

Inhalt

Vorwort	5
Vorwort zur 2. Auflage	7
1 Der Ursprung der DIN EN 62061 (VDE 0113-50) – darum musste sich etwas ändern	17
1.1 Die EG-Maschinenrichtlinie und ihre Folgen	17
1.2 Geschichte der DIN EN 954-1 – eine Norm mit Grenzen	19
1.3 Die DIN EN 61508-1 (VDE 0803-1):2011-02 als Grundlage zur Bewertung von elektrischen/elektronischen/programmierbaren Lösungen	20
1.4 European Project STSARCES – die EU macht Druck	21
1.5 Die Welt der Theorie und der Praxis – eine Anwendernorm ist notwendig	24
1.6 Der Anwender muss umdenken – was hindert ihn daran?	25
1.7 Zusammenführung der DIN EN 62061 (VDE 0113-50) und DIN EN ISO 13849-1 – längst überfällig	26
2 Moderne Maschinensicherheit – das europäische Referenzmodell und die Richtlinien	29
2.1 Das europäische Regelwerk	30
2.2 Warum grundlegende Sicherheitsanforderungen?	31
2.2.1 Wie war das noch mal mit der Haftung?	32
2.2.2 Was möchte die Europäische Kommission?	33
2.2.3 Liste der grundlegenden Sicherheits- und Gesundheitsanforderungen ..	37
2.3 Haftung – Motivation der Maschinenhersteller	48
2.4 Der Anspruch der harmonisierten Normen	49
2.5 Die Organisation und das Management – warum wiederentdeckt? ...	52
2.6 Risikobeurteilung – immer notwendig und doch unterschätzt	53
2.7 Die Dokumentation	55
2.8 Das Ziel vor Augen – die CE-Konformitäts- oder die CE-Einbauerklärung	56
2.9 Das CE-Kennzeichen anzubringen, aber wohin damit?	57
2.10 Der Prozess im Überblick	59
2.11 Wesentliche Veränderung	59

3	Der Begriff Sicherheitsfunktion – was ist wahr?	63
3.1	Woher kommt der Begriff eigentlich?	63
3.2	Was muss ich berücksichtigen?	65
3.3	Wege aus der Krise	67
3.4	Der Streit um die Grenzen der Sicherheitsfunktion.	68
3.5	Was sind keine Sicherheitsfunktionen und werden es auch nie sein? . . .	69
4	Sicherheitsfunktionen und Funktionale Sicherheit – eine sinnvolle Kombination?	75
4.1	Ist Funktionale Sicherheit etwas Neues?	75
4.2	Warum soll Funktionale Sicherheit dem Anwender helfen?	77
4.3	Was keine Funktionale Sicherheit sein kann	77
4.4	Daten und Fakten.	79
4.5	Die Geschichte des Sicherheitsbauteils – was wurde früher dazu gesagt?	80
4.6	Worin liegt der Unterschied zwischen Sicherheitsbauteil und Sicherheitsfunktion?	82
4.7	Was kein Sicherheitsbauteil sein kann, es sei denn	85
4.8	Verantwortlichkeiten – nicht alles, was glänzt und gelb ist, macht auch automatisch sicher	87
5	Die Anwendernorm DIN EN 62061 (VDE 0113-50), in Verbindung mit DIN EN ISO 13849-1	91
5.1	Welche Norm ist anzuwenden: DIN EN ISO 13849-1 oder DIN EN 62061 (VDE 0113-50)?	91
5.2	Die Zielsetzung	94
5.3	Der Anwendungsbereich	98
5.4	Begriffe und Abkürzungen.	102
5.5	Abkürzungen	110
5.6	Der Begriff Ausfallrate	110
5.7	Plan der Funktionalen Sicherheit – unterschätzt und doch so wertvoll	113
5.8	Spezifikation der Anforderungen für sicherheitsbezogene Steuerungsfunktionen	117
5.8.1	Spezifikation der funktionalen Anforderungen für sicherheitsbezogene Steuerungsfunktionen	117
5.8.2	Spezifikation der Anforderungen zur Sicherheitsintegrität für sicherheitsbezogene Steuerungsfunktionen	118
5.9	Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	120

5.9.1	Vergleich zu DIN EN ISO 13849-1	120
5.9.2	Allgemeine Anforderungen	123
5.9.3	Anforderungen zum Verhalten bei Erkennung eines Fehlers	124
5.9.4	Anforderungen zur systematischen Sicherheitsintegrität	126
5.10	Entwurf des sicherheitsbezogenen elektrischen Steuerungssystems	129
5.10.1	Entwurf der Systemarchitektur	131
5.10.2	Entwurf des Teilsystems (en: subsystem)	134
5.10.3	Entwurf des Teilsystemelements (en: subsystem element)	135
5.10.4	Ein exemplarisches System	136
5.10.5	Bestimmung des erreichten Sicherheitsintegritätslevels (SIL) oder Performance Level (PL)	138
5.11	Realisierung von Teilsystemen (und SRP/CS)	143
5.11.1	Anforderungen für den Entwurf	143
5.11.2	Sicherheitsparameter des Teilsystems	144
5.11.3	Auswahl geeigneter Komponenten und Geräte	145
5.11.4	Bestimmung der sicherheitsbezogenen Leistungsfähigkeit des Teilsystems	145
5.11.5	Strukturelle Einschränkungen der Sicherheitsintegrität der Hardware von Teilsystemen	146
5.11.6	Abschätzung des Anteils sicherer Ausfälle (<i>SFF</i>)	151
5.11.7	Anforderungen zur Wahrscheinlichkeit Gefahr bringender zufälliger Hardwareausfälle von Teilsystemen	153
5.12	Abschätzung der Wahrscheinlichkeit Gefahr bringender zufälliger Hardwareausfälle von Teilsystemen	155
5.12.1	Empfehlung B_{10} -Werte unter Standardbedingungen, Siemens AG	156
5.12.2	Empfehlung B_{10D} - und $MTTF_D$ -Werte nach DIN EN ISO 13849-1	158
5.12.3	Basis-Teilsystemarchitekturen A bis D	160
5.13	Bestimmung des erforderlichen Sicherheitsintegritätslevels SIL – was will ich eigentlich?	170
5.14	Faktor der Ausfälle infolge gemeinsamer Ursache β (CCF-Faktor)	174
5.15	Benutzerinformationen des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	178
5.16	Validierung des Steuerungssystems	179
5.17	Modifikation	180
5.18	Dokumentation eines SRECS	181
5.19	Leitfaden für den Entwurf eines sicherheitsbezogenen Steuerungssystems (SRECS)	183
5.20	Ein Beispiel zur praktischen Vorgehensweise	185
5.21	Vereinfachte Vorgehensweise mit B_{10D} , $MTTF_D$ und erreichbarer PFH_D	196

5.21.1	Beispiel mit der vereinfachten Vorgehensweise	199
5.22	Zusammenfassung – Schritt für Schritt	201
6	Das VDMA-Einheitsblatt 66413	203
6.1	Motivation der Komponentenhersteller und Maschinenhersteller.	203
6.2	Warum erst jetzt? – ein Erklärungsversuch	204
6.3	Gerätetypen – ohne sie geht nichts mehr heute	204
6.4	Kennwerte auf Basis der Gerätetypen – Schluss mit den Diskussionen	208
6.5	Anwendung der Gerätetypen – die Praxis ist maßgebend.	209
6.5.1	Anwendung Gerätetyp 1	209
6.5.2	Anwendung Gerätetyp 2	210
6.5.3	Anwendung Gerätetyp 3	212
6.5.4	Anwendung Gerätetyp 4	214
6.6	Austausch elektronischer Daten für alle lesbar – XML soll helfen.	215
6.7	Erläuterungen zu einigen wichtigen Kennwerten	216
7	Typische grundlegende Architekturen	221
7.1	Architekturen im Überblick	221
7.2	Diagnosedeckungsgrad (<i>DC</i>).	222
7.3	Einkanalig ohne Testung	226
7.4	Einkanalig mit Testung	227
7.5	Zweikanalig ohne Testung.	230
7.6	Zweikanalig mit geringer bis mittlerer Testung.	231
7.7	Zweikanalig mit hoher Testung	234
8	Tipps und Beispiele	237
8.1	Liste oft verwendeter Sicherheitsfunktionen.	237
8.2	Allgemeine Betrachtungen	238
8.2.1	Definieren einer Sicherheitsfunktion einfach gemacht	238
8.2.2	Warum darf man mit der DIN EN 62061 (VDE 0113-50) „nicht elektromechanische Komponenten“ (z. B. Ventile) berechnen?	240
8.2.3	Was tun mit den Kategorien der C-Normen?	241
8.2.4	Die Berechnungsmethode der DIN EN 62061 (VDE 0113-50):2016-05, Abschnitt 6.7.8.2 ist „normativ“, warum ist die der DIN EN ISO 13849-1:2016-06, Anhänge C und K dagegen nur „informativ“?	242
8.2.5	$MTTF_D$ -Wert gleich PFH_D -Wert	246
8.2.6	Verschleißbehaftete Komponenten und die Kategorie 2	247
8.2.7	Was bedeutet T_1 als Proof-Test oder Lebensdauer in der Praxis?	249
8.2.8	T_{10D} und T_1 , wann gilt was und warum?	251

8.2.9	Den Betätigungszyklus C (1/h) im Verhältnis zu den effektiven Betriebsstunden im Jahr umrechnen?	253
8.2.10	Bei einer einkanaligen Architektur gilt $PFH_D = (1 - DC) \cdot \lambda_D$ – Was passiert mit dem Diagnose-Testintervall T_2 ?	254
8.2.11	Welches erforderliche Testintervall ist für welchen SIL sinnvoll?	255
8.3	Grundsätzliche Betrachtungen – Sensorik.	257
8.3.1	Not-Halt-Befehlsgeräte – jedes für sich ist Teil einer entsprechenden „ergänzenden“ Sicherheitsfunktion	257
8.3.2	Verschleißbehaftete Komponenten haben keinen Anteil sicherer Ausfälle (SFF) – ob Sensor oder Aktor	258
8.3.3	SIL 2 in einer zweikanaligen Architektur ohne Diagnose ($SFF = 80\%$?) – bringt das etwas?	260
8.3.4	Muss ein Zustimmschalter als Teil einer Sicherheitsfunktion berücksichtigt werden?	261
8.3.5	PL e oder SIL 3 mit einem Positionsschalter mit getrenntem Betätiger?	262
8.3.6	Drehzahlüberwachung – wann dürfen die Geber außer Acht gelassen werden?	264
8.3.7	Stromwertüberwachung eines Motors in SIL 2	265
8.4	Grundsätzliche Betrachtungen – Aktorik.	268
8.4.1	Muss ein Antrieb (Motor) in einer Sicherheitsfunktion berücksichtigt werden?	268
8.4.2	Zwei Lastschütze an einem einzelnen sicherheitsgerichteten Ausgang mit SIL 3	269
8.4.3	Zwangsgeführte Kontaktelemente von Hilfsschützen und Spiegelkontakte von Leistungsschützen	269
8.4.4	Ist eine Überwachung von Hilfs- oder Leistungsschützen durch nicht sicherheitsgerichtete Eingangsbaugruppen möglich?	272
8.4.5	Welcher PL oder SIL kann mit einem einzelnen Leistungsschütz erreicht werden?	273
8.4.6	Bewerten von „Standard-Ausgangsbaugruppen“	274
8.4.7	Bewertung von Hilfsschützen oder Koppelrelais in einer Sicherheitsfunktion	277
8.4.8	Stern-Dreieck-Schaltung sicherheitsgerichtet bewerten	280
8.4.9	Lastfreies Schalten mit Leistungsschützen oder Hilfsschützen.	282
8.4.10	Was tun, wenn keine $MTTF_D$ -Werte vorliegen?	282
9	Berechnungen von typischen Sicherheitsfunktionen	285
9.1	Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine beweglichtrennende Schutzeinrichtung (Schutztür, -klappe, ...)	287

9.2	Sicherheitsbezogene Stoppfunktion, eingeleitet durch eine nicht trennende Schutzeinrichtung (Lichtvorhänge, Laserscanner, ...)	295
9.3	Handbetätigte Befehlseinrichtungen (Handsteuerung)	297
9.4	Zweihandschaltung	299
9.5	Manuelles Aufheben von Sicherheitsfunktionen	301
9.6	Einrichten, Teachen, Umrüsten, die Fehlersuche sowie für Reinigungs- oder Instandhaltungsarbeiten	303
9.7	Sichere Bewegungen	305
9.8	Sichere Positionserfassung	307
9.9	Auswahl von Steuerungs- und Betriebsarten	310
9.10	Zuhaltung einer Schutzeinrichtung	312
9.11	Funktion zum Stillsetzen im Notfall	315
9.12	SIL 1 und SIL 2 gleich SIL 3	322
10	Mal kritisch hinterfragt	327
10.1	Die Not-Halt-Funktion sinnvoll bewerten	327
10.2	Betriebsarten	332
10.3	Die Zuhaltung einer Verriegelungsreinrichtung berücksichtigen	337
10.4	Nicht alles muss berechnet werden	339
10.5	Nur sinnvolle Diagnosedeckungsgrade verwenden	341
10.6	„Standard“-Komponenten mit Vorsicht wählen	343
10.7	Ein Vergleich mit dem Anhang K der DIN EN ISO 13849-1:2016-06 lohnt sich	345
10.8	Die Einstufung des Risikos einmal anders vornehmen	350
10.9	Den Prozess als Hilfsmittel nutzen	352
11	Die Mathematik und das Warum	353
11.1	Definition der Wahrscheinlichkeit Gefahr bringender Ausfälle	353
11.1.1	Teilsystemelemente und Teilsysteme	353
11.1.2	Ausfallraten	353
11.1.3	Definition des PFH_D	354
11.2	Einkanalige Architektur	354
11.2.1	Annahmen	354
11.2.2	Logische Darstellung	354
11.2.3	Wahrscheinlichkeitsblockdiagramm	355
11.2.4	Berechnung	356
11.2.5	PFH_D der Teilsystemarchitektur C	356
11.3	Zweikanalige Architektur	356
11.3.1	Annahmen	356
11.3.2	Logische Darstellung	357

11.3.3	Wahrscheinlichkeitsblockdiagramm	358
11.3.4	Berechnung	359
11.3.5	PFH_D der Teilsystemarchitektur D	361
11.4	Diskussion der Ergebnisse der einkanaligen Architektur	361
11.4.1	Diagnosedeckungsgrad 60 %	361
11.4.2	Diagnosedeckungsgrad 90 %	362
11.4.3	Schlussfolgerung	363
11.5	Diskussion der Ergebnisse der zweikanaligen Architektur	364
11.5.1	Diagnosedeckungsgrad 60 %	364
11.5.2	Diagnosedeckungsgrad 90 %	364
11.5.3	Diagnosedeckungsgrad 99 %	364
11.5.4	Schlussfolgerung	364
12	Ausblick	369
13	Terminologie	371
14	Fachwörterbuch	403
	Literatur	413
	Stichwortverzeichnis	417