

Inhalt

	Seite
Vorwort.....	2
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	13
4 Übereinstimmung mit dieser Norm	13
5 Dokumentation	13
6 Zusätzliche Anforderungen an das Management der sicherheitsbezogenen Software.....	13
6.1 Ziele	13
6.2 Anforderungen	13
7 Anforderungen des Software-Sicherheitslebenszyklus.....	14
7.1 Allgemeines	14
7.2 Spezifikation der Anforderungen an die Sicherheit der Software.....	22
7.3 Validierungsplan für die Softwareaspekte der Systemsicherheit	26
7.4 Softwareentwurf und Entwicklung	27
7.5 Integration der programmierbaren Elektronik (Hardware und Software)	39
7.6 Software-Betriebs- und Modifikationsverfahren	40
7.7 Softwareaspekte bezüglich der Validierung der Sicherheit des Systems	40
7.8 Softwaremodifikation	42
7.9 Softwareverifikation	44
8 Beurteilung der funktionalen Sicherheit.....	48
Anhang A (normativ) Leitfaden für die Auswahl der Verfahren und Maßnahmen.....	50
Anhang B (informativ) Detailtabellen	59
Anhang C (informativ) Eigenschaften für die systematische Eignung der Software	64
C.1 Einleitung	64
C.1.1 Struktur des Anhangs C hinsichtlich der Anhänge A und B	64
C.1.2 Methode der Anwendung – 1	66
C.1.3 Methode der Anwendung – 2	67
C.2 Eigenschaften der systematischen Sicherheitsintegrität.....	69
C.3 Eigenschaften für die systematische Sicherheitsintegrität – Ausführliche Tabellen	101
Anhang D (normativ) Sicherheitshandbuch für konforme Objekte – zusätzliche Anforderungen an Softwareelemente.....	114
D.1 Zweck des Sicherheitshandbuchs	114
D.2 Inhalt des Sicherheitshandbuchs für ein Softwareelement	114
D.3 Begründung der Ansprüche im Sicherheitshandbuch für konforme Elemente	115
Anhang E (informativ) Beziehungen zwischen IEC 61508-2 und IEC 61508-3	117
Anhang F (informativ) Verfahren zum Erreichen der Nicht-Beeinflussung zwischen Softwareelementen auf einem einzelnen Rechner.....	119

	Seite
F.1 Einleitung	119
F.2 Bereiche des Verhaltens.....	119
F.3 Analyse ursächlicher Faktoren	119
F.4 Erreichung räumlicher Unabhängigkeit.....	120
F.5 Erreichung zeitlicher Unabhängigkeit	120
F.6 Anforderungen an die Hilfssoftware.....	121
F.7 Unabhängigkeit von Softwaremodulen – Aspekte zu Programmiersprachen	121
Anhang G (informativ) Leitlinien zur Anpassung des Lebenszyklus im Zusammenhang mit datengesteuerten Systemen.....	124
G.1 Datengesteuert – Systemteil und Anwendungsteil	124
G.2 Eingeschränkter Freiheitsgrad der Konfiguration, eingeschränkte Anwendungskonfigurierbarkeit	125
G.3 Eingeschränkter Freiheitsgrad der Konfiguration, vollständige Anwendungskonfigurierbarkeit	126
G.4 Eingeschränkter Freiheitsgrad der Programmierung, eingeschränkte Anwendungskonfigurierbarkeit	126
G.5 Eingeschränkter Freiheitsgrad der Programmierung, vollständige Anwendungskonfigurierbarkeit	126
G.6 Vollständige Funktionalität der Programmierung/Konfiguration, eingeschränkte Anwendungskonfigurierbarkeit	127
G.7 Vollständige Funktionalität der Programmierung/Konfiguration, vollständige Anwendungskonfigurierbarkeit	127
Literaturhinweise	128
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen.....	129
Bilder	
Bild 1 – Gesamtrahmen der Normenreihe IEC 61508.....	11
Bild 2 – Gesamtsicherheitslebenszyklus.....	12
Bild 3 – Sicherheitslebenszyklus des E/E/PE-Systems (in der Realisierungsphase).....	16
Bild 4 – Software-Sicherheitslebenszyklus (in der Realisierungsphase).....	16
Bild 5 – Beziehung zwischen IEC 61508-2 und IEC 61508-3 und ihre Anwendungsbereiche.....	17
Bild 6 – Systematische Eignung der Software und Entwicklungslebenszyklus (V-Modell)	17
Bild G.1 – Freiheitsgrad gegen Komplexität bei datengesteuerten Systemen	125
Tabellen	
Tabelle 1 – Software-Sicherheitslebenszyklus – Überblick	18
Tabelle A.1 – Spezifikation der Anforderungen an die Sicherheit der Software.....	51
Tabelle A.2 – Softwareentwurf und Softwareentwicklung – Entwurf der Softwarearchitektur	51
Tabelle A.3 – Softwareentwurf und Softwareentwicklung – Werkzeuge und Programmiersprachen	53
Tabelle A.4 – Softwareentwurf und Softwareentwicklung – Detaillierter Entwurf.....	54
Tabelle A.5 – Softwareentwurf und Softwareentwicklung – Test der Softwaremodule und Integration	54
Tabelle A.6 – Integration der programmierbaren Elektronik (Hardware und Software).....	55
Tabelle A.7 – Softwareaspekte zur Validierung der Sicherheit des Systems.....	56

	Seite
Tabelle A.8 – Modifikation	56
Tabelle A.9 – Softwareverifikation	57
Tabelle A.10 – Beurteilung der funktionalen Sicherheit.....	58
Tabelle B.1 – Entwurfs- und Programmierrichtlinien	59
Tabelle B.2 – Dynamische Analyse und Test.....	59
Tabelle B.3 – Funktionstest und Black-Box-Test.....	60
Tabelle B.4 – Ausfall-/Versagensanalyse	61
Tabelle B.5 – Modellierung	61
Tabelle B.6 – Leistungstest	62
Tabelle B.7 – Semiformale Methoden	62
Tabelle B.8 – Statische Analyse	63
Tabelle B.9 – Modularer Ansatz	63
Tabelle C.1 – Eigenschaften für die systematische Sicherheitsintegrität – Spezifikation der Anforderungen an die Sicherheit der Software	69
Tabelle C.2 – Eigenschaften für die systematische Sicherheitsintegrität – Softwareentwurf und -entwicklung – Entwurf der Softwarearchitektur	73
Tabelle C.3 – Eigenschaften für die systematische Sicherheitsintegrität – Softwareentwurf und -entwicklung – Unterstützende Werkzeuge und Programmiersprache	87
Tabelle C.4 – Eigenschaften für die systematische Sicherheitsintegrität – Softwareentwurf und -entwicklung – Detaillierter Entwurf (einschließlich Software-Systementwurf, Entwurf der Softwaremodule und Kodierung)	88
Tabelle C.5 – Eigenschaften für die systematische Sicherheitsintegrität – Softwareentwurf und -entwicklung – Test der Softwaremodule und Integration	91
Tabelle C.6 – Eigenschaften für die systematische Sicherheitsintegrität – Integration der programmierbaren Elektronik (Hardware und Software).....	93
Tabelle C.7 – Eigenschaften für die systematische Sicherheitsintegrität – Softwareaspekte bezüglich der Validierung der Sicherheit des Systems	94
Tabelle C.8 – Eigenschaften für die systematische Sicherheitsintegrität – Softwaremodifikation	95
Tabelle C.9 – Eigenschaften für die systematische Sicherheitsintegrität – Softwareverifikation	97
Tabelle C.10 – Eigenschaften für die systematische Sicherheitsintegrität – Beurteilung der funktionalen Sicherheit	99
Tabelle C.11 – Ausführliche Eigenschaften – Entwurfs- und Programmierrichtlinien	101
Tabelle C.12 – Ausführliche Eigenschaften – Dynamische Analyse und Test.....	104
Tabelle C.13 – Ausführliche Eigenschaften – Funktionstest und Black-Box-Test.....	106
Tabelle C.14 – Ausführliche Eigenschaften – Ausfall-/Versagensanalyse.....	107
Tabelle C.15 – Ausführliche Eigenschaften – Modellierung	108
Tabelle C.16 – Ausführliche Eigenschaften – Leistungstest	108
Tabelle C.17 – Ausführliche Eigenschaften – Semiformale Methoden	109
Tabelle C.18 – Eigenschaften der systematischen Sicherheitsintegrität – Statische Analyse.....	111
Tabelle C.19 – Ausführliche Eigenschaften – Modularer Ansatz	112
Tabelle E.1 – Kategorien der IEC 61508-2-Anforderungen.....	117

	Seite
Tabelle E.2 – Anforderungen der 61508-2 an Software und ihre typische Bedeutung für bestimmte Typen von Software	117
Tabelle F.1 – Modulkopplung – Definition von Begriffen	121
Tabelle F.2 – Arten von Modulkopplungen	122