

Anwendungsbereich

Anwendungsbereich dieser Norm ist ...

Inhalt

	Seite
Einleitung	13
1 Anwendungsbereich	14
2 Normative Verweisungen	14
3 Begriffe und Abkürzungen	15
3.1 Alphabetische Liste der Begriffe	15
3.2 Begriffe	17
3.3 Abkürzungen	30
4 Gestaltungsprozess eines sicherheitsrelevanten Steuerungssystems (SCS) und Beherrschung der funktionalen Sicherheit	31
4.1 Zielsetzung	31
4.2 Gestaltungsprozess	31
4.3 Beherrschung der funktionalen Sicherheit durch einen funktionalen Sicherheitsplan	34
4.4 Konfigurationsmanagement	36
4.5 Modifikation	36
5 Spezifikation einer Sicherheitsfunktion	37
5.1 Zielsetzung	37
5.2 Spezifikation der Sicherheitsanforderungen (SRS)	37
5.2.1 Bereitstellende Informationen	37
5.2.2 Spezifikation der funktionalen Anforderungen	37
5.2.3 Spezifikation der Sicherheitsanforderungen	38
6 Gestaltung eines sicherheitsrelevanten Steuerungssystems zur Erfüllung einer Sicherheitsfunktion	39
6.1 Subsystem-Architektur auf der Grundlage der Aufschlüsselung von oben nach unten	39
6.2 Grundlegende Methodologie – Anwendung des Subsystems	39
6.2.1 Allgemeines	39
6.2.2 Gestaltung der Architektur des sicherheitsrelevanten Steuerungssystems auf der Grundlage von Subsystemen	40
6.2.3 Zuweisung einer Subfunktion	42
6.3 Gestaltung des sicherheitsrelevanten Steuerungssystems durch die Integration eines oder mehrerer Subsysteme	42
6.3.1 Allgemeines	42
6.4 Elektromagnetische Störfestigkeit	44
6.5 Softwarebasierte manuelle Parametrisierung	44
6.5.1 Allgemeines	44
6.5.2 Einflüsse auf sicherheitsrelevante Parameter	45
6.5.3 Anforderungen an die softwarebasierte manuelle Parametrisierung	45
6.5.4 Prüfung des Parametrisierungsinstruments	46

	Seite	
6.6	Sicherheitsaspekte.....	47
6.7	Gestaltung regelmäßiger Prüfungen.....	48
6.7.1	Allgemeines.....	48
6.7.2	Nachweisprüfungen.....	49
7	Gestaltung und Entwicklung eines Subsystems.....	49
7.1	Allgemeines.....	49
7.2	Gestaltung der Subsystem-Architektur.....	50
7.3	Anforderungen an die Auswahl und Gestaltung von Subsystemen und Subsystem-Elementen.....	50
7.3.1	Allgemeines.....	50
7.3.2	Systematische Integrität.....	51
7.3.3	Betrachtung und Ausschluss von Fehlern.....	53
7.3.4	Ausfallrate eines Subsystem-Elements.....	55
7.4	Architektonische Beschränkungen eines Subsystems.....	58
7.4.1	Allgemeines.....	58
7.4.2	Schätzung des Anteils sicherer Ausfälle (SFF).....	59
7.4.3	Verhalten (des SCS) bei Erkennung eines Fehlers in einem Subsystem.....	61
7.4.4	Ausführung von Diagnosefunktionen.....	62
7.5	Gestaltung der Subsystem-Architektur.....	63
7.5.1	Allgemeines.....	63
7.5.2	Grundlegende Subsystem-Architekturen.....	63
7.6	Wahrscheinlichkeit gefahrbringender zufälliger Hardware-Ausfälle von Subsystemen.....	65
7.6.1	Allgemeines.....	65
7.6.2	Vereinfachte Ansätze zur Schätzung des PFH _D eines Subsystems.....	65
7.6.3	Vereinfachte Ansätze für die Betriebsart mit geringem Bedarf.....	65
7.6.4	Vereinfachter Ansatz zur Schätzung des Beitrags eines Ausfalls aufgrund gemeinsamer Ursache (CCF).....	65
8	Software.....	65
8.1	Allgemeines.....	65
8.2	Tool-Nutzung.....	66
8.3	Software-Sicherheitslebensdauer.....	66
8.3.1	Softwarestufe.....	66
8.3.2	Software-Sicherheitslebensdauermodell.....	67
8.3.3	Unabhängigkeit der Prüfungs- und Verifizierungsaktivitäten.....	68
8.4	Softwaregestaltung.....	69
8.4.1	Allgemeines.....	69
8.4.2	Softwaresicherheitsanforderungen.....	70
8.4.3	Softwaregestaltungsspezifikation für die SW-Stufen A, B und C.....	75
8.5	Softwaresystemgestaltung.....	76
8.5.1	Allgemeines.....	76

	Seite
8.5.2 Softwaresystemgestaltungsspezifikation	76
8.6 Modulgestaltung	77
8.6.1 Allgemeines	77
8.6.2 Eingabeinformationen	77
8.6.3 Modulgestaltungsspezifikation	77
8.7 Codierung	77
8.8 Modulprüfung.....	78
8.8.1 Modulprüfung für die SW-Stufen A, B und C	78
8.8.2 Zusätzliche Modulprüfanforderungen für die SW-Stufe B und C	78
8.9 Softwareintegrationsprüfung	78
8.10 Softwareprüfung	78
8.10.1 Allgemeines	78
8.10.2 Planung und Ausführung der Prüfung.....	79
8.11 Dokumentation	80
8.12 Konfigurations- und Änderungssteuerungsprozess	80
9 Validierung.....	81
9.1 Validierungsgrundsätze	81
9.1.1 Validierungsplan	84
9.1.2 Allgemeine Fehlerlisten	84
9.1.3 Besondere Fehlerlisten	84
9.1.4 Informationen zur Validierung	84
9.1.5 Validierungsprotokoll	85
9.2 Validierung durch Analyse.....	85
9.2.1 Allgemeines	85
9.2.2 Analyseverfahren.....	86
9.3 Validierung durch Prüfung.....	86
9.3.1 Allgemeines	86
9.3.2 Messunsicherheit.....	87
9.3.3 Strengere Anforderungen	87
9.3.4 Anzahl der Prüfproben	88
9.4 Validierung der Sicherheitsanforderungsspezifikation für Sicherheitsfunktionen	88
9.5 Validierung der Sicherheitsfunktion.....	88
9.5.1 Allgemeines	88
9.5.2 Analyse und Prüfung	89
9.6 Validierung der Sicherheitsanforderung des SCS.....	89
9.6.1 Validierung des/der Subsystems/Subsysteme.....	89
9.6.2 Validierung von Maßnahmen gegen systematische Ausfälle	90
9.6.3 Validierung sicherheitsrelevanter Software	91
9.6.4 Validierung von Subsystemkombinationen	92

	Seite
9.6.5 Prüfung der Sicherheitsanforderung	93
10 Dokumentation	93
10.1 Allgemeines	93
10.2 Technische Dokumentation	93
10.3 Informationen zur Nutzung des SCS	94
10.3.1 Allgemeines	94
10.3.2 Von dem Subsystem-Hersteller bereitgestellte Nutzungsinformationen	95
10.3.3 Von dem SCS-Integrator bereitgestellte Nutzungsinformationen	96
Anhang A (informativ) Bestimmung der erforderlichen Sicherheitsanforderung	97
A.1 Allgemeines	97
A.2 Matrix-Zuweisung für die erforderliche SIL	97
A.2.1 Identifizierung/Angabe von Gefahren	97
A.2.2 Risikoeinschätzung	97
A.2.3 Schweregrad (Se)	98
A.2.4 Wahrscheinlichkeit des Auftretens eines Schadens	98
A.2.4.1 Häufigkeit und Dauer der Gefährdung	98
A.2.4.2 Wahrscheinlichkeit des Auftretens eines Gefährdungsereignisses	99
A.2.4.3 Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (Av)	100
A.2.5 Wahrscheinlichkeitsklasse eines Schadens (Cl)	100
A.2.6 SIL- oder PL-Zuweisung	101
A.3 Überlappende Gefahren	102
Anhang B (informativ) Beispiel für die SCS-Gestaltungsmethodik	103
B.1 Allgemeines	103
B.2 Sicherheitsanforderungsspezifikation	103
B.3 Aufschlüsselung der Sicherheitsfunktion	103
B.4 Gestaltung des SCS auf der Grundlage von Subsystemen	104
B.4.1 Allgemeines	104
B.4.2 Gestaltung des Subsystems 1 – „Schutztürüberwachung“	104
B.4.2.1 Architektonische Beschränkungen	104
B.4.2.2 Beurteilung des SFF	105
B.4.2.3 Beurteilung von DC_{11} und DC_{12}	106
B.4.2.4 Beurteilung von PFH_D	106
B.4.3 Gestaltung des Subsystems 2 – „Beurteilungslogik“	106
B.4.4 Gestaltung des Subsystems 3 – „Motorsteuerung“	107
B.4.4.1 Architektonische Beschränkung	107
B.4.4.2 Bewertung von PFH_D	107
B.4.5 Beurteilung des SCS	107
B.4.5.1 Systematische Integrität und CCF	108
B.4.5.2 Architektonische Beschränkungen (oder Kategorien)	108

	Seite
B.4.5.3 Wahrscheinlichkeit eines gefahrbringenden Hardware-Ausfalls	108
B.5 Verifizierung	108
B.5.1 Analyse	109
B.5.2 Prüfungen	109
Anhang C (informativ) Beispiele für $MTTF_D$ -Werte für einzelne Komponenten	110
C.1 Allgemeines	110
C.2 Verfahren auf der Grundlage anerkannter technischer Praktiken	110
C.3 Hydraulische Komponenten	110
C.4 $MTTF_D$ -Wert für pneumatische, mechanische und elektromechanische Komponenten	110
Anhang D (normativ) Anforderungen bei geringem Bedarf	112
D.1 Allgemeines	112
D.2 Normative Verweisungen	112
D.3 Begriffe	112
D.4 Gestaltungsprozess eines SCS und Beherrschung der funktionalen Sicherheit	115
D.5 Spezifikation einer Sicherheitsfunktion	115
D.6 Gestaltung eines SCS zur Erfüllung einer Sicherheitsfunktion	115
D.6.2.4 Anwendung des vorgestalteten Subsystems	116
D.6.3.2 Bestimmung der Sicherheitsanforderung des SCS	116
D.6.7.2 Nachweisprüfung	118
D.7 Gestaltung und Entwicklung eines Subsystems	118
D.7.4.1 Allgemein	118
D.7.5 Architekturen für die Subsystemgestaltung	119
D.7.6.1 Allgemeines	119
D.7.6.2 Vereinfachte Ansätze zur Schätzung des PFH_D eines Subsystems	119
D.7.6.3 Vereinfachte Ansätze für die Betriebsart mit geringem Bedarf	119
D.8 Software	119
D.9 Validierung	119
D.10 Dokumentation	119
D.10.3.3 Von dem SCS-Integrator bereitgestellte Nutzungsinformationen	119
Anhang E (informativ) Beispiele für die diagnostische Abdeckung (DC)	121
Anhang F (informativ) Methodik zur Schätzung der Anfälligkeit für Ausfälle mit gemeinsamer Ursache (CFF)	125
F.1 Allgemeines	125
F.2 Methodik	125
F.2.1 Anforderungen für CCF	125
F.2.2 Schätzung der Auswirkung von CCF	125
Anhang G (informativ) Leitlinie für Softwaresicherheitsanforderungen für die Softwarestufe A	127
G.1 Relevante Eingabe- und Ausgabeinformationen sind in Tabelle G.1 enthalten	127
G.2 Programmierungsleitlinien	128

	Seite
G.3 Spezifikation von Sicherheitsfunktionen	129
G.4 Spezifikation der Hardwaregestaltung	131
G.5 Softwaresystemgestaltungsspezifikation	132
G.6 Protokolle	136
Anhang H (informativ) ((leer)).....	138
Anhang I (informativ) Beispiele für Sicherheitsfunktionen.....	138
I.1 Beispiele für Sicherheitsfunktionen	138
Anhang J (informativ) ((leer)).....	139
Anhang K (informativ) Vereinfachte Ansätze zur Schätzung des PFHD-Werts eines Subsystems	139
K.1 Allgemeines.....	139
K.2 Tabellenzuweisungsansatz	139
K.3 Numerischer Ansatz zur Darstellung der exponentiellen Verteilung.....	143
K.4 Vereinfachte Formeln.....	149
K.4.1 Allgemein.....	149
K.4.2 Grundlegende Subsystem-Architektur A: einzelner Kanal ohne Diagnosefunktion.....	150
K.4.3 Grundlegende Subsystem-Architektur B: zwei Kanäle ohne Diagnosefunktion	150
K.4.4 Grundlegende Subsystem-Architektur C: einzelner Kanal mit Diagnosefunktion.....	150
K.4.5 Grundlegende Subsystem-Architektur D: Zweikanal mit Diagnosefunktion(en).....	152
K.5 Teilezahlverfahren.....	152
Anhang L (informativ) Wechselbeziehung zu ISO 13849-1	154
L.1 Allgemeines.....	154
L.2 Grundlegende Eigenschaften eines Subsystems	154
L.3 Maximal erreichbare SIL auf der Grundlage der Kategorien und von DC_{avg}	155
L.4 Grundlegende Anforderungen.....	155
Anhang M (informativ) Beherrschung der funktionalen Sicherheit.....	157
M.1 Allgemeines.....	157
M.2 Beispiel für einen Maschinengestaltungsplan einschließlich eines Sicherheitsplans	157
M.3 Beispiel für Aktivitäten, Dokumente und Aufgaben.....	157
Literaturhinweise	160
Bilder	
Bild 1 – Integration innerhalb des Risikoreduzierungsprozesses nach ISO 12100	32
Bild 2 – Schrittweiser Prozess zur Gestaltung des sicherheitsrelevanten Steuerungssystems	33
Bild 3 – Beispiele für die Kombination von Subsystemen zu einem sicherheitsrelevanten Steuerungssystem.....	34
Bild 4 – Beispiele für die typische Aufschlüsselung einer Sicherheitsfunktion in Subfunktionen und Zuweisung zu Subsystemen	41
Bild 5 – Beispiel für die Sicherheitsanforderung einer Sicherheitsfunktion auf der Grundlage der als ein sicherheitsrelevantes Steuerungssystem zugewiesenen Subsysteme.....	43
Bild 6 – Logische Darstellung des Subsystems A.....	63
Bild 7 – Logische Darstellung des Subsystems B.....	63

	Seite
Bild 8 – Logische Darstellung des Subsystems C	64
Bild 9 – Logische Darstellung des Subsystems D 7.5.3 Grundlegende Anforderungen	64
Bild 10 – V-Modell für SW-Stufe A	68
Bild 11 – V-Modell für von dem Gestalter angepasste Softwaremodule für die SW-Stufe A	68
Bild 12 – V-Modell der Softwaresicherheitslebensdauer für SW-Stufe B und C	68
Bild 13 – Überblick über den Validierungsprozess	83
Bild A.1 – Für die Risikoeinschätzung verwendete Parameter	97
Bild A.2 – Pro-forma-Beispiele für den SIL-Zuweisungsprozess	102
Bild B.1 – Aufschlüsselung der Sicherheitsfunktion	104
Bild B.2 – Übersicht der Gestaltung der Subsysteme des SCS	104
Bild D.5 – Beispiel für die Sicherheitsanforderung einer Sicherheitsfunktion auf der Grundlage der als ein SCS zugewiesenen Subsysteme	117
Bild G.1 – Anlagenskizze	129
Bild G.2 – Zuweisung von Sicherheitsfunktionen zu verschiedenen SCS mit relevanten Subsystemen und üblichen Softwareebenen	131
Bild G.3 – Grundlegende modulare Architekturgestaltung	133
Bild G.4 – Grundlegender Gestaltungsansatz der logischen Beurteilung	134
Bild G.5 – Beispiel der logischen Darstellung (Programmskizze)	135
Bild K.1 – Grundlegende Subsystem-Architektur C logische Ansicht mit Einleitung des sicheren Zustands	151
Bild K.2 – Grundlegende Subsystem-Architektur C logische Ansicht mit Fehlzustandsreaktion	151
Bild M.1 – Beispiel für einen Maschinengestaltungsplan einschließlich eines Sicherheitsplans	157
Bild M.2 – Beispiel für Aktivitäten, Dokumente und Aufgaben	158
Bild M.2 – Beispiel für Aktivitäten, Dokumente und Aufgaben (Fortsetzung)	159
Tabellen	
Tabelle 1 – Sicherheitsanforderungsstufen und PFH_D -Grenzwerte	39
Tabelle 2 – Geforderte Sicherheitsanforderungsstufen und PFH_D eines vorgestalteten Systems	42
Tabelle 3 – Relevante Informationen für jedes Subsystem	49
Tabelle 4 – Architektonische Beschränkungen für Subsysteme: höchste SIL, die für ein SCS, das dieses Subsystem verwendet, geltend gemacht werden kann	59
Tabelle 5 – Übersicht der grundlegenden Anforderungen und Interrelation zu grundlegenden Subsystem-Architekturen	64
Tabelle 6 – Verschiedene Softwarestufen	66
Tabelle 7 – Übersicht der Softwarestufen, Routen und erreichbaren SIL/PL	67
Tabelle 8 – Mindestunabhängigkeitsgrade für Prüfungs- und Verifizierungsaktivitäten	69
Tabelle 9 – Software-Ausfälle und Erkennungsmaßnahmen (1)	72
Tabelle 10 – Software-Ausfälle und Erkennungsmaßnahmen (2)	73
Tabelle 11 – Grundlegende Anforderungen und Interrelation zu grundlegenden zu validierenden Subsystemarchitekturen	91
Tabelle 12 – Dokumentation eines SCS	94
Tabelle A.1 – Klassifizierung des Schweregrads (Se)	98

	Seite
Tabelle A.2 – Klassifizierung der Häufigkeit und Dauer der Gefährdung (Fr).....	99
Tabelle A.3 – Klassifizierung der Wahrscheinlichkeit (Pr).....	100
Tabelle A.4 – Klassifizierung der Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (Av).....	100
Tabelle A.5 – Angewendete Parameter zur Bestimmung der Wahrscheinlichkeitsklasse eines Schadens (Cl).....	101
Tabelle A.6 – Matrixzuweisung zur Bestimmung der erforderlichen SIL (oder PL) für eine Sicherheitsfunktion	101
Tabelle B.1 – Sicherheitsanforderungsspezifikation – Übersichtsbeispiel	103
Tabelle B.2 – Systematische Integrität – Übersichtsbeispiel	108
Tabelle B.3 – Verifizierung durch Prüfungen.....	109
Tabelle C.1 – Normenverweisungen und $MTTF_D$ - oder B_{10D} -Werte für Komponenten	111
Tabelle D.1 – SIL und PFD_{avg} -Grenzwerte für den Betrieb bei geringem Bedarf.....	115
Tabelle E.1 – Schätzungen für die diagnostische Abdeckung (DC)	121
Tabelle E.1 (2 von 4)	122
Tabelle E.1 (3 von 4)	123
Tabelle E.1 (4 von 4)	124
Tabelle F.1 – Kriterien für die Schätzung der CCF	125
Tabelle F.1 (2 von 2)	126
Tabelle F.2 – Kriterien für die Schätzung der CCF	126
Tabelle G.1 – Beispiele relevanter Dokumente in Verbindung mit dem vereinfachten V-Modell	127
Tabelle G.2 – Beispiele für Programmierleitlinien	128
Tabelle G.3 – Festgelegte Sicherheitsfunktionen	130
Tabelle G.4 – Relevante Liste der Eingangs- und Ausgangssignale.....	132
Tabelle G.5 – Beispiel für eine vereinfachte Ursachen- und Wirkungsmatrix.....	135
Tabelle G.6 – Verifizierung der Softwaresystemgestaltungsspezifikation	136
Tabelle G.7 – Softwarecodeprüfung.....	136
Tabelle G.8 – Software-Validierung	137
Tabelle I.1 – Beispiele für übliche Sicherheitsfunktionen	138
Tabelle K.1 – Zuweisung des PFH_D -Werts eines Subsystems	141
Tabelle K.2 – Beziehung zwischen $B_{10D} > \text{Betrieb}$ und $MTTF_D$	142
Tabelle K.3 – Numerischer Ansatz mit $\beta = 10\%$ für $MTTF_D$ -Werte.....	144
Tabelle K.4 – Numerischer Ansatz mit $\beta = 5\%$ für $MTTF_D$ -Werte.....	145
Tabelle K.5 – Numerischer Ansatz mit $\beta = 2\%$ für $MTTF_D$ -Werte.....	146
Tabelle K.6 – Numerischer Ansatz mit $\beta = 10\%$ für $MTTF_D$ -Werte basierend auf B_{10D}	147
Tabelle K.7 – Numerischer Ansatz mit $\beta = 5\%$ für $MTTF_D$ -Werte basierend auf B_{10D}	148
Tabelle K.8 – Numerischer Ansatz mit $\beta = 2\%$ für $MTTF_D$ -Werte basierend auf B_{10D}	149
Tabelle L.1 – Quantifizierbare Eigenschaften je nach Subsystem-Art und Subsystem-Element	154

	Seite
Tabelle L.2 – Bezeichnete Architekturen: Maximal erreichbare SIL oder PL eines Subsystems	155
Tabelle L.3 – Wechselbeziehung zwischen den grundlegenden Anforderungen der Kategorien, der Hardware-Fehlertoleranz (HFT) und den grundlegenden Subsystem-Architekturen	156