

## Inhalt

	<b>Seite</b>
Einleitung.....	9
1 Anwendungsbereich .....	11
2 Normative Verweisungen.....	13
3 Definitionen und Abkürzungen.....	13
Anhang A (informativ) Überblick über Verfahren und Maßnahmen für E/E/PES: Beherrschung von zufälligen Hardwareausfällen (siehe IEC 61508-2) .....	14
A.1 Elektrik .....	14
A.1.1 Erkennung von Ausfällen durch Überwachung während des Betriebs .....	14
A.1.2 Überwachung von Relaiskontakten .....	14
A.1.3 Vergleicher .....	14
A.1.4 Mehrheitsentscheider.....	15
A.1.5 Ruhestromprinzip.....	15
A.2 Elektronik .....	15
A.2.1 Tests durch redundante Hardware .....	15
A.2.2 Dynamische Prinzipien .....	15
A.2.3 Standardtestschnittstelle (Access Port) und Boundary-Scan Architektur.....	16
A.2.4 Hardware mit sicherer Ausfallrichtung .....	16
A.2.5 Überwachte Redundanz .....	16
A.2.6 Hardware mit automatischen Tests .....	17
A.2.7 Analogsignal-Überwachung .....	17
A.2.8 Unterlastung.....	17
A.3 Verarbeitungseinheiten (CPUs).....	17
A.3.1 Selbsttest per Software: begrenzte Anzahl von Mustern (ein Kana).....	17
A.3.2 Selbsttest per Software: Walking Bit (ein Kanal).....	18
A.3.3 Selbsttest unterstützt durch Hardware (ein Kanal).....	18
A.3.4 Codierte Verarbeitung (ein Kanal).....	18
A.3.5 Gegenseitiger Vergleich durch Software .....	18
A.4 Unveränderliche Speicherbereiche.....	19
A.4.1 Wortsicherungsverfahren mit Mehr-Bit-Redundanz (zum Beispiel ROM-Überwachung mit einem modifizierten Hammingcode) .....	19
A.4.2 Modifizierte Prüfsumme .....	19
A.4.3 Signatur mit einfacher Wortbreite (8 Bit).....	19
A.4.4 Signatur mit doppelter Wortbreite (16 Bit) .....	20
A.4.5 Blockwiederholung (zum Beispiel doppeltes ROM mit Hardware- oder Softwarevergleich).....	20
A.5 Veränderliche Speicherbereiche.....	20
A.5.1 RAM-Test „Checkerboard“ oder „March“ .....	20
A.5.2 RAM-Test „Walkpath“ .....	21
A.5.3 RAM-Test „Galpat“ oder „transparenter Galpat“ .....	21
A.5.4 RAM-Test „Abraham“ .....	22

	<b>Seite</b>
A.5.5 Ein-Bit-Redundanz (zum Beispiel RAM-Überwachung mit einem Parity-Bit) .....	22
A.5.6 RAM-Überwachung mit einem modifizierten Hammingcode oder Erkennung von Datenfehlern mit fehlererkennenden und -korrigierenden Codes (en: error-detection-correction codes (EDC)) .....	22
A.5.7 Doppeltes RAM mit Hardware- oder Softwarevergleich und Schreib-/Lesetest .....	23
A.6 E/A-Einheiten und Schnittstellen (externe Kommunikation) .....	23
A.6.1 Testmuster .....	23
A.6.2 Codesicherung .....	23
A.6.3 Mehrkanalige parallele Ausgabe .....	24
A.6.4 Überwachte Ausgaben .....	24
A.6.5 Eingabevergleich/-entscheidung .....	24
A.7 Datenwege (interne Kommunikation) .....	25
A.7.1 Ein-Bit-Hardware-Redundanz .....	25
A.7.2 Mehr-Bit-Hardware-Redundanz .....	25
A.7.3 Vollständige Hardware-Redundanz .....	25
A.7.4 Inspektion durch Verwendung von Testmustern .....	25
A.7.5 Übertragungsredundanz .....	26
A.7.6 Informationsredundanz .....	26
A.8 Spannungsversorgung .....	26
A.8.1 Überspannungsschutz mit Sicherheitsabschaltung .....	26
A.8.2 Spannungsüberwachung (sekundärseitig) .....	26
A.8.3 Energieabschaltung mit Sicherheitsabschaltung .....	26
A.9 Zeitliche und logische Programmlaufüberwachung .....	27
A.9.1 Watchdog mit separater Zeitbasis ohne Zeitfenster .....	27
A.9.2 Watchdog mit separater Zeitbasis und Zeitfenster .....	27
A.9.3 Logische Überwachung des Programmablaufs .....	27
A.9.4 Kombination von zeitlicher und logischer Überwachung des Programmablaufs .....	28
A.9.5 Zeitliche Überwachung mit Test während des Betriebs .....	28
A.10 Lüftung und Beheizung .....	28
A.10.1 Temperatursensor .....	28
A.10.2 Lüfterkontrolle .....	28
A.10.3 Auslösung der Sicherheitsabschaltung über eine thermische Sicherung .....	28
A.10.4 Gestaffelte Meldung von Thermosensoren und bedingter Alarm .....	29
A.10.5 Zuschaltung von Fremdkühlung und Statusanzeige .....	29
A.11 Kommunikation und Massenspeicher .....	29
A.11.1 Trennung elektrischer Energieleitungen von Informationsleitungen .....	29
A.11.2 Räumliche Trennung mehrfacher Leitungen .....	29
A.11.3 Erhöhung der Störfestigkeit .....	29
A.11.4 Antivalente Signalübertragung .....	30
A.12 Sensoren .....	30

	<b>Seite</b>
A.12.1 Referenzsensor.....	30
A.12.2 Zwangsöffnender Schalter.....	30
A.13 Stellglieder (Aktoren) .....	30
A.13.1 Überwachung.....	30
A.13.2 Kreuzweise Überwachung mehrfacher Aktoren .....	31
A.14 Maßnahmen gegen die Einwirkung der physikalischen Umgebung.....	31
Anhang B (informativ) Überblick über Verfahren und Maßnahmen für E/E/PES: Vermeidung von systematischen Ausfällen (siehe IEC 61508-2 und IEC 61508-3).....	32
B.1 Allgemeine Maßnahmen und Verfahren .....	32
B.1.1 Projektmanagement.....	32
B.1.2 Dokumentation .....	33
B.1.3 Trennung sicherheitsbezogener Systeme von nicht sicherheitsbezogenen Systemen .....	34
B.1.4 Diversitäre Hardware .....	34
B.2 Spezifikation der E/E/PES-Sicherheitsanforderungen.....	34
B.2.1 Strukturierte Spezifikation .....	34
B.2.2 Formale Methoden .....	35
B.2.3 Semi-formale Methoden.....	35
B.2.4 Rechnerunterstützte Spezifikationswerkzeuge .....	37
B.2.5 Checklisten.....	38
B.2.6 Inspektion der Spezifikation .....	39
B.3 E/E/PES-Entwurf und Entwicklung .....	39
B.3.1 Beachtung von Richtlinien und Normen .....	39
B.3.2 Strukturierter Entwurf .....	40
B.3.3 Verwendung von bewährten Bauteilen .....	41
B.3.4 Modularisierung .....	41
B.3.5 Rechnerunterstützte Entwurfswerkzeuge .....	41
B.3.6 Simulation .....	42
B.3.7 Inspektion (Überprüfungen und Analysen) .....	42
B.3.8 Walk-through.....	43
B.4 E/E/PES-Betriebs- und Instandhaltungsverfahren.....	43
B.4.1 Betriebs- und Instandhaltungsanweisungen.....	43
B.4.2 Benutzerfreundlichkeit .....	43
B.4.3 Instandhaltungsfreundlichkeit .....	44
B.4.4 Eingeschränkte Betriebsmöglichkeiten .....	44
B.4.5 Betrieb nur durch erfahrene Bediener .....	44
B.4.6 Schutz gegen Irrtümer des Bedieners .....	44
B.4.7 (Nicht verwendet).....	45
B.4.8 Schutz vor Modifikation .....	45
B.4.9 Eingabebestätigung .....	45
B.5 E/E/PES-Integration.....	45

	<b>Seite</b>
B.5.1 Funktionstest .....	45
B.5.2 Black-Box Test .....	46
B.5.3 Statistisches Testen .....	47
B.5.4 Felderfahrung .....	47
B.6 Validierung des E/E/PES bezüglich der Sicherheit .....	48
B.6.1 Funktionstest unter Umgebungsbedingungen .....	48
B.6.2 Test der Störfestigkeit gegen Stoßspannungen .....	48
B.6.3 (Nicht verwendet) .....	49
B.6.4 Statische Analyse .....	49
B.6.5 Dynamische Analyse .....	49
B.6.6 Ausfallanalyse .....	49
B.6.7 „Worst-Case“-Analyse .....	52
B.6.8 Erweiterte Funktionstests .....	52
B.6.9 Test unter Grenzbedingungen .....	52
B.6.10 Test durch Fehlereinbau .....	52
Anhang C (informativ) Überblick über Verfahren und Maßnahmen zum Erreichen der Sicherheitsintegrität der Software (siehe IEC 61508-3) .....	54
C.1 Allgemeines .....	54
C.2 Anforderungen und detaillierter Entwurf .....	54
C.2.1 Strukturierte Methoden .....	54
C.2.2 Datenflussdiagramme .....	57
C.2.3 Strukturdiagramme .....	58
C.2.4 Formale Methoden .....	59
C.2.5 Defensive Programmierung .....	64
C.2.6 Entwurfs- und Programmierrichtlinien .....	65
C.2.7 Strukturierte Programmierung .....	67
C.2.8 Geheimnisprinzip/Kapselung .....	67
C.2.9 Modularisierung .....	68
C.2.10 Verwendung bewährter/verifizierter Softwaremodule und Komponenten .....	68
C.3 Entwurf der Architektur .....	70
C.3.1 Fehlererkennung und Diagnose .....	70
C.3.2 Fehlererkennende und korrigierende Codes .....	70
C.3.3 Plausibilitätskontrollen .....	71
C.3.4 Externe Überwachungseinrichtungen .....	71
C.3.5 Diversitäre Programmierung .....	72
C.3.6 Regenerationsblöcke .....	72
C.3.7 Rückwärtsregeneration .....	73
C.3.8 Vorwärtsregeneration .....	73
C.3.9 Regeneration durch Wiederholung .....	73
C.3.10 Aufzeichnung ausgeführter Abschnitte .....	73

	<b>Seite</b>
C.3.11 Abgestufte Funktionseinschränkungen .....	74
C.3.12 Künstliche Intelligenz – Fehlerkorrektur .....	74
C.3.13 Dynamische Rekonfiguration .....	75
C.4 Entwicklungswerkzeuge und Programmiersprachen .....	75
C.4.1 Streng typisierte Programmiersprache .....	75
C.4.2 Sprachenteilmengen .....	76
C.4.3 Zertifizierte Werkzeuge und Compiler .....	76
C.4.4 Betriebsbewährte Werkzeuge und Compiler .....	77
C.4.5 Bibliothek bewährter/verifizierter Softwaremodule und Komponenten .....	78
C.4.6 Geeignete Programmiersprache .....	78
C.5 Verifikation und Modifikation .....	81
C.5.1 Probabilistisches Testen .....	81
C.5.2 Datenaufzeichnung und Analyse .....	82
C.5.3 Schnittstellenprüfung .....	83
C.5.4 Durchführung von Testfällen nach einer Grenzwertanalyse .....	83
C.5.5 Durchführung von Testfällen aus der Fehlerschätzung („Fehler erraten“) .....	84
C.5.6 Durchführung von Testfällen aus Einbringung von Fehlern .....	84
C.5.7 Äquivalenzklassentest (aufgrund von Partitionen des Eingangsbereichs) .....	84
C.5.8 Strukturabhängige Prüfungen .....	85
C.5.9 Steuerflussanalyse .....	85
C.5.10 Datenflussanalyse .....	86
C.5.11 Nebenpfadanalyse .....	86
C.5.12 Symbolische Ausführung .....	87
C.5.13 Formale Beweise .....	87
C.5.14 Software-Komplexitätsmetriken .....	87
C.5.15 Fagan-Inspektion .....	88
C.5.16 Walk-through/Entwurfsüberprüfungen .....	88
C.5.17 Prototypenerstellung/Animation .....	89
C.5.18 Simulation des Prozesses .....	89
C.5.19 Anforderungen an die Leistungsfähigkeit .....	90
C.5.20 Modellierung der Leistungsfähigkeit .....	90
C.5.21 Belastungstest (en: Avalanche/stress testing) .....	91
C.5.22 Reaktionszeiten und Speicherbeschränkung .....	91
C.5.23 Einflussanalyse .....	91
C.5.24 Konfigurationsmanagement der Software .....	92
C.6 Beurteilung der funktionalen Sicherheit .....	92
C.6.1 Entscheidungs-/Wahrheitstabellen .....	92
C.6.2 Gefährdungs- und Betriebbarkeitsuntersuchung (en: hazard and operability study, HAZOP, auch PAAG-Verfahren) .....	93
C.6.3 Analyse von Ausfällen infolge gemeinsamer Ursache .....	94

	<b>Seite</b>
C.6.4 Markov-Modelle .....	94
C.6.5 Zuverlässigkeits-Blockdiagramm .....	95
C.6.6 Monte-Carlo Simulation .....	96
Anhang D (informativ) Ein probabilistischer Ansatz zur Bestimmung der Sicherheitsintegrität von vorentwickelter Software .....	97
D.1 Allgemeines .....	97
D.2 Gleichungen für statistische Tests und ihre Anwendungen .....	98
D.2.1 Einfacher statistischer Test für die Betriebsart mit niedriger Anforderungsrate .....	98
D.2.2 Test des Wertebereichs der Eingänge für die Betriebsart mit niedriger Anforderungsrate .....	98
D.2.3 Einfacher statistischer Test für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung .....	99
D.2.4 Vollständiger Test .....	100
D.3 Literaturhinweise .....	101
Literaturhinweise .....	102
Stichwortverzeichnis .....	104
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen .....	111
<b>Bilder</b>	
Bild 1 – Gesamtrahmen der Betrachtung der IEC 61508 .....	12
<b>Tabellen</b>	
Tabelle C.1 – Empfehlungen für bestimmte Programmiersprachen .....	81
Tabelle D.1 – Notwendige Vorgeschichte zur Zuordnung von Sicherheits-Integritätsleveln bei gegebenem Vertrauensniveau .....	97
Tabelle D.2 – Wahrscheinlichkeiten eines Versagens für die Betriebsart mit niedriger Anforderungsrate .....	98
Tabelle D.3 – Mittlerer Abstand von zwei Testpunkten .....	99
Tabelle D.4 – Wahrscheinlichkeit eines Versagens für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung .....	100
Tabelle D.5 – Wahrscheinlichkeit des Tests aller Programmeigenschaften .....	101