

Inhalt

Vorwort	7	Weitere Richtlinien	21
		Niederspannungsrichtlinie 2006/95/EG	22
		EMV-Richtlinie 2004/108/EG	22
		ATEX-Produktrichtlinie 94/9/EG	22
		Druckgeräterichtlinie 97/23/EG	22
		Richtlinie über einfache Druckbehälter 2009/105/EG	23
Teil A: Grundlagen der Maschinensicherheit – Gesetzliche und normative Anforderungen	11		
A-1 Europäische Richtlinien und nationale Gesetze	13	A-2 Basisnormen zur funktionalen Sicherheit	25
Richtlinien	14	Aufbau internationaler Normen zur Maschinensicherheit	25
Nationale Gesetze und Verordnungen	14	Normungsorganisationen	26
Normen	14	Vermutungswirkung durch harmonisierte Normen	27
Anforderungen aus der Maschinenrichtlinie und der Arbeitsmittelbenutzungsrichtlinie	14	Berücksichtigung von Ausfallwahrscheinlichkeiten	27
Anwendungsbereich der Maschinenrichtlinie	15	Normen zur funktionalen Sicherheit	27
Mit der Maschinenrichtlinie zur Konformitätserklärung	15	ISO 12100	28
Wofür steht die CE-Kennzeichnung?	16	IEC 61508	28
Umsetzung der Maschinenrichtlinie bei Maschinen	17	IEC 61800-5-2	28
Definition	17	IEC 60204-1	28
Umsetzung	17	IEC 62061	29
Mitgelieferte Dokumentation	17	ISO 13849 (Nachfolger der EN 954-1)	29
CE-Kennzeichnung	17	Historie der Normen zur funktionalen Sicherheit	29
Umsetzung der Maschinenrichtlinie bei unvollständigen Maschinen	19	Funktionale Sicherheit – Anwendungsbereich der ISO 13849	29
Definition	19	Eine Steuerung, mehrere Normen	30
Umsetzung	19	Globale Märkte und lokale Vorschriften	31
Mitgelieferte Dokumentation	19		
CE-Kennzeichnung	19	Teil B: 10 Schritte zum Performance Level	33
Umsetzung der Maschinenrichtlinie bei Sicherheitsbauteilen	20	B-1 Risikobeurteilung	35
Definition	20	Grundlagen	35
„Sicherheitsbauteile“ versus „sicherheitsbezogene Teile“	20	Risikobeurteilung als Grundlage für die Maschinensicherheit	35
Umsetzung	20	Risikobeurteilung nach Normen	37
Mitgelieferte Dokumentation	20	Vorgehen	37
CE-Kennzeichnung	20	Beispiel	47
Wesentliche Veränderungen von Maschinen	20	Dokumente für die Validierung	49
Definition	20		
Umsetzung	21		
Neue Dokumentation	21		
CE-Kennzeichnung	21		

B-2 Identifikation der Sicherheitsfunktionen	51	B-6 Fehler und Diagnose	89
Grundlagen	51	Grundlagen	89
Sicherheitsfunktionen	51	Berücksichtigung von Fehlern (Fehlerliste)	89
Vorgehen	52	Fehlerausschluss	91
Bestimmen der Sicherheitsfunktionen	52	Diagnosedeckungsgrad (DC)	91
Festlegen der sicherheitstechnischen Eigenschaften der Sicherheitsfunktionen	52	Vorgehen	95
Varianten der Sicherheitsfunktionen	55	Beispiel	95
Teilsicherheitsfunktionen von elektrischen Antriebssystemen gemäß IEC 61800-5-2	56	Fehlerliste	95
Beispiel	60	Bestimmung des Diagnosedeckungsgrads (DC) der Komponenten	98
Dokumente für die Validierung	61	Berechnung des DC_{avg}	98
<hr/>		Dokumente für die Validierung	98
B-3 Bestimmung des PL_r	63	B-7 Bestimmung des PL	99
Grundlagen	63	Grundlagen	99
Wahl des Verfahrens	64	Zuverlässigkeit ($MTTF_d$, B_{10d})	101
Bestimmung des PL_r nach ISO 13849	64	Bestimmung des Performance Levels ($PL_{SRP/CSI}$)	102
Bestimmung des PL_r in Anlehnung an IEC 62061	65	Vorgehen	104
Vorgehen	65	Beispiel	105
Beispiel	68	Subsystem 1: $SRP/CS_{Kat3/4}$	105
Identifikation der Sicherheitsfunktion	68	Subsystem 2: SRP/CS_{zert}	108
Festlegung des PL_r	68	Ermittlung des PL_{SF}	108
Vergleich mit dem Verfahren der ISO 13849	68	Anpassung der PL_{SF}	108
Dokumente für die Validierung	69	Dokumente für die Validierung	109
<hr/>		<hr/>	
B-4 Auswahl der Kategorie	71	B-8 Bewertung der Robustheit der Steuerung – Fehlervermeidung	111
Grundlagen	71	Grundlagen	111
Beziehung zwischen Performance Level und Kategorie	71	Maßnahmen gegen Fehler gemeinsamer Ursache (CCF)	111
Freie Wahl der Kategorie	72	Grundlegende und bewährte Sicherheitsprinzipien	113
Rekursiver Vorgang	73	Bewährte Bauteile	116
Eigenschaften der Kategorien	73	Systematische Fehler	117
Vorgehen	75	Vorgehen	119
Beispiel	76	Beispiel	120
Dokumente für die Validierung	77	Beispiel 1: Maßnahmen gegen CCF	120
<hr/>		Beispiel 2: Sicherheitsprinzipien	121
B-5 Modellierung des Block-Diagramms	79	Dokumente für die Validierung	123
Grundlagen	79	<hr/>	
Analyse	79	B-9 Software-Anforderungen	125
Prinzipien der Modellierung	80	Grundlagen	125
Unterteilung in Subsysteme	80	Softwarebasierende Parametrisierung	126
Vorgehen	81	Sicherheitsbezogene Anwendersoftware (SRASW)	126
Beispiel	84	Sicherheitsbezogene Embedded Software (SRESW)	127
Beschreibung der Komponenten des SRP/CS	84	Vorgehen	127
Eigenschaften der Sicherheitsfunktion	85	Projektunabhängige Vorbereitungen	128
Dokumente für die Validierung	87	Projektspezifische Tätigkeiten für SRASW	128

Beispiel	132	2. Schritt: Identifikation der Sicherheitsfunktionen	209
Erstellung und Überprüfung der Software-Spezifikation	132	3. Schritt: Bestimmung des PL_r	211
Auswahl der Werkzeuge	133	4. Schritt: Auswahl der Kategorie	211
Entwurf der Software	135	5. Schritt: Modellierung des Blockdiagramms	211
Kombination sicherheitsbezogener und Standard-Programme	135	6. Schritt: Fehler und Diagnose	215
Codierung der Software	136	7. Schritt: Bestimmung des PL_{SF}	217
Test	136	8. Schritt: Bewertung der Robustheit	219
Dokumente für die Validierung	138	9. Schritt: Software-Anforderungen	225
		10. Schritt: Verifizieren und Validieren	225
B-10 Verifizieren und Validieren	139	Teil D: Anhang	227
Grundlagen	139	D-1 ISO 13849: Maschinensicherheit hängt von Zuverlässigkeit ab	229
Validierungsplan	141	Übersicht	229
Dokumentation des Validierungsprozesses	141	Grundlage der Zuverlässigkeit	229
Validierung durch Analyse	142	Badewannenkurve	229
Validierung durch Prüfung	142	Kennwerte der Zuverlässigkeit	230
Vorgehen	143	Grundlage der statistisch basierten Sicherheitstechnik	231
Dokumente für die Validierung	145	Zustandsdiagramm	231
Checkliste „Validierung“	145	Kennwerte der statistisch basierten Sicherheitstechnik	232
Erläuterung	145	Risikobeurteilung, Sicherheitsfunktion, Performance Level (PL)	233
Teil C: Anwendungsbeispiele	151	Anwendbarkeit einer Komponente für die funktionale Sicherheit	233
C-1 Beispiel: Werkzeugmaschine	153	Methoden zur Ermittlung der Zuverlässigkeitskennwerte	234
Maschinenbeschreibung	154	Berechnungen der Lebensdauer elektronischer Komponenten	235
1. Schritt: Risikobeurteilung	155	Erprobungen der Lebensdauer	235
2. Schritt: Identifikation der Sicherheitsfunktionen	155	Lebensdauerauswertungen von Felddaten	237
3. Schritt: Bestimmung des PL_r	162	Ausfallwahrscheinlichkeit einer Sicherheitsfunktion	237
4. Schritt: Auswahl der Kategorie	163	Zuverlässigkeitsmodell: Block-Diagramm	237
5. Schritt: Modellierung des Blockdiagramms	164	Bedeutung des $MTTF_d$ -Wertes für die Sicherheitsfunktion	238
6. Schritt: Fehler und Diagnose	167	Berechnung der gefahrbringenden Ausfallwahrscheinlichkeit (PFH_D)	239
7. Schritt: Bestimmung des PL_{SF}	170	Beispiel von sicherheitstechnischen Kennwerten	239
8. Schritt: Bewertung der Robustheit	173	Fazit	240
9. Schritt: Software-Anforderungen	179	D-2 Begriffe, Formelzeichen und Abkürzungen	241
10. Schritt: Verifizieren und Validieren	188	D-3 Literaturverzeichnis	255
C-2 Beispiel: Werkzeugmaschine, pneumatisches Subsystem	191	Im Buch verwendete Quellen	255
1. bis 3. Schritt zum PL	191	Weiterführende Literatur	257
4. Schritt: Auswahl der Kategorie	191	D-4 Stichwortverzeichnis	259
5. Schritt: Modellierung des Blockdiagramms	191		
6. Schritt: Fehler und Diagnose	193		
7. Schritt: Bestimmung des PL_{SF}	196		
8. Schritt: Bewertung der Robustheit	199		
9. Schritt: Software-Anforderungen	206		
10. Schritt: Verifizieren und Validieren	206		
C-3 Beispiel: Spritzgießmaschine	207		
Maschinenbeschreibung	207		
1. Schritt: Risikobeurteilung	208		