

Inhalt

Vorwort	5
1 Der Ursprung der DIN EN 62061 (VDE 0113-50) – darum musste sich etwas ändern	15
1.1 Die EG-Maschinenrichtlinie und ihre Folgen	15
1.2 Geschichte der DIN EN 954-1 – eine Norm mit Grenzen	17
1.3 Die DIN EN 61508-1 (VDE 0803-1):2002-11 als Grundlage zur Bewertung von elektrischen/elektronischen/programmierbaren Lösungen	18
1.4 European Project STSARCES – die EU macht Druck	19
1.5 Die Welt der Theorie und der Praxis – eine Anwendernorm ist notwendig	22
1.6 Der Anwender muss umdenken – was hindert ihn daran?	23
1.7 Zusammenführung der DIN EN 62061 (VDE 0113-50) und DIN EN ISO 13849-1 – längst überfällig	24
2 Moderne Maschinensicherheit – das europäische Referenzmodell und die Richtlinien	27
2.1 Das europäische Regelwerk	28
2.2 Warum grundlegende Sicherheitsanforderungen?	29
2.2.1 Wie war das noch mal mit der Haftung?	30
2.2.2 Was möchte die europäische Kommission?	31
2.2.3 Liste der grundlegenden Sicherheits- und Gesundheitsanforderungen	35
2.3 Haftung – Motivation der Maschinenhersteller	46
2.4 Der Anspruch der harmonisierten Normen	47
2.5 Die Organisation und das Management – warum wiederentdeckt?	50
2.6 Risikobeurteilung – immer notwendig und doch unterschätzt	51
2.7 Die Dokumentation	53
2.8 Das Ziel vor Augen – die CE-Konformitäts- oder die CE-Einbauerklärung	54
2.9 Das CE-Kennzeichen anzubringen, aber wohin damit?	55
2.10 Der Prozess im Überblick	57
2.11 Wesentliche Veränderung	57
3 Der Begriff Sicherheitsfunktion – was ist wahr?	61
3.1 Woher kommt der Begriff eigentlich?	61

3.2	Was muss ich berücksichtigen?	63
3.3	Wege aus der Krise	65
3.4	Der Streit um die Grenzen der Sicherheitsfunktion.	66
3.5	Was sind keine Sicherheitsfunktionen und werden es auch nie sein? ...	67
4	Sicherheitsfunktionen und Funktionale Sicherheit – eine sinnvolle Kombination?	71
4.1	Ist Funktionale Sicherheit etwas Neues?	71
4.2	Warum soll Funktionale Sicherheit dem Anwender helfen?	73
4.3	Was keine Funktionale Sicherheit sein kann	73
4.4	Daten und Fakten.	75
4.5	Die Geschichte des Sicherheitsbauteils – was wurde früher dazu gesagt?	76
4.6	Worin liegt der Unterschied zwischen Sicherheitsbauteil und Sicherheitsfunktion?	78
4.7	Was kein Sicherheitsbauteil sein kann, es sei denn ...	81
4.8	Verantwortlichkeiten – nicht alles, was glänzt und gelb ist, macht auch automatisch sicher	83
5	Die Anwendernorm DIN EN 62061 (VDE 0113-50), in Verbindung mit DIN EN ISO 13849-1	87
5.1	Welche Norm ist anzuwenden: DIN EN ISO 13849-1 oder DIN EN 62061 (VDE 0113-50)?	87
5.2	Die Zielsetzung	90
5.3	Der Anwendungsbereich	93
5.4	Begriffe und Abkürzungen.	96
5.5	Abkürzungen	101
5.6	Der Begriff Ausfallrate	101
5.7	Plan der Funktionalen Sicherheit – unterschätzt und doch so wertvoll	104
5.8	Spezifikation der Anforderungen für sicherheitsbezogene Steuerungsfunktionen	106
5.8.1	Spezifikation der funktionalen Anforderungen für sicherheitsbezogene Steuerungsfunktionen	107
5.8.2	Spezifikation der Anforderungen zur Sicherheitsintegrität für sicherheitsbezogene Steuerungsfunktionen	108
5.9	Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	109
5.9.1	Vergleich zu DIN EN ISO 13849-1	109
5.9.2	Allgemeine Anforderungen	110

5.9.3	Anforderungen zum Verhalten bei Erkennung eines Fehlers	111
5.9.4	Anforderungen zur systematischen Sicherheitsintegrität	113
5.10	Entwurf des sicherheitsbezogenen elektrischen Steuerungssystems . . .	115
5.10.1	Entwurf der Systemarchitektur	118
5.10.2	Entwurf des Teilsystems (en: subsystem)	120
5.10.3	Entwurf des Teilsystemelements (en: subsystem element)	121
5.10.4	Ein exemplarisches System	122
5.10.5	Bestimmung des erreichten Sicherheitsintegritätslevels (SIL) oder Performance Level (PL)	124
5.11	Realisierung von Teilsystemen (und SRP/CS)	127
5.11.1	Anforderungen für den Entwurf	127
5.11.2	Sicherheitsparameter des Teilsystems	128
5.11.3	Auswahl geeigneter Komponenten und Geräte	129
5.11.4	Bestimmung der sicherheitsbezogenen Leistungsfähigkeit des Teilsystems	129
5.11.5	Strukturelle Einschränkungen der Sicherheitsintegrität der Hardware von Teilsystemen	130
5.11.6	Abschätzung des Anteils sicherer Ausfälle (<i>SFF</i>)	132
5.11.7	Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen	134
5.12	Abschätzung der Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen	136
5.12.1	Empfehlung B_{10} -Werte unter Standardbedingungen, Siemens AG . . .	137
5.12.2	Empfehlung B_{10D} - und $MTTF_D$ -Werte nach DIN EN ISO 13849-1 . . .	139
5.12.3	Basis-Teilsystemarchitekturen A bis D	141
5.13	Bestimmung des erforderlichen Sicherheitsintegritätslevels SIL – was will ich eigentlich?	151
5.14	Faktor der Ausfälle infolge gemeinsamer Ursache β (CCF-Faktor) . . .	155
5.15	Benutzerinformationen des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	159
5.16	Validierung des Steuerungssystems	160
5.17	Modifikation	161
5.18	Dokumentation eines SRECS	162
5.19	Leitfaden für den Entwurf eines sicherheitsbezogenen Steuerungssystems (SRECS)	164
5.20	Ein Beispiel zur praktischen Vorgehensweise	166
5.21	Vereinfachte Vorgehensweis mit B_{10D} , $MTTF_D$ und erreichbarer PFH_D	177
5.21.1	Beispiel mit der vereinfachten Vorgehensweise	180
5.22	Zusammenfassung – Schritt für Schritt	182

6	Das VDMA-Einheitsblatt 66413	185
6.1	Motivation der Komponentenhersteller und Maschinenhersteller	185
6.2	Warum erst jetzt? – ein Erklärungsversuch	186
6.3	Gerätetypen – ohne sie geht nichts mehr heute	186
6.4	Kennwerte auf Basis der Gerätetypen – Schluss mit den Diskussionen	190
6.5	Anwendung der Gerätetypen – die Praxis ist maßgebend	191
6.5.1	Anwendung Gerätetyp 1	191
6.5.2	Anwendung Gerätetyp 2	192
6.5.3	Anwendung Gerätetyp 3	194
6.5.4	Anwendung Gerätetyp 4	196
6.6	Austausch elektronischer Daten für alle lesbar – XML soll helfen	197
6.7	Erläuterungen zu einigen wichtigen Kennwerten	198
7	Typische grundlegende Architekturen	203
7.1	Architekturen im Überblick	203
7.2	Diagnosedeckungsgrad (DC)	204
7.3	Einkanalig ohne Testung	208
7.4	Einkanalig mit Testung	209
7.5	Zweikanalig ohne Testung	212
7.6	Zweikanalig mit geringer bis mittlerer Testung	213
7.7	Zweikanalig mit hoher Testung	216
8	Tipps und Beispiele	219
8.1	Liste oft verwendeter Sicherheitsfunktionen	219
8.2	Allgemeine Betrachtungen	220
8.2.1	Definieren einer Sicherheitsfunktion einfach gemacht	220
8.2.2	Warum darf man mit der DIN EN 62061 (VDE 0113-50) „nicht elektromechanische Komponenten“ (z. B. Ventile) berechnen?	222
8.2.3	Was tun mit den Kategorien der C-Normen?	223
8.2.4	Die Berechnungsmethode der DIN EN 62061 (VDE 0113-50), Abschnitt 6.7.8.2 ist „normativ“, warum ist die der DIN EN ISO 13849-1, Anhänge C und K dagegen nur „informativ“?	224
8.2.5	$MTTF_D$ -Wert gleich PFH_D -Wert	228
8.2.6	Verschleißbehaftete Komponenten und die Kategorie 2	229
8.2.7	Was bedeutet T_1 als Proof-Test oder Lebensdauer in der Praxis?	231
8.2.8	T_{10D} und T_1 , wann gilt was und warum?	233
8.2.9	Den Betätigungszyklus C (1/h) im Verhältnis zu den effektiven Betriebsstunden im Jahr umrechnen?	235
8.2.10	Bei einer einkanaligen Architektur gilt $PFH_D = (1 - DC) \cdot \lambda_D$ – Was passiert mit dem Diagnose-Testintervall T_2 ?	236

8.2.11	Welches erforderliche Testintervall ist für welchen SIL sinnvoll?	237
8.3	Grundsätzliche Betrachtungen – Sensorik.	239
8.3.1	Not-Halt-Befehlsgeräte – jedes für sich ist Teil einer entsprechenden „ergänzenden“ Sicherheitsfunktion	239
8.3.2	Verschleißbehaftete Komponenten haben keinen Anteil sicherer Ausfälle (<i>SFF</i>) – ob Sensor oder Aktor	240
8.3.3	SIL 2 in einer zweikanaligen Architektur ohne Diagnose (<i>SFF</i> = 80 %?) – bringt das etwas?	242
8.3.4	Muss ein Zustimmschalter als Teil einer Sicherheitsfunktion berücksichtigt werden?	243
8.3.5	PL e oder SIL 3 mit einem Positionsschalter mit getrenntem Betätiger?	244
8.3.6	Drehzahlüberwachung – wann dürfen die Geber außer Acht gelassen werden?	246
8.3.7	Stromwertüberwachung eines Motors in SIL 2	247
8.4	Grundsätzliche Betrachtungen – Aktorik.	250
8.4.1	Muss ein Antrieb (Motor) in einer Sicherheitsfunktion berücksichtigt werden?	250
8.4.2	Zwei Lastschütze an einem einzelnen sicherheitsgerichteten Ausgang mit SIL 3	251
8.4.3	Zwangsgeführte Kontaktelemente von Hilfsschützen und Spiegelkontakte von Leistungsschützen	251
8.4.4	Ist eine Überwachung von Hilfs- oder Leistungsschützen durch nicht sicherheitsgerichtete Eingangsbaugruppen möglich?	254
8.4.5	Welcher PL oder SIL kann mit einem einzelnen Leistungsschütz erreicht werden?	255
8.4.6	Bewerten von „Standard-Ausgangsbaugruppen“	256
8.4.7	Bewertung von Hilfsschützen oder Koppelrelais in einer Sicherheitsfunktion	259
8.4.8	Stern-Dreieck-Schaltung sicherheitsgerichtet bewerten	262
8.4.9	Lastfreies Schalten mit Leistungsschützen oder Hilfsschützen	264
8.4.10	Was tun, wenn keine $MTTF_D$ -Werte vorliegen?	264
9	Berechnungen von typischen Sicherheitsfunktionen	267
9.1	Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine beweglich trennende Schutzeinrichtung (Schutztür, -klappe, ...)	269
9.2	Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine nicht trennende Schutzeinrichtung (Lichtvorhänge, Laserscanner, ...)	277
9.3	Handbetätigte Befehlsrichtungen (Handsteuerung)	279

9.4	Zweihandschaltung	281
9.5	Manuelles Aufheben von Sicherheitsfunktionen	283
9.6	Einrichten, Teachen, Umrüsten, die Fehlersuche sowie für Reinigungs- oder Instandhaltungsarbeiten	285
9.7	Sichere Bewegungen	287
9.8	Sichere Positionserfassung	289
9.9	Auswahl von Steuerungs- und Betriebsarten	292
9.10	Zuhaltung einer Schutzeinrichtung	294
9.11	Funktion zum Stillsetzen im Notfall	297
9.12	SIL 1 und SIL 2 gleich SIL 3	304
10	Mal kritisch hinterfragt	309
10.1	Die Not-Halt-Funktion sinnvoll bewerten	309
10.2	Betriebsarten	314
10.3	Die Zuhaltung einer Verriegelungsreinrichtung berücksichtigen	319
10.4	Nicht alles muss berechnet werden	321
10.5	Nur sinnvolle Diagnosedeckungsgrade verwenden	323
10.6	„Standard“-Komponenten mit Vorsicht wählen	325
10.7	Ein Vergleich mit dem Anhang K der DIN EN ISO 13849-1 lohnt sich	327
10.8	Die Einstufung des Risikos einmal anders vornehmen	332
10.9	Den Prozess als Hilfsmittel nutzen	334
11	Die Mathematik und das warum	335
11.1	Definition der Wahrscheinlichkeit gefahrbringender Ausfälle	335
11.1.1	Teilsystemelemente und Teilsysteme	335
11.1.2	Ausfallraten	335
11.1.3	Definition des PFH_D	336
11.2	Einkanalige Architektur	336
11.2.1	Annahmen	336
11.2.2	Logische Darstellung	336
11.2.3	Wahrscheinlichkeits-Blockdiagramm	337
11.2.4	Berechnung	338
11.2.5	PFH_D der Teilsystemarchitektur C	338
11.3	Zweikanalige Architektur	338
11.3.1	Annahmen	338
11.3.2	Logische Darstellung	339
11.3.3	Wahrscheinlichkeits-Blockdiagramm	340
11.3.4	Berechnung	341
11.3.5	PFH_D der Teilsystemarchitektur D	343

11.4	Diskussion der Ergebnisse der einkanaligen Architektur	343
11.4.1	Diagnosedeckungsgrad 60 %	343
11.4.2	Diagnosedeckungsgrad 90 %	344
11.4.3	Schlussfolgerung	345
11.5	Diskussion der Ergebnisse der zweikanaligen Architektur	346
11.5.1	Diagnosedeckungsgrad 60 %	346
11.5.2	Diagnosedeckungsgrad 90 %	346
11.5.3	Diagnosedeckungsgrad 99 %	346
11.5.4	Schlussfolgerung	346
12	Ausblick	351
13	Terminologie	353
14	Fachwörterbuch	385
	Literatur	395
	Stichwortverzeichnis	399