1	Umsetzung in ein Sicherheitsblockschaltbild	130
10.4.2	Bewertung nach Norm	133
10.5	Sicherheitstechnische Verbesserung	136
10.6	Berechnung der zweikanaligen Lösung	138
11	Verwendung sicherer Antriebe	141
11.1	Wirkung sicherer Antriebe	141
11.2	Erfüllung der Anforderungen aus der MRL und den Normen	141
11.2.1	Sicheres Stillsetzen	142
11.2.2	Schutz gegen unerwarteten Anlauf	142
11.3	Die Funktion STO (Safe Torque Off)	143
11.4	Die Funktion SS1 (Safe Stop 1)	145
11.5	Technische Realisierungsprinzipien für STO und SS1	145
11.5.1	Unterbrechung der Kommutierung	146
11.5.2	Verwendung eines Sicherheitsgeräts	147
11.5.3	Verwendung einer speicherprogrammierbaren Steuerung	150
11.6	Weitergehende Sicherheitsfunktionen von Antrieben	154
12	Erstellung von sicherheitsrelevanter Steuerungssoftware	159
12.1	Systematische Fehler	160
12.2	Sicherheitsbezogene Software Spezifikation	161
12.2.1	Aufbau einer Beispieldapplikation	162
12.3	Formulierung der Sicherheitsanforderungen	164
12.3.1	Sicherheitsfachsprache	165
12.3.2	Formular für Anforderungen	166
12.3.3	Definition der Sicherheitsanforderungen	166
12.3.4	Verwendung von Prioritäten	169
12.4	Sicherheitsarchitektur	169

12.4.1	Aufbau einer Softwaresicherheitsarchitektur entsprechend der Beispieldapplikation	170
12.5	Moduldesign	173
12.5.1	Semi-formale Methoden.....	173
12.5.2	Anwendung einer semi-formalen Beschreibung	174
12.5.3	Beschreibung der Module aus der Beispieldapplikation.....	177
12.6	Codierung	182
12.6.1	Umgang und Verwendung von Passwörtern.....	185
12.6.2	Arten der Kontaktaufnahme zwischen Programmiersystem und Steuerung	185
12.7	Verifizieren und Validieren	189
12.8	Test der Module	190
12.8.1	Modultestbeispiel.....	190
12.9	Integrationstest	193
12.9.1	Erfassung der Reaktionszeiten	193
12.9.2	Beispiel einer Integrationstestspezifikation	195
12.10	Validierung der Sicherheitsspezifikation	196
12.11	Weitere Anforderungen an das Software-Sicherheitsmanagement	197
13	Mathematische Formeln.....	199
14	Zuordnung SIL-Werte, HFT und Ausfallraten	201
15	Begriffe und Abkürzungen	203
16	Literaturangaben.....	207
17	Stichwortverzeichnis	209