

Inhalt

Vorwort	7
DIN EN 62061 (VDE 0113-50)	15
Einleitung	17
1 Anwendungsbereich	23
2 Normative Verweisungen	27
3 Begriffe und Abkürzungen	31
3.1 Alphabetische Liste der Definitionen	31
3.2 Begriffe und Definitionen	33
3.3 Abkürzungen	60
4 Management der funktionalen Sicherheit	61
4.1 Zielsetzung	61
4.2 Entwurfsprozess	61
4.3 Management der funktionalen Sicherheit unter Verwendung eines Plans für funktionale Sicherheit	68
4.4 Konfigurationsmanagement	70
4.5 Modifikation	71
5 Spezifikation einer Sicherheitsfunktion	73
5.1 Zielsetzung	73
5.2 Spezifikation der Sicherheitsanforderungen (SRS)	73
5.2.1 Allgemeines	73
5.2.2 Benötigte Informationen	76
5.2.3 Spezifikation der funktionalen Anforderungen	76
5.2.4 Abschätzung der Anforderungsbetriebsart	76
6 Entwurf eines SCS	79
6.1 Allgemeines	79
6.2 Teilsystemarchitektur basierend auf Top-Down-Zerlegung	80
6.3 Grundlegende Methodik – Verwendung von Teilsystemen	82
6.3.1 Allgemeines	82

6.3.2	SCS-Zuordnung [Aufteilung, Zerlegung]	83
6.3.3	Zuweisung von Teilfunktionen	84
6.4	Bestimmung der Sicherheitsintegrität des SCS	85
6.4.1	Allgemeines	85
6.5	Anforderungen an die systematische Sicherheitsintegrität des SCS	87
6.5.1	Anforderungen zur Vermeidung systematischer Hardwareausfälle.	87
6.5.2	Anforderungen zur Beherrschung systematischer Ausfälle.	88
6.6	Elektromagnetische Störfestigkeit	88
6.7	Softwarebasierte manuelle Parametrierung	89
6.7.1	Allgemeines	89
6.7.2	Einflüsse auf sicherheitsbezogene Parameter	89
6.7.3	Anforderungen an softwarebasierte manuelle Parametrierung	90
6.7.4	Verifikation des Parametrisierungswerkzeugs	91
6.7.5	Durchführung der softwarebasierten manuellen Parametrierung	91
6.8	Security Aspekte	92
6.9	Aspekte der periodischen Testungen	97
7	Entwerfen und Entwickeln eines Teilsystems	99
7.1	Allgemeines	99
7.2	Entwurf der Teilsystemarchitektur	100
7.3	Anforderungen für die Auswahl und den Entwurf von Teilsystemen und Teilsystem-Elementen	102
7.3.1	Allgemeines	102
7.3.2	Systematische Integrität	102
7.3.2.1	Allgemeines	102
7.3.2.2	Anforderungen zur Vermeidung von systematischen Ausfällen	103
7.3.2.3	Anforderungen an die Beherrschung von systematischen Ausfällen.	103
7.3.2.4	Elektromagnetische Störfestigkeit	104
7.3.2.5	Security Aspekte	104
7.3.3	Fehlerbetrachtung und Fehlerausschluss	104
7.3.3.1	Allgemeines	104
7.3.3.2	Berücksichtigung von Fehlern	105
7.3.3.3	Fehlerausschluss	105
7.3.3.4	Funktionsprüfung zur Erkennung von Fehleranhäufungen und unentdeckten Fehlern	108
7.3.4	Ausfallrate eines Teilsystem-Elements	109
7.3.4.1	Allgemeines	109
7.3.4.2	Beziehung der betreffenden Parameter	109
7.4	Strukturelle Einschränkungen eines Teilsystems	112
7.4.1	Allgemeines	112

7.4.2	Abschätzung der Anteil sicherer Ausfälle (<i>SFF</i>)	116
7.4.3	Verhalten (des SCS) bei der Erkennung eines Fehlers in einem Teilsystem	116
7.4.3.1	Allgemeines	116
7.4.4	Realisierung von Diagnosefunktionen.	120
7.5	Architekturen für den Teilsystementwurf	121
7.5.1	Allgemeines	121
7.5.2	Basis-Teilsystemarchitekturen	121
7.5.2.1	Basis-Teilsystemarchitektur A: Einkanalig ohne Diagnosefunktion	121
7.5.2.2	Basis-Teilsystemarchitektur B: Zweikanalig ohne Diagnosefunktion.	121
7.5.2.3	Basis-Teilsystemarchitektur C: Einkanalig mit Diagnosefunktion	121
7.5.2.4	Basis-Teilsystemarchitektur D: Zweikanalig mit Diagnosefunktion	121
7.5.3	Grundlegende Anforderungen	122
7.6	<i>PFH</i> von Teilsystemen.	123
7.6.1	Allgemeines	123
7.6.2	Methoden zur Abschätzung des <i>PFH</i> eines Teilsystems	124
7.6.3	Vereinfachter Ansatz zur Abschätzung des Beitrags von Versagen aufgrund von Fehlern gemeinsamer Ursache (<i>CCF</i>)	125
8	Software	127
8.1	Allgemeines	127
8.2	Definition der Software-Level.	128
8.3	Software-Level 1	129
8.3.1	Software-Sicherheits-Lebenszyklus – SW-Level 1	129
8.3.1.1	Maximal erreichbarer SIL – SW-Level 1.	129
8.3.1.2	Software-Sicherheits-Lebenszyklusmodell – SW-Level 1	129
8.3.2	Softwareentwurf – SW-Level 1	133
8.3.2.1	Allgemein – SW-Level 1	133
8.3.2.2	Software-Sicherheitsanforderungen – SW-Level 1	133
8.3.2.3	Softwareentwurfsspezifikation – SW-Level 1	133
8.3.3	Modulentwurf – SW-Level 1	135
8.3.3.1	Allgemeines – SW-Level 1	135
8.3.3.2	Eingangsinformationen – SW-Level 1.	135
8.3.4	Programmierung – SW-Level 1	135
8.3.5	Software-Tests – SW-Level 1	136
8.3.5.1	Allgemeines – SW-Level 1	136

8.3.6	Konfigurations- und Änderungsmanagementprozess – SW-Level 1	137
8.4	Software-Level 2	138
8.4.1	Software-Sicherheits-Lebenszyklus – SW-Level 2	138
8.4.1.1	Maximal erreichbarer SIL – SW-Level 2	138
8.4.1.2	Software-Sicherheits-Lebenszyklusmodell – SW-Level 2	138
8.4.2	Softwareentwurf – SW-Level 2	140
8.4.2.1	Allgemeines – SW-Level 2	140
8.4.2.2	Software-Sicherheitsanforderungen – SW-Level 2	140
8.4.2.3	Softwareentwurfsspezifikation – SW-Level 1	140
8.4.3	Software-Systementwurf – SW-Level 2	142
8.4.3.1	Allgemeines – SW-Level 2	142
8.4.3.2	Eingangsinformationen – SW-Level 2	143
8.4.4	Modulentwurf – SW-Level 2	143
8.4.5	Programmierung – SW-Level 2	144
8.4.6	Modultest – SW-Level 2	145
8.4.7	Software-Integrationstest SW-Level 2	145
8.4.8	Software-Tests SW-Level 2	146
8.4.8.1	Allgemeines – SW-Level 2	146
8.4.8.2	Testplanung und -durchführung – SW-Level 2	146
8.4.9	Dokumentation – SW-Level 2	146
8.4.10	Konfigurations- und Änderungsverwaltungsprozess – SW-Level 2	147
9	Validierung	149
9.1	Grundsätze der Validierung	149
9.1.1	Validierungsplan	151
9.1.2	Verwendung von generischen Fehlerlisten	151
9.1.3	Spezifische Fehlerlisten	152
9.1.4	Informationen für die Validierung	152
9.1.5	Validierungsbericht	153
9.2	Analyse als Teil der Validierung	153
9.2.1	Allgemeines	153
9.2.2	Analysetechniken	153
9.2.3	Verifizierung der Spezifikation der Sicherheitsanforderungen (SRS)	153
9.3	Prüfung als Teil der Validierung	155
9.3.1	Allgemeines	155
9.3.2	Messgenauigkeit	155
9.3.3	Strengere Anforderungen	155
9.3.4	Prüflinge	155

9.4	Validierung der Sicherheitsfunktion	156
9.4.1	Allgemeines	156
9.4.2	Analyse und Tests	156
9.5	Validierung der Sicherheitsintegrität des SCS.	157
9.5.1	Allgemeines	157
9.5.2	Validierung des (der) Teilsystems (Teilsysteme).	157
9.5.3	Validierung von Maßnahmen gegen systematisches Versagen	158
9.5.4	Validierung von sicherheitsbezogener Software	158
9.5.5	Validierung der Kombination von Teilsystemen	159
10	Dokumentation.	161
10.1	Allgemeines	161
10.2	Technische Dokumentation	162
10.3	Benutzerinformationen für die SCS.	163
10.3.1	Allgemeines	163
10.3.1.1	Einführung	163
10.3.1.2	Spezifikation der Sicherheitsintegrität.	163
10.3.1.3	SCS und Teilsysteme	163
10.3.2	Benutzerinformation des Herstellers der Teilsysteme	164
10.3.3	Vom SCS-Integrator zur Verfügung gestellte Informationen zur Verwendung.	164
Anhang A (informativ) –	Bestimmung der erforderlichen Sicherheitsintegrität	167
Anhang B (informativ) –	Beispiel einer SCS-Entwurfsmethodik.	181
Anhang C (informativ) –	Beispiele für $MTTF_D$-Werte einzelner Komponenten	191
Anhang D (informativ) –	Beispiele für Diagnosedeckungsgrade	195
Anhang E (informativ) –	Methodik zur Abschätzung der Anfälligkeit für Ausfälle aufgrund gemeinsamer Ursache (CCF).	203
Anhang F (informativ) –	Leitfaden für Software-Level 1.	207

Anhang G (informativ) – Beispiele für Sicherheitsfunktionen	215
Anhang H (informativ) – Vereinfachte Ansätze zur Bewertung des <i>PFH</i>-Werts eines Teilsystems.	227
Anhang I (informativ) – Der Plan für funktionale Sicherheit und Entwurfsaktivitäten . .	235
Anhang J (informativ) – Unabhängigkeit für Überprüfungen und Test-/Verifizierungs-/ Validierungsaktivitäten	241