

	DIN EN 61508-7 (VDE 0803-7)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 35.240.50	Einsprüche bis 2009-08-31 Vorgesehen als Ersatz für DIN EN 61508-7 (VDE 0803-7):2003-06 Entwurf	
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (IEC 65A/528/CDV:2008); Deutsche Fassung FprEN 61508-7:2008		
Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures (IEC 65A/528/CDV:2008); German version FprEN 61508-7:2008		
Anwendungswarnvermerk		
Dieser Norm-Entwurf mit Erscheinungsdatum 2009-06-15 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.		
Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.		
Stellungnahmen werden erbeten		
– vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.		
Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.		
Gesamtumfang 300 Seiten		
DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Diese Norm gilt ab

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 61508-7:2008 „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 65A/528/CDV:2008 „Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures“ unverändert in den Entwurf FprEN 61508-7:2008 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 65A „System aspects“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Änderungen

Gegenüber DIN EN 61508-7 (VDE 0803-7):2003-06 wurden folgende Änderungen vorgenommen:

- a) Textliche Überarbeitung;
- b) Beschreibung der Verfahren und Maßnahmen an den Stand der Technik angepasst;
- c) Hinzufügung des Anhanges E „Überblick über Verfahren und Maßnahmen für den Entwurf von ASICs“;
- d) Hinzufügung des Anhanges F „Definitionen der Eigenschaften der Software-Lebenszyklusphasen.“;
- e) Hinzufügung des Anhanges G „Anleitung zur Entwicklung von sicherheitsbezogener objektorientierter Software“.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils neueste gültige Ausgabe der in Bezug genommenen Norm.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm.

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
	ISO/IEC Guide 51:1999		
	IEC Guide 104:1997		
FprEN61508-1:2008	65A/522/CDV:2008	E DIN EN 61805-1 (VDE 0803-1) in Vorbereitung	(VDE 0803-1)
FprEN61508-2:2008	65A/523/CDV:2008	E DIN EN 61805-2 (VDE 0803-2) in Vorbereitung	(VDE 0803-2)
FprEN61508-3:2008	65A/524/CDV:2008	E DIN EN 61805-3 (VDE 0803-3) in Vorbereitung	(VDE 0803-3)
FprEN61508-4:2008	65A/525/CDV:2008	E DIN EN 61805-4 (VDE 0803-4) in Vorbereitung	(VDE 0803-4)
FprEN61508-5:2008	65A/526/CDV:2008	E DIN EN 61805-5 (VDE 0803-5) in Vorbereitung	(VDE 0803-5)
FprEN61508-6:2008	65A/527/CDV:2008	E DIN EN 61805-6 (VDE 0803-6) in Vorbereitung	(VDE 0803-6)

Nationaler Anhang NB (informativ)

Literaturhinweise

E DIN EN 61805-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

E DIN EN 61805-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

E DIN EN 61805-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

— Entwurf —

E DIN EN 61508-7 (VDE 0803-7):2009-06

E DIN EN 61805-4 (VDE 0803-4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen*

E DIN EN 61805-5 (VDE 0803-5), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele von Methoden für die Bestimmung von Sicherheits-Integritätsleveln*

E DIN EN 61805-6 (VDE 0803-6), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3*

Deutsche Fassung

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer
Systeme –

Teil 7: Anwendungshinweise über Verfahren und Maßnahmen

Inhalt

	Seite
Einleitung	9
1 Anwendungsbereich	11
2 Normative Verweisungen	13
3 Begriffe und Abkürzungen	13
Anhang A (informativ) Überblick über Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE- Systeme: 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 Vergleiche	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 (Nicht verwendet)	16
A.2.5 Überwachte Redundanz	16
A.2.6 Hardware mit automatischen Tests	16
A.2.7 Analogsignal-Überwachung	17
A.2.8 Unterlastung	17
A.3 Verarbeitungseinheiten (CPUs)	17
A.3.1 Selbsttest durch Software: begrenzte Anzahl von Mustern (ein Kanal)	17
A.3.2 Selbsttest durch 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

	Seite
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.....	21
A.5.1 RAM-Test „Checkerboard“ oder „March“	22
A.5.2 RAM-Test „Walkpath“	22
A.5.3 RAM-Test „Galpat“ oder „transparenter Galpat“	22
A.5.4 RAM-Test „Abraham“	23
A.5.5 Ein-Bit-Redundanz (zum Beispiel RAM-Überwachung mit einem Parity-Bit).....	23
A.5.6 RAM-Überwachung mit einem modifizierten Hammingcode oder Erkennung von Datenfehlern mit fehlererkennenden und -korrigierenden Codes (en: error-detection- correction codes, EDC).....	24
A.5.7 Doppeltes RAM mit Hardware- oder Softwarevergleich und Schreib-/Lesetest.....	24
A.6 E/A-Einheiten und Schnittstellen (externe Kommunikation)	24
A.6.1 Testmuster	24
A.6.2 Codesicherung	25
A.6.3 Mehrkanalige parallele Ausgabe	25
A.6.4 Überwachte Ausgaben	25
A.6.5 Eingabevergleich/-entscheidung.....	26
A.7 Datenwege (interne Kommunikation)	26
A.7.1 Ein-Bit-Hardware redundanz	26
A.7.2 Mehr-Bit-Hardware redundanz	26
A.7.3 Vollständige Hardware redundanz.....	26
A.7.4 Inspektion durch Verwendung von Testmustern	27
A.7.5 Übertragungsredundanz	27
A.7.6 Informationsredundanz	27
A.8 Spannungsversorgung.....	27
A.8.1 Überspannungsschutz mit Sicherheitsabschaltung.....	27
A.8.2 Spannungsüberwachung (sekundärseitig)	28
A.8.3 Energieabschaltung mit Sicherheitsabschaltung.....	28
A.9 Zeitliche und logische Programmlaufüberwachung.....	28
A.9.1 Watchdog mit separater Zeitbasis ohne Zeitfenster	28
A.9.2 Watchdog mit separater Zeitbasis und Zeitfenster	28
A.9.3 Logische Überwachung des Programmablaufs.....	29
A.9.4 Kombination von zeitlicher und logischer Überwachung des Programmablaufs	29
A.9.5 Zeitliche Überwachung mit Test während des Betriebs	29
A.10 Lüftung und Beheizung.....	29
A.10.1 Temperatursensor.....	29
A.10.2 Lüfterkontrolle	30

	Seite
A.10.3 Auslösung der Sicherheitsabschaltung über eine thermische Sicherung	30
A.10.4 Gestaffelte Meldung von Thermosensoren und bedingter Alarm.....	30
A.10.5 Zuschaltung von Fremdkühlung und Statusanzeige	30
A.11 Kommunikation und Massenspeicher	30
A.11.1 Trennung elektrischer Energieleitungen von Informationsleitungen	30
A.11.2 Räumliche Trennung mehrfacher Leitungen	30
A.11.3 Erhöhung der Störfestigkeit	31
A.11.4 Antivalente Signalübertragung	31
A.12 Sensoren	31
A.12.1 Referenzsensor	31
A.12.2 Zwangsöffnender Schalter.....	32
A.13 Stellglieder (Aktoren)	32
A.13.1 Überwachung	32
A.13.2 Kreuzweise Überwachung mehrfacher Aktoren	32
A.14 Maßnahmen gegen die Einwirkung der physikalischen Umgebung	33
Anhang B (informativ) Überblick über Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE- Systeme: Vermeidung von systematischen Ausfällen (siehe IEC 61508-2 und IEC 61508-3).....	34
B.1 Allgemeine Maßnahmen und Verfahren.....	34
B.1.1 Projektmanagement	34
B.1.2 Dokumentation	35
B.1.3 Trennung sicherheitsbezogener Systeme von nicht sicherheitsbezogenen Systemen	36
B.1.4 Diversitäre Hardware	36
B.2 Spezifikation der Entwurfsanforderungen des E/E/PE-Systems.....	36
B.2.1 Strukturierte Spezifikation.....	36
B.2.2 Formale Methoden	37
B.2.3 Semi-formale Methoden	37
B.2.4 Rechnerunterstützte Spezifikationswerkzeuge	39
B.2.5 Checklisten	41
B.2.6 Inspektion der Spezifikation.....	41
B.3 Entwurf und Entwicklung des E/E/PE-Systems.....	42
B.3.1 Beachtung von Richtlinien und Normen	42
B.3.2 Strukturierter Entwurf.....	42
B.3.3 Verwendung von bewährten Bauteilen.....	43
B.3.4 Modularisierung	44
B.3.5 Rechnerunterstützte Entwurfswerkzeuge.....	44
B.3.6 Simulation	45
B.3.7 Inspektion (Überprüfungen und Analysen).....	45
B.3.8 Walkthrough.....	46
B.4 Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems.....	46

	Seite
B.4.1 Betriebs- und Instandhaltungsanweisungen.....	46
B.4.2 Benutzerfreundlichkeit	46
B.4.3 Instandhaltungsfreundlichkeit	47
B.4.4 Eingeschränkte Betriebsmöglichkeiten.....	47
B.4.5 Betrieb nur durch erfahrene Bediener	47
B.4.6 Schutz gegen Irrtümer des Bedieners	48
B.4.7 (Nicht verwendet).....	48
B.4.8 Schutz vor Modifikation.....	48
B.4.9 Eingabebestätigung	48
B.5 Integration des E/E/PE-Systems	48
B.5.1 Funktionstest.....	49
B.5.2 Black-Box Test.....	49
B.5.3 Statistisches Testen.....	50
B.5.4 Felderfahrung.....	51
B.6 Validierung der Sicherheit des E/E/PE-Systems	51
B.6.1 Funktionstest unter Umgebungsbedingungen	51
B.6.2 Test der Störfestigkeit gegen Stoßspannungen	52
B.6.3 (Nicht verwendet).....	52
B.6.4 Statische Analyse	52
B.6.5 Dynamische Analyse	53
B.6.6 Ausfallanalyse.....	53
B.6.7 Worst-Case Analyse	59
B.6.8 Erweiterte Funktionstests	59
B.6.9 Test unter Grenzbedingungen	60
B.6.10 Test durch Fehlereinbau	60
Anhang C (informativ) Überblick über Verfahren und Maßnahmen zum Erreichen der Sicherheitsintegrität der Software (siehe IEC 61508-3)	61
C.1 Allgemeines	61
C.2 Anforderungen und detaillierter Entwurf	61
C.2.1 Strukturierte schematische Methoden	61
C.2.2 Datenflussdiagramme	63
C.2.3 Strukturdiagramme	64
C.2.4 Formale Methoden.....	65
C.2.5 Defensive Programmierung	69
C.2.6 Entwurfs- und Programmierrichtlinien.....	70
C.2.7 Strukturierte Programmierung	75
C.2.8 Information Hiding/Kapselung.....	75
C.2.9 Modularisierung	76
C.2.10 Verwendung bewährter/verifizierter Softwareelemente.....	77

	Seite
C.2.11 Nachvollziehbarkeit	79
C.2.12 Softwareentwurf und Softwareentwicklung: Entwurf der Software-Architektur - zustandsloser Entwurf (oder Entwurf eingeschränkter Zustände)	80
C.2.13 Numerische Offline-Analyse	81
C.2.14 Nachrichtenverlaufstabellen	81
C.3 Entwurf der Architektur	81
C.3.1 Fehlererkennung und Diagnose	81
C.3.2 Fehlererkennende und korrigierende Codes	82
C.3.3 Assertion-Programmierung (en: failure assertion programming)	82
C.3.4 Diversitäre Überwachungseinrichtung	83
C.3.5 Diversitäre Programmierung	83
C.3.6 Rückwärtsregeneration	84
C.3.7 Regeneration durch Wiederholung	84
C.3.8 Abgestufte Funktionseinschränkungen	85
C.3.9 Künstliche Intelligenz – Fehlerkorrektur	85
C.3.10 Dynamische Rekonfiguration	86
C.3.11 Sicherheit und Leistungsfähigkeit in Echtzeit: zeitgesteuerte Architektur	86
C.4 Entwicklungswerkzeuge und Programmiersprachen	87
C.4.1 Streng typisierte Programmiersprache	87
C.4.2 Sprachenteilmenge	88
C.4.3 Zertifizierte Werkzeuge und Compiler	88
C.4.4 Betriebsbewährte Werkzeuge und Compiler	89
C.4.5 Geeignete Programmiersprache	90
C.4.7 Testmanagement und Automatisierungswerkzeuge	93
C.5 Verifikation und Modifikation	93
C.5.1 Probabilistisches Testen	93
C.5.2 Datenaufzeichnung und Analyse	94
C.5.3 Schnittstellenprüfung	94
C.5.4 Durchführung von Testfällen nach einer Grenzwertanalyse	95
C.5.5 Durchführung von Testfällen aus der Fehlerschätzung („Fehler erraten“)	95
C.5.6 Durchführung von Testfällen aus Einbringung von Fehlern	96
C.5.7 Äquivalenzklassentest (aufgrund von Partitionen des Eingangsbereichs)	96
C.5.8 Strukturabhängige Prüfungen	97
C.5.9 Steuerflussanalyse	97
C.5.10 Datenflussanalyse	98
C.5.11 Symbolische Ausführung	98
C.5.12 Formaler Beweis (Verifikation)	99
C.5.13 Software-Komplexitätsmetriken	100
C.5.14 Formale Inspektion	101

	Seite
C.5.15 Walkthrough (Software)	101
C.5.16 Entwurfsüberprüfung	102
C.5.17 Prototypenerstellung/Animation	102
C.5.18 Simulation des Prozesses	103
C.5.19 Anforderungen an die Leistungsfähigkeit	103
C.5.20 Modellierung der Leistungsfähigkeit	104
C.5.21 Belastungstest (en: Avalanche/stress testing)	104
C.5.22 Reaktionszeiten und Speicherbeschränkungen	105
C.5.23 Einflussanalyse	105
C.5.24 Konfigurationsmanagement der Software	105
C.5.25 Validierung der Regressionstests	106
C.5.26 Animation der Spezifikation und des Entwurfs	106
C.6 Beurteilung der funktionalen Sicherheit	107
C.6.1 Entscheidungs-/Wahrheitstabellen	107
C.6.2 Software-Gefährdungs- und Betreibbarkeitsuntersuchung (en: software hazard and operability study, CHAZOP, FMEA)	107
C.6.3 Analyse von Ausfällen infolge gemeinsamer Ursache	108
C.6.4 Zuverlässigkeits-Blockdiagramm	108
Anhang D (informativ) Ein probabilistischer Ansatz zur Bestimmung der Sicherheitsintegrität von vorentwickelter Software	110
D.1 Allgemeines	110
D.2 Gleichungen für statistische Tests und ihre Anwendungen	111
D.2.1 Einfacher statistischer Test für die Betriebsart mit niedriger Anforderungsrate	111
D.2.2 Test des Wertebereichs der Eingänge für die Betriebsart mit niedriger Anforderungsrate	111
D.2.3 Einfacher statistischer Test für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung	112
D.2.4 Vollständiger Test	113
D.3 Literaturhinweise	114
Anhang E (informativ) Überblick über Verfahren und Maßnahmen für den Entwurf von ASICs	115
E.1 Entwurfsbeschreibung in (V)HDL	115
E.2 Schaltplaneingabe	115
E.3 Strukturierte Beschreibungsmethodik	115
E.4 Betriebsbewährte Werkzeuge	116
E.5 (V)HDL-Simulation	116
E.6 Funktionstest auf Modulebene	116
E.7 Funktionstest auf oberster Ebene	117
E.8 Funktionstest eingebettet in Systemumgebung	117
E.9 Eingeschränkte Verwendung asynchroner Konstrukte	117
E.10 Synchronisation von primären Eingängen und Kontrolle von Metastabilitäten	117

	Seite
E.11 Entwurf für Testbarkeit	118
E.12 Modularisierung	118
E.13 Testabdeckung der Verifikationsszenarien (Testbenches)	118
E.14 Beachtung von Programmierrichtlinien	119
E.15 Verwendung eines Codecheckers.....	120
E.16 Defensive Programmierung.....	120
E.17 Dokumentation von Simulationsergebnissen	120
E.18 Codeinspektion	121
E.19 Walkthrough.....	121
E.20 Anwendung validierter Soft-Cores.....	121
E.21 Validierung von Soft-Cores.....	122
E.22 Simulation der Gatter-Netzliste zur Überprüfung der Zeitvorgaben.....	122
E.23 Statische Laufzeitanalyse (STA)	122
E.24 Vergleich der Gatter-Netzliste gegen ein Referenzmodell durch Simulation	123
E.25 Vergleich der Gatter-Netzliste mit dem Referenzmodell (formale Äquivalenzprüfung).....	123
E.26 Überprüfung der Anforderungen und Beschränkungen des Herstellers	123
E.27 Dokumentation der Synthesevorgaben, Ergebnisse und Werkzeuge	124
E.28 Verwendung von betriebsbewährten Synthesewerkzeugen	124
E.29 Verwendung von betriebsbewährten Zielbibliotheken.....	124
E.30 Skriptbasierende Verfahren.....	124
E.31 Implementierung von Teststrukturen.....	125
E.32 Abschätzung der Testabdeckung durch Simulation	125
E.33 Abschätzung der Testabdeckung durch Anwendung eines ATPG-Werkzeugs.....	126
E.34 Nachweis der Betriebsbewährung für verwendete Hard-Cores	126
E.35 Verwendung validierter Hard-Cores	126
E.36 Online-Tests der Hard-Cores	126
E.37 Design-Rule-Check (DRC)	126
E.38 Überprüfung des Layouts gegen die Netzliste (LVS)	127
E.39 Zusätzliche Reserven (> 20 %) für Prozesstechnologien mit weniger als 3 Jahren Anwendung.....	127
E.40 Burn-in-Test.....	127
E.41 Verwendung von betriebsbewährten Schaltkreisfamilien.....	127
E.42 Betriebsbewährter Fertigungsprozess.....	127
E.43 Qualitätskontrolle des Fertigungsprozesses	128
E.44 Produktions-Qualitätsprüfung des Schaltkreises.....	128
E.45 Funktionale Qualitätsprüfung des Schaltkreises	128
E.46 Qualitätsnormen	128
Anhang F (informativ) Definitionen der Eigenschaften der Software-Lebenszyklusphasen	129
Anhang G (informativ) Anleitung zur Entwicklung von sicherheitsbezogener objektorientierter	

	Seite
Software	136
Literaturhinweise	138
Index.....	140
Bilder	
Bild 1 – Gesamtrahmen der IEC 61508	12
Tabellen	
Tabelle C.1 – Empfehlungen für bestimmte Programmiersprachen.....	91
Tabelle D.1 – Notwendige Vorgeschichte zur Zuordnung von Sicherheits-Integritätsleveln bei gegebenem Vertrauensniveau.....	110
Tabelle D.2 – Wahrscheinlichkeiten eines Versagens für die Betriebsart mit niedriger Anforderungsrate	111
Tabelle D.3 – Mittlerer Abstand von zwei Testpunkten	112
Tabelle D.4 – Wahrscheinlichkeit eines Versagens für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung.....	113
Tabelle D.5 – Wahrscheinlichkeit des Tests aller Programmeigenschaften.....	114
Tabelle F.1 – Spezifikation der Software-Sicherheitsanforderungen.....	129
Tabelle F.2 – Softwareentwurf und Softwareentwicklung: Entwurf der Software-Architektur	130
Tabelle F.3 – Softwareentwurf und Softwareentwicklung: Hilfswerkzeuge und Programmiersprache	131
Tabelle F.4 – Softwareentwurf und Softwareentwicklung: detaillierter Entwurf	131
Tabelle F.5 – Softwareentwurf und Softwareentwicklung: Test der Softwaremodule und Integration	132
Tabelle F.6 – Integration der programmierbaren Elektronik (Hardware und Software).....	132
Tabelle F.7 – Softwareaspekte bezüglich der Validierung der Systemsicherheit.....	133
Tabelle F.8 – Software-Modifikation	133
Tabelle F.9 – Software-Verifikation	134
Tabelle F.10 – Beurteilung der funktionalen Sicherheit	134
Tabelle G.1 – Objektorientierte Software-Architektur	136
Tabelle G.2 – Detaillierter objektorientierter Entwurf	137
Tabelle G.3 – Einige detaillierte objektorientierte Begriffe	137

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Elementen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme) werden in allen Anwendungsbereichen benutzt, um Nichtsicherheitsfunktionen und zunehmend auch um Sicherheitsfunktionen auszuführen. Falls Rechnersystemtechnologie wirksam und sicherheitsgerichtet eingesetzt wird, ist es wichtig, dass die für die Entscheidungsfindung Verantwortlichen ausreichende Hilfestellung bezüglich der Sicherheitsaspekte erhalten, nach denen diese Entscheidungen getroffen werden.

Diese Internationale Norm beschreibt einen allgemeinen Lösungsweg für alle Tätigkeiten während des Sicherheitslebenszyklus für Systeme, die aus elektrischen und/oder elektronischen und/oder programmierbaren elektronischen (E/E/PE) Elementen bestehen und die eingesetzt werden, um Sicherheitsfunktionen auszuführen. Dieser allgemeine Lösungsweg wurde gewählt, um ein sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme zu entwickeln. Ein Hauptziel ist es, die Entwicklung von anwendungsspezifischen Normen zu erleichtern.

In den meisten Situationen wird Sicherheit durch eine Anzahl von Systemen erreicht, die auf vielerlei Technologien (zum Beispiel Mechanik, Hydraulik, Pneumatik, Elektrik, Elektronik, programmierbare Elektronik) basieren. Jede Sicherheitsstrategie muss deshalb nicht nur alle Elemente innerhalb eines Einzelsystems (zum Beispiel Sensoren, Steuereinheiten und Aktoren) betrachten, sondern auch all die sicherheitsbezogenen Systeme, welche die Gesamtheit von sicherheitsbezogenen Systemen bilden. Da sich diese Internationale Norm mit sicherheitsbezogenen E/E/PE-Systemen beschäftigt, kann sie auch einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme, basierend auf anderen Technologien, betrachtet werden können.

Es ist berücksichtigt worden, dass eine große Vielfalt von Anwendungen in vielfältigen Anwendungsbereichen vorliegt, die sicherheitsbezogene E/E/PE-Systeme verwenden und diese einen weiten Bereich in Bezug auf Komplexität, Gefährdungs- und Risikopotentiale abdeckt. In jeder speziellen Anwendung sind die erforderlichen Sicherheitsmaßnahmen von vielen anwendungsspezifischen Faktoren abhängig. Dadurch, dass diese Internationale Norm allgemein gehalten ist, wird die Formulierung solcher Maßnahmen in zukünftigen anwendungsspezifischen internationalen Normen und in Revisionen der bereits bestehenden Normen ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Implementierung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PE-Systeme benutzt werden, um Sicherheitsfunktionen auszuführen;
- wurde unter Berücksichtigung einer sich schnell entwickelnden Technologie entworfen. Der Betrachtungsrahmen ist ausreichend robust und ausführlich genug, um auch für zukünftige Entwicklungen verwendbar zu sein;
- ermöglicht die Erstellung anwendungsspezifischer internationaler Normen, die sich mit sicherheitsbezogenen E/E/PE-Systemen befassen. Die Entwicklung anwendungsspezifischer internationaler Normen sollte innerhalb des Rahmens dieser Norm zu einem hohen Grad an Übereinstimmung (zum Beispiel von zugrunde liegenden Prinzipien, Terminologie usw.) führen, sowohl innerhalb der Anwendungsbereiche als auch über die Anwendungsbereiche hinweg. Dies hat sowohl sicherheitstechnische als auch wirtschaftliche Vorteile;

ANMERKUNG 1 Hinweise [1] und [2] in den Literaturhinweisen sind anwendungsspezifische internationale Normen.

- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die erforderliche funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen;
- verwendet einen auf dem Risiko basierenden Lösungsansatz, durch den die Anforderungen zur Sicherheitsintegrität bestimmt werden können;

- führt Sicherheits-Integritätslevel für die Festlegung der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen, die von den sicherheitsbezogenen E/E/PE-Systemen zu implementieren sind, ein;

ANMERKUNG 2 Diese Norm legt weder die Anforderungen zur Sicherheitsintegrität für irgendeine Sicherheitsfunktion fest noch bestimmt sie, wie der Sicherheits-Integritätslevel festgelegt wird. Stattdessen stellt sie einen risikobasierenden konzeptionellen Rahmen und Beispielverfahren bereit.

- legt Ausfallgrenzwerte für die von den sicherheitsbezogenen E/E/PE-Systemen auszuführenden Sicherheitsfunktionen fest, die mit den Sicherheits-Integritätsleveln verbunden sind;
- legt eine untere Grenze für die Ausfallgrenzwerte für eine Sicherheitsfunktion fest, die von einem einzelnen sicherheitsbezogenen E/E/PE-System ausgeführt wird. Für sicherheitsbezogene E/E/PE-Systeme, die
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze bei einer mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung von 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen Anforderungsrate oder bei kontinuierlicher Anforderung betrieben werden, ist die untere Grenze bei einer mittleren Häufigkeit gefahrbringender Ausfälle von $10^{-9} [h^{-1}]$ festgelegt;

ANMERKUNG 3 Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht notwendigerweise eine einkanalige Architektur.

ANMERKUNG 4 Es kann für einfache Systeme möglich sein, Entwürfe von sicherheitsbezogenen Systemen mit niedrigeren Zielwerten für die Sicherheitsintegrität zu erreichen, aber diese Grenzen werden als das betrachtet, was für relativ komplexe Systeme (zum Beispiel sicherheitsbezogene programmierbare elektronische Systeme) gegenwärtig erreicht werden kann.

- legt Anforderungen für die Vermeidung und Beherrschung von systematischen Fehlern fest, die auf Erfahrung und Urteilsvermögen beruhen, das durch praktische Erfahrung in der Industrie gewonnen wurde. Wenn auch die Wahrscheinlichkeit des Auftretens systematischer Ausfälle im Allgemeinen nicht quantifiziert werden kann, erlaubt die Norm jedoch für eine festgelegte Sicherheitsfunktion den Anspruch zu erheben, dass der mit der Sicherheitsfunktion verbundene Ausfallgrenzwert als erreicht betrachtet werden kann, wenn alle Anforderungen dieser Norm erfüllt worden sind;
- lässt einen weiten Bereich von Prinzipien, Verfahren und Maßnahmen zu, um funktionale Sicherheit für sicherheitsbezogene E/E/PE-Systeme zu erreichen, verwendet aber nicht das Fail-Safe-Konzept, das genutzt werden kann, wenn das Ausfallverhalten eindeutig definiert und das Niveau der Komplexität verhältnismäßig niedrig ist. Das Fail-Safe-Konzept wurde wegen des weiten Bereiches der Komplexität von sicherheitsbezogenen E/E/PE-Systemen, die im Rahmen der Norm behandelt werden, als ungeeignet betrachtet.

1 Anwendungsbereich

1.1 Dieser Teil der IEC 61508 beinhaltet einen Überblick über verschiedene Sicherheitsverfahren und -maßnahmen zur Anwendung der IEC 61508-2 und IEC 61508-3.

Die Literaturhinweise sollten als grundlegende Verweise auf Methoden und Werkzeuge oder als Beispiele betrachtet werden und können möglicherweise nicht den Stand der Technik wiedergeben.

1.2 Die Teile 1, 2, 3 und 4 dieser Norm sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen sicherheitsbezogenen E/E/PE-Systemen nicht anwendbar (siehe 3.4.4 von Teil 4). Als Sicherheits-Grundnormen sind sie zur Verwendung durch technische Komitees bei der Erstellung von Normen nach IEC Guide 104 und ISO/IEC Guide 51 vorgesehen. Die Teile 1, 2, 3 und 4 sind ebenfalls zur Verwendung als eigenständige Norm vorgesehen. Die horizontale Sicherheitsfunktion dieser internationalen Norm trifft nicht auf medizinische Einrichtungen gemäß IEC 60601 zu.

Es steht in der Verantwortlichkeit eines Technischen Komitees, zur Vorbereitung und Erstellung eigener Festlegungen soweit möglich die Sicherheits-Grundnormen anzuwenden. In diesem Zusammenhang gilt, dass die Anforderungen, Prüfverfahren oder Prüfbedingungen dieser Sicherheits-Grundnorm nur dann anwendbar sind, wenn in den Festlegungen der Technischen Komitees darauf verwiesen wird oder diese eingebunden werden.

1.3 Bild 1 zeigt den gesamten Rahmen für die Teile 1 bis 7 der IEC 61508 und zeigt die Rolle, die IEC 61508-4 zum Erreichen der funktionalen Sicherheit der sicherheitsbezogenen E/E/PE-Systeme spielt.

Bild 1 – Gesamtrahmen der IEC 61508

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for the inclusion of in standards*

IEC Guide 104:1997, *Guide to the drafting of safety standards, and the role of Committees with safety pilot functions and safety group functions*

IEC 61508-1:—, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:—, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related systems*

IEC 61508-3:—, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:—, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:—, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:—, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

ANMERKUNG Für eine Einleitung in die Normenreihe IEC 61508 siehe Literaturhinweis [20].

3 Begriffe und Abkürzungen

Für die Anwendung dieses Teils der IEC 61508 gelten die in IEC 61508-4 aufgeführten Begriffe und Abkürzungen.

Anhang A (informativ)

Überblick über Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Beherrschung von zufälligen Hardwareausfällen (siehe IEC 61508-2)

A.1 Elektrik

Allgemeines Ziel: Beherrschung von Ausfällen in elektromechanischen Bauteilen.

A.1.1 Erkennung von Ausfällen durch Überwachung während des Betriebs

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.2, A.3, A.7 und A.13 bis A.18 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen durch Überwachung des Verhaltens des sicherheitsbezogenen E/E/PE-Systems in Bezug auf den normalen (Online) Betrieb der EUC.

Beschreibung: Unter bestimmten Bedingungen können Ausfälle durch (zum Beispiel) die Verwendung von Informationen über das Zeitverhalten der EUC erkannt werden. Wenn zum Beispiel ein Schalter, der Teil eines sicherheitsbezogenen E/E/PE-Systems ist und normalerweise durch die EUC betätigt wird, seinen Zustand nicht zur erwarteten Zeit ändert, wird ein Ausfall erkannt. Es ist gewöhnlich nicht möglich, den Ausfall zu lokalisieren.

A.1.2 Überwachung von Relaiskontakten

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.2 und A.14 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen von Relaiskontakten (zum Beispiel Verschweißen).

Beschreibung: Zwangsgeführte Relais sind derart entworfen, dass ihre Kontakte fest miteinander verbunden sind. Wenn, ausgehend von zwei Sätzen von Wechselkontakten *a* und *b*, der Schließerkontakt *a* verschweißt, kann der Öffnerkontakt *b* bei der nächsten Entregung der Relaispule nicht schließen. Daher kann die Überwachung des Schließens des Öffnerkontakts *b* bei Entregung der Relaispule verwendet werden, um zu prüfen, ob der Schließerkontakt *a* geöffnet hat. Das Nichtschließen des Öffnerkontakts *b* zeigt einen Ausfall von Kontakt *a* an, so dass der Überwachungskreis eine sichere Abschaltung und ggf. eine Fortsetzung des sicheren Abschaltens für jede Maschine, die durch Kontakt *a* angesteuert wird, gewährleistet.

Literaturhinweise:

Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. F. Kreutzkamp, W. Hertel, Sicherheitstechnisches Informations- und Arbeitsblatt 330212, BIA-Handbuch. 17. Lfg. X/91, Erich Schmidt Verlag, Bielefeld.

Anlagensicherung mit Mitteln der MSR-Technik. G. Strohrman, Oldenburg, 1983.

A.1.3 Vergleich

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.2, A.3 und A.4 der IEC 61508-2 aufgeführt.

Ziel: So früh wie möglich Erkennung von (nicht-gleichzeitigen) Ausfällen in einer unabhängigen Verarbeitungseinheit oder im Vergleich.

Beschreibung: Die Signale unabhängiger Verarbeitungseinheiten werden zyklisch oder kontinuierlich von einem Hardware-Vergleicher verglichen. Der Vergleich selbst kann extern getestet werden oder selbstüberwachende Technologie verwenden. Erkannte Unterschiede im Verhalten der Prozessoren führen zu einer Ausfallmeldung.

A.1.4 Mehrheitsentscheider

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.2, A.3 und A.4 der IEC 61508-2 aufgeführt.

Ziel: Erkennung und Maskierung von Ausfällen in einem von mindestens drei Hardware-Kanälen.

Beschreibung: Eine Entscheidungseinheit nach dem Mehrheitsprinzip (2 aus 3, 3 aus 3 oder m aus n) wird zur Erkennung und Maskierung von Ausfällen verwendet. Die Einheit selbst kann extern getestet werden oder selbstüberwachende Technologie verwenden.

Literaturhinweise:

Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

Anlagensicherung mit Mitteln der MSR-Technik. Praxis der Sicherheitstechnik, Vol. 1, Dechema, 1988.

Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Mess-, Steuerungs- und Regelungstechnik. VDI/VDE 2180 Blatt 1 bis 5, 1984 bis 1988.

A.1.5 Ruhestromprinzip

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.13 und A.16 der IEC 61508-2 aufgeführt.

Ziel: Ausführung der Sicherheitsfunktion bei Energieunterbrechung oder -verlust.

Beschreibung: Die Sicherheitsfunktion wird ausgeführt, wenn die Kontakte offen sind und kein Strom fließt. Werden zum Beispiel Bremsen zum Anhalten einer gefahrbringenden Bewegung eines Motors verwendet, dann werden die Bremsen durch das Schließen von Kontakten in dem sicherheitsbezogenen System gelöst und durch das Öffnen der Kontakte im sicherheitsbezogenen System betätigt.

Literaturhinweis: Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

A.2 Elektronik

Allgemeines Ziel: Beherrschung von Ausfällen in Halbleiter-Bauelementen.

A.2.1 Tests durch redundante Hardware

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.3, A.15, A.16 und A.18 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen durch Verwendung von Hardwareredundanz, d. h. Verwendung zusätzlicher Hardware, die nicht erforderlich ist, um die Prozessfunktionen auszuführen.

Beschreibung: Redundante Hardware kann verwendet werden, um mit angemessener Häufigkeit die festgelegten Sicherheitsfunktionen zu testen. Dieser Ansatz ist normalerweise zur Realisierung von A.1.1 oder A.2.2 notwendig.

A.2.2 Dynamische Prinzipien

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.3 der IEC 61508-2 aufgeführt.

Ziel: Erkennung statischer Ausfälle durch dynamische Signalverarbeitung.

Beschreibung: Ein erzwungener Wechsel von normalerweise statischen Signalen (intern oder extern erzeugt) hilft, statische Ausfälle in Bauteilen zu erkennen. Dieses Verfahren wird oft mit elektromechanischen Bauteilen in Verbindung gebracht.

Literaturhinweis: Elektronik in der Sicherheitstechnik. H. Jürs, D. Reinert, Sicherheitstechnisches Informations- und Arbeitsblatt 330220, BIA-Handbuch, Erich-Schmidt Verlag, Bielefeld 1993.

A.2.3 Standardtestschnittstelle (Access Port) und Boundary-Scan Architektur

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.3, A.15 und A.18 der IEC 61508-2 aufgeführt.

Ziel: Steuerung und Beobachtung der Ereignisse an jedem Anschluss eines ICs.

Beschreibung: Der Boundary-Scan-Test ist ein IC-Entwurfsverfahren, das die Testbarkeit des ICs verbessert, indem das Problem gelöst wurde, einen Zugriff auf die Testpunkte des Schaltkreises im Inneren des ICs zu erhalten. In einem typischen Boundary-Scan-IC, das aus einer Kernlogik und Eingabe- und Ausgabepuffern besteht, wird eine Schieberegisterstufe zwischen der Kernlogik und den Eingabe- und Ausgabepuffern, die mit jedem IC-Anschluss verbunden sind, platziert. Jede Schieberegisterstufe ist in einer Boundary-Scan-Zelle enthalten. Die Boundary-Scan-Zelle kann die Ereignisse an jedem Eingabe- und Ausgabeanschluss eines ICs über den standardisierten Testanschluss steuern und beobachten. Die interne Testung der IC-Kernlogik wird durch Isolation der auf dem Chip befindlichen Kernlogik von den Signalen der umgebenden Bauteilen und anschließender interner Selbsttests erreicht. Diese Tests können zur Ausfallerkennung im IC verwendet werden.

Literaturhinweis: IEEE 1149.1:1990, Standard Test Access Port and Boundary-Scan Architecture.

A.2.4 (Nicht verwendet)

A.2.5 Überwachte Redundanz

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.3 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen durch Bereitstellung mehrerer funktionaler Einheiten, durch Überwachung des Verhaltens jeder dieser Einheiten, um Ausfälle zu erkennen, und durch Einleiten eines Übergangs in einen sicheren Zustand, wenn irgendeine Unstimmigkeit im Verhalten erkannt wird.

Beschreibung: Die Sicherheitsfunktion wird durch mindestens zwei Hardware-Kanäle ausgeführt. Die Ausgaben dieser Kanäle werden überwacht, und ein sicherer Zustand wird eingeleitet, wenn ein Fehler erkannt wird (d. h. wenn die Ausgabesignale von allen Kanälen nicht identisch sind).

Literaturhinweise:

Elektronik in der Sicherheitstechnik. H. Jürs, D. Reinert, Sicherheitstechnisches Informations- und Arbeitsblatt 330220, BIA-Handbuch, Erich-Schmidt Verlag Bielefeld, 1993.

Dependability of Critical Computer Systems 1. F. J. Redmill, Elsevier Applied Science, 1988, ISBN 1-85166-203-0.

A.2.6 Hardware mit automatischen Tests

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.3 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Fehlern durch periodische Tests der Sicherheitsfunktionen.

Beschreibung: Die Hardware wird vor Anlauf des Prozesses und zyklisch in geeigneten Intervallen getestet. Die EUC setzt den Betrieb nur dann weiter fort, wenn jeder Test erfolgreich gewesen ist.

Literaturhinweise:

Elektronik in der Sicherheitstechnik. H. Jürs, D. Reinert, Sicherheitstechnisches Informations- und Arbeitsblatt 330220, BIA-Handbuch, Erich-Schmidt Verlag, Bielefeld 1993.

Dependability of Critical Computer Systems 1. F. J. Redmill, Elsevier Applied Science, 1988, ISBN 1-85166-203-0.

A.2.7 Analogsignal-Überwachung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.3 und A.13 der IEC 61508-2 aufgeführt.

Ziel: Verbesserung des Vertrauens in gemessene Signale.

Beschreibung: Wenn eine Wahlmöglichkeit besteht, werden Analogsignale binären Ein-/Aus-Zuständen vorgezogen. Zum Beispiel werden energielose oder sichere Zustände durch analoge Signalpegel dargestellt, normalerweise mit Toleranzüberwachung der Signalpegel. Dieses Verfahren liefert eine kontinuierliche Überwachung und einen höheren Vertrauensgrad in die Übertragungseinrichtung, indem die notwendige Häufigkeit von Selbsttests einer Messkette verringert wird. Externe Schnittstellen, zum Beispiel Impulsleitungen, erfordern ebenfalls eine Testung.

Literaturhinweis: UKOOA Guidelines for Instrument-Based Systems, UK Offshore Operators Association Limited, December 1995.

A.2.8 Unterlastung

ANMERKUNG Dieses Verfahren/Maßnahme ist in 7.4.2.13 der IEC 61508-2 aufgeführt.

Ziel: Erhöhung der Zuverlässigkeit von Hardware-Bauteilen.

Beschreibung: Hardware-Bauteile werden in Bereichen betrieben, die aufgrund des Entwurfs des Systems weit unterhalb der festgelegten Höchstgrenzen liegen. Unterlastung ist die Methode, um zu gewährleisten, dass Bauteile unter allen normalen Betriebsumständen weit unterhalb ihrer Belastungsgrenzen betrieben werden.

A.3 Verarbeitungseinheiten (CPUs)

Allgemeines Ziel: Erkennung von Ausfällen, die zu falschen Ergebnissen in Verarbeitungseinheiten führen.

A.3.1 Selbsttest durch Software: begrenzte Anzahl von Mustern (ein Kanal)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.4 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen in der Verarbeitungseinheit so früh wie möglich.

Beschreibung: Die Hardware ist unter Verwendung von Standardverfahren aufgebaut, die keine besonderen Sicherheitsanforderungen in Betracht ziehen. Die Ausfallerkennung ist vollständig durch zusätzliche Softwarefunktionen realisiert, die Selbsttests durchführen. Diese verwenden mindestens zwei komplementäre Datenmuster (zum Beispiel 55hex und AAhex).

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.3.2 Selbsttest durch Software: Walking Bit (ein Kanal)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.4 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen im physikalischen Speicher (zum Beispiel Register) und Befehlsdecoder der Verarbeitungseinheit so früh wie möglich.

Beschreibung: Die Ausfallerkennung wird vollständig durch zusätzliche Softwarefunktionen realisiert, die Selbsttests durchführen. Diese verwenden ein Datenmuster (zum Beispiel ein wanderndes Bitmuster), welches den physikalischen Speicher (Daten- und Adressregister) und den Befehlsdecoder testet. Der Diagnosedegrad beträgt jedoch nur 90 %.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.3.3 Selbsttest unterstützt durch Hardware (ein Kanal)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.4 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen in der Verarbeitungseinheit durch Verwendung besonderer Hardware, die die Geschwindigkeit und den Umfang der Fehlererkennung erhöht, so früh wie möglich.

Beschreibung: Zusätzliche besondere Hardwaremittel unterstützen Selbsttestfunktionen, um Ausfälle zu erkennen. Dies könnte zum Beispiel eine Hardwareeinheit sein, die zyklisch die Ausgabe eines bestimmten Bitmusters gemäß dem Watchdog-Prinzip überwacht.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.3.4 Codierte Verarbeitung (ein Kanal)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.4 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen in der Verarbeitungseinheit so früh wie möglich.

Beschreibung: Verarbeitungseinheiten können mit besonderen fehlererkennenden oder fehlerkorrigierenden Schaltkreisverfahren entworfen werden. Bisher wurden diese Verfahren nur in relativ einfachen Schaltkreisen angewendet und sind nicht weit verbreitet, jedoch sollten zukünftige Entwicklungen nicht ausgeschlossen werden.

Literaturhinweise:

The Coded Microprocessor Certification. P. Ozello, Proc. SAFECOMP '92, 185-190, 1992.

Le Processeur Codé: un nouveau concept appliqué à la sécurité des systèmes de transports. Gabriel, Martin, Wartski, Revue Générale des chemins de fer, No. 6, June 1990.

Vital Coded Microprocessor Principles and Application for Various Transit Systems. P. Forin, IFAC Control Computers Communications in Transportation, 79-84, 1989.

A.3.5 Gegenseitiger Vergleich durch Software

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.4 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen in der Verarbeitungseinheit durch dynamischen Softwarevergleich so früh wie möglich.

Beschreibung: Zwei Verarbeitungseinheiten tauschen kreuzweise Daten (einschließlich Ergebnissen, Zwischenergebnissen und Testdaten) aus. Ein Vergleich der Daten wird durch Verwendung von Software in jeder Einheit durchgeführt und erkannte Unterschiede führen zu einer Ausfallmeldung.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.4 Unveränderliche Speicherbereiche

Allgemeines Ziel: Die Erkennung von Veränderungen der Informationen im invarianten Speicher.

A.4.1 Wortsicherungsverfahren mit Mehr-Bit-Redundanz (zum Beispiel ROM-Überwachung mit einem modifizierten Hammingcode)

ANMERKUNG Siehe auch A.5.6 und C.3.2. Dieses Verfahren/Maßnahme ist in Tabelle A.5 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von allen Einbitfehlern, allen Zweibitfehlern, einigen Dreibitfehlern und einigen Fehlern, bei denen alle Bits eines 16-Bit-Wortes verfälscht werden.

Beschreibung: Jedes Speicherwort wird durch mehrere redundante Bits erweitert, um einen modifizierten Hammingcode mit einer Hammingdistanz von mindestens 4 zu erzeugen. Jedes Mal, wenn ein Wort gelesen wird, kann eine Testung der redundanten Bits bestimmen, ob eine Verfälschung stattgefunden hat oder nicht. Wenn ein Unterschied festgestellt wird, wird eine Ausfallmeldung erzeugt. Das Verfahren kann auch zur Erkennung von Adressierungsfehlern verwendet werden, indem die redundanten Bits mit Hilfe der Verknüpfung des Datenwortes mit dessen Adresse berechnet werden.

Literaturhinweise:

Prüfbare und korrigierbare Codes. W. W. Peterson, München, Oldenburg, 1967.

Error detecting and error correcting codes. R. W. Hamming, The Bell System Technical Journal 29 (2), 147-160, 1950.

A.4.2 Modifizierte Prüfsumme

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.5 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller ungeradzahigen Bitfehler, d. h. ungefähr 50 % aller möglichen Bitfehler.

Beschreibung: Eine Prüfsumme wird durch einen geeigneten Algorithmus erzeugt, der alle Worte in einem Speicherblock verwendet. Die Prüfsumme kann als zusätzliches Wort im ROM gespeichert werden, oder ein zusätzliches Wort kann in einem Speicherblock hinzugefügt werden, um zu gewährleisten, dass der Prüfsummenalgorithmus einen vorbestimmten Wert erzeugt. In einem späteren Speichertest wird unter Verwendung des gleichen Algorithmus wieder eine Prüfsumme erzeugt. Das Ergebnis wird mit dem gespeicherten oder definierten Wert verglichen. Wenn ein Unterschied festgestellt wird, wird eine Ausfallmeldung erzeugt.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.4.3 Signatur mit einfacher Wortbreite (8 Bit)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.5 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller Einbitfehler und aller Mehrbitfehler innerhalb eines Wortes sowie ungefähr 99,6 % aller möglichen Bitfehler.

Beschreibung: Der Inhalt eines Speicherblocks wird unter Verwendung eines CRC-Algorithmus (en: cyclic redundancy check) zu einem Speicherwort komprimiert (entweder durch Verwendung von Hardware oder Software). Ein typischer CRC-Algorithmus behandelt den gesamten Inhalt eines Blocks als byte- oder bitseriellen Datenstrom, auf den unter Verwendung eines Generatorpolynoms eine laufende Polynomdivision durchgeführt wird. Der Rest der Division stellt den komprimierten Speicherinhalt dar – er ist die „Signatur“ des Speichers – und wird gespeichert. Die Signatur wird in späteren Tests nochmalig berechnet und mit der bereits gespeicherten verglichen. Im Falle eines Unterschiedes wird eine Ausfallmeldung erzeugt.

Literaturhinweise:

Berechnung von Fehlererkennungswahrscheinlichkeiten bei Signaturregistern. D. Leisengang, Elektronische Rechenanlagen 24, H. 2, S. 55-61, 1982.

Calculating an error checking character in software. S. Vasa, Computer Design, 5, 1976.

A.4.4 Signatur mit doppelter Wortbreite (16 Bit)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.5 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller Einbitfehler und aller Mehrbitfehler innerhalb eines Wortes sowie ungefähr 99,998 % aller möglichen Bitfehler.

Beschreibung: Dieses Verfahren berechnet eine Signatur unter Verwendung eines CRC-Algorithmus (en: cyclic redundancy check), jedoch umfasst das Ergebnis mindestens zwei Worte. Die erweiterte Signatur wird gespeichert, neu berechnet und verglichen, wie bei der Signatur mit einfacher Wortbreite. Im Falle eines Unterschiedes zwischen dem gespeicherten und dem neu berechneten Wert wird eine Ausfallmeldung erzeugt.

Literaturhinweise:

Signaturanalyse in der Datenverarbeitung. D. Leisengang, M. Wagner, Elektronik 32, H. 21, S. 67-72, 1983.

Signaturregister für selbsttestende ICs. B. Könnemann, J. Mucha, G. Zwiehoff, Größtintegration/NTG-Fachtagung Baden-Baden, S. 109 - 112, April 1977.

A.4.5 Blockwiederholung (zum Beispiel doppeltes ROM mit Hardware- oder Softwarevergleich)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.5 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller Bitfehler.

Beschreibung: Der Adressraum wird in zwei Speichern hinterlegt. Der erste Speicher wird wie üblich betrieben. Der zweite Speicher beinhaltet die gleiche Information und wird parallel zum ersten angesprochen. Die Ausgaben werden verglichen, und wenn ein Unterschied erkannt wird, wird eine Ausfallmeldung erzeugt. Um bestimmte Arten der Abweichungen der Bits zu erkennen, müssen die Daten in einem der beiden Speicher invers abgelegt und beim Lesen erneut invertiert werden.

Literaturhinweise:

Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

Computers can now perform vital safety functions safely. Otto Berg von Linde, Railway Gazette International, Vol. 135, No. 11, 1979.

A.5 Veränderliche Speicherbereiche

Allgemeines Ziel: Erkennung von Ausfällen während der Adressierung, des Schreibens, des Speicherns und des Lesens.

ANMERKUNG Soft-Errors werden in Tabelle A.1 der IEC 61508-2 als Fehler verzeichnet, die während des Betriebs aufzudecken sind oder bei der Herleitung des Anteils sicherer Ausfälle zu analysieren sind. Ursachen von Soft-Errors sind: (1) Alphateilchen vom radioaktiven Zerfall, (2) Neutronen, (3) externe elektromagnetische Störungen, (4) internes Übersprechen. Externe elektromagnetische Störungen werden durch andere Anforderungen dieser Internationalen Norm abgedeckt.

Die Auswirkungen von Alphateilchen und Neutronen sollte durch Maßnahmen zur Sicherheitsintegrität zur Laufzeit beherrscht werden. Für Hard-Errors wirksame Maßnahmen zur Sicherheitsintegrität müssen nicht für Soft-Errors wirksam sein, z.B. RAM-Tests wie Walkpath, Galpat usw. sind nicht wirksam, wohingegen überwachende Verfahren wie Parity und ECC mit dem wiederholenden Lesen der Speicherzellen wirksam sind.

Ein Soft-Error kommt vor, wenn ein Strahlungsereignis eine ausreichende Störung der Ladung verursacht, um den Datenzustand einer niedrig erregten Halbleiter-Speicherzelle, eines Registers, Latches oder Flip-Flops zu invertieren oder zu kippen. Der Fehler wird "Soft" genannt, weil der Schaltkreis selbst durch die Strahlung nicht dauerhaft beschädigt wird. Soft-Errors werden in Single-Bit-Upsets (SBU), Single-Event-Upsets (SEU) und Multi-Bit-Upsets (MBU) klassifiziert.

Wenn der gestörte Schaltkreis ein speicherndes Element wie eine Speicherzelle oder ein Flip-Flop ist, wird der Zustand bis zum nächsten (beabsichtigten) Schreibzugriff gespeichert. Die neuen Daten werden korrekt gespeichert. In einem kombinatorischen Schaltkreis entspricht die Wirkung eher eine Störung, weil es einen kontinuierlichen Energiefluss von dem Bauteil gibt, der diesen Knoten treibt. Die Wirkung auf Verbindungs- und Kommunikationsleitungen kann auch eine Störung sein. Jedoch wird wegen der größeren Kapazität die Wirkung durch Alphateilchen und Neutronen als vernachlässigbar betrachtet.

Soft-Errors können für veränderliche Speicher jeder Art, d. h. für DRAM, SRAM, Register-Bänke in Mikroprozessoren, Caches, Pipelines, Konfigurationsregister von Einheiten wie ADC, DMA, MMU, Interrupt-Controller, komplexe Timer, relevant sein. Die Empfindlichkeit gegen Alphateilchen und Neutronen ist abhängig von der Kernspannung und der geometrischen Struktur. Kleinere geometrische Strukturen bei einer Kernspannung von 2,5 V und besonders unterhalb 1,8 V würden mehr Aufwand bei der Beurteilung und wirksamere Schutzmaßnahmen erfordern.

Die Soft-Error-Rate für (eingebettete) Speicher wird in einem Bereich von 700 Fit/MBit bis 1200 Fit/MBit ausgewiesen (siehe a) und i) unten). Dies ist ein Bezugswert zum Vergleich mit Daten, die aus dem Halbleiterproduktionsprozess kommen, mit dem das Bauteil realisiert wird. Bis vor kurzem wurden SBU als vorherrschend angesehen, aber die neueste Prognose (siehe a) unten) berichtet von einem wachsenden Prozentsatz der MBU an der Gesamtrate der Soft-Errors (en: soft-error rate, SER) für Technologien von geringer als 65 nm.

Die folgende Literatur und Quellen liefern Einzelheiten über Soft-Errors:

- a) Altitude SEE Test European Platform (ASTEP) and First Results in CMOS 130 nm SRAM. J-L. Autran, P. Roche, C. Sudre et al. Nuclear Science, IEEE Transactions on Volume 54, Issue 4, Aug. 2007 Page(s):1002 - 1009,
- b) Radiation-Induced Soft Errors in Advanced Semiconductor Technologies, Robert C. Baumann, Fellow, IEEE, IEEE TRANSACTIONS ON DEVICE AND MATERIALS RELIABILITY, VOL. 5, NO. 3, SEPTEMBER 2005,
- c) Soft errors' impact on system reliability, Ritesh Mastipuram and Edwin C Wee, Cypress Semiconductor, 2004,
- d) Trends And Challenges In VLSI Circuit Reliability, C. Costantinescu, Intel, 2003, IEEE Computer Society,
- e) Basic mechanisms and modeling of single-event upset in digital microelectronics, P. E. Dodd and L. W. Massengill, IEEE Trans. Nucl. Sci., vol. 50, no. 3, pp. 583–602, Jun. 2003,
- f) Destructive single-event effects in semiconductor devices and ICs, F. W. Sexton, IEEE Trans. Nucl. Sci., vol. 50, no. 3, pp. 603–621, Jun. 2003,
- g) Coming Challenges in Microarchitecture and Architecture, Ronen, Mendelson, Proceedings of the IEEE, Volume 89, Issue 3, Mar 2001 Page(s):325 – 340,
- h) Scaling and Technology Issues for Soft Error Rates, A Johnston, 4th Annual Research Conference on Reliability Stanford University, October 2000,
- i) International Technology Roadmap for Semiconductors (ITRS), several papers.

A.5.1 RAM-Test „Checkerboard“ oder „March“

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Vorwiegend zur Erkennung statischer Bitfehler.

Beschreibung: Ein schachbrettartiges Muster von Nullen und Einsen wird in die Zellen eines bitorientierten Speichers geschrieben. Die Zellen werden dann paarweise überprüft, um zu gewährleisten, dass die Inhalte gleich und korrekt sind. Die Adresse der ersten Zelle eines solchen Paares ist veränderlich und die Adresse der zweiten Zelle des Paares wird durch bitweise Invertierung der ersten Adresse gebildet. Im ersten Durchlauf wird der Adressbereich des Speichers von der veränderlichen Adresse zu höheren Adressen durchlaufen und in einem zweiten Durchlauf zu niedrigeren Adressen. Beide Durchläufe werden dann mit invertierter Vorbelegung wiederholt. Im Falle eines Unterschiedes wird eine Ausfallmeldung erzeugt.

Bei einem RAM-Test „March“ werden die Zellen eines bitorientierten Speichers durch eine einheitliche Bitfolge vorbelegt. Im ersten Durchlauf werden die Zellen in aufsteigender Folge überprüft. Jede Zelle wird auf korrekten Inhalt getestet und ihr Inhalt invertiert. Der Hintergrund, der im ersten Durchlauf erzeugt wird, wird in einem zweiten Durchlauf in absteigender Folge und in der gleichen Art und Weise behandelt. Die ersten beiden Durchläufe werden mit einer invertierten Vorbelegung in einem dritten und vierten Durchlauf wiederholt. Im Falle eines Unterschiedes wird eine Ausfallmeldung erzeugt.

Literaturhinweise:

Halbleiterspeicher-Testfolgen. Th. John, E. Schaefer, Elektronikpraxis, H. 6, 18-26 und H. 7, 10-14, 1980.

Memory testing. P. Rosenfield, Electronics and Power, H. 1, P. 26-31, 1979.

Memory testing. W. G. Fee, LSI Testing (Tutorial at the COMPCON 77 in San Francisco), IEEE Computer Society, W. G. Fee (ed.), 81-88, 1978.

A.5.2 RAM-Test „Walkpath“

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Erkennung statischer und dynamischer Bitfehler und Übersprechen zwischen Speicherzellen.

Beschreibung: Der zu testende Speicherbereich wird mit einer einheitlichen Bitfolge vorbelegt. Die erste Zelle wird dann invertiert und der verbleibende Speicherbereich wird überprüft, um zu gewährleisten, dass der Hintergrund korrekt ist. Danach wird die erste Zelle erneut in ihren ursprünglichen Wert invertiert, und das gesamte Verfahren wird für die nächste Zelle wiederholt. Ein zweiter Durchlauf des „wandernden Bit-Modells“ wird mit einer inversen Hintergrundbelegung durchgeführt. Im Falle eines Unterschiedes wird eine Ausfallmeldung erzeugt.

Literaturhinweise:

Memory testing. W. G. Fee, LSI Testing (Tutorial at the COMPCON 77 in San Francisco), IEEE Computer Society, W. G. Fee (ed.), 81-88, 1978.

Techniques for testing the microprocessor family. W. Barraclough, A. Chiang, W. Sohl, Proceedings of the IEEE, 64 (6), 943-950, 1976.

A.5.3 RAM-Test „Galpat“ oder „transparenter Galpat“

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von statischen Bitfehlern und eines Großteils dynamischer Kopplungen.

Beschreibung: Im RAM-Test „Galpat“ wird der ausgewählte Speicherbereich zunächst einheitlich (d. h. alles Nullen oder alles Einsen) vorbelegt. Die erste zu testende Speicherzelle wird dann invertiert und alle verbleibenden Zellen überprüft, um zu gewährleisten, dass ihre Inhalte korrekt sind. Nach jedem Lesezugriff auf eine der verbleibenden Zellen wird auch die invertierte Zelle überprüft. Dieses Verfahren wird für jede Zelle in dem gewählten Speicherbereich wiederholt. Ein zweiter Durchlauf wird mit der gegensätzlichen Vorbelegung durchgeführt. Jeder Unterschied erzeugt eine Ausfallmeldung.

Der „transparente Galpat“-Test ist eine Variation des obigen Verfahrens. Statt einer Vorbelegung aller Zellen im ausgewählten Speicherbereich wird der bestehende Inhalt unverändert beibehalten, und es werden Signaturen verwendet, um den Inhalt der Zellenauswahl zu vergleichen. Die erste zu testende Zelle im ausgewählten Bereich wird ausgewählt und die Signatur S1 aller verbleibenden Zellen im Bereich wird berechnet und gespeichert. Die zu testende Zelle wird daraufhin invertiert und die Signatur S2 aller verbleibenden Zellen erneut berechnet. (Nach jedem Lesezugriff auf eine der verbleibenden Zellen wird die invertierte Zelle ebenfalls getestet) S2 wird mit S1 verglichen und jeder Unterschied erzeugt eine Ausfallmeldung. Die dem Test unterliegende Zelle wird erneut invertiert, um den ursprünglichen Inhalt wiederherzustellen, und die Signatur S3 aller verbleibenden Zellen wird neu berechnet und mit S1 verglichen. Jeder Unterschied erzeugt eine Ausfallmeldung. Alle Speicherzellen in dem ausgewählten Bereich werden in der gleichen Art und Weise getestet.

Literaturhinweise:

Periodischer Selbsttest einer mikroprozessorgesteuerten Sicherheitsschaltung. U. Stinnesbek, Diplomarbeit am Institut für theoretische Elektrotechnik der RWTH Aachen 1980.

Entwurf von Selbsttestprogrammen für Mikrocomputer. E. Maehle, Microcomputing. Berichte der Tagung III/79 des German Chapter of the ACM, W. Remmele, H. Schecher, (ed.), Stuttgart, Teubner, 204-216, 1979.

A.5.4 RAM-Test „Abraham“

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller Stuck-at-Fehler und Kopplungen zwischen Speicherzellen.

Beschreibung: Der Anteil erkannter Fehler übersteigt den beim RAM-Test „Galpat“. Die Anzahl der notwendigen Operationen, um den gesamten Speichertest durchzuführen, beträgt $30n$, wobei n die Anzahl der Speicherzellen ist. Der Test kann zur Anwendung während des Betriebszyklus transparent durchgeführt werden, indem der Speicher unterteilt und jeder Teil in verschiedenen Zeitsegmenten getestet wird.

Literaturhinweis: Efficient Algorithms for Testing Semiconductor Random-Access Memories. R. Nair, S. M. Thatte, J. A. Abraham, IEEE Trans. Comput. C-27 (6), 572-576, 1978.

A.5.5 Ein-Bit-Redundanz (zum Beispiel RAM-Überwachung mit einem Parity-Bit)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von 50 % aller möglichen Bitfehler im getesteten Speicherbereich.

Beschreibung: Jedes Speicherwort wird um ein Bit (das Paritätsbit) erweitert, welches jedes Wort zu einer geraden oder ungeraden Anzahl logischer Einsen vervollständigt. Die Parität des Datenworts wird bei jedem Lesezugriff getestet. Wenn die falsche Anzahl von Einsen gefunden wird, wird eine Ausfallmeldung erzeugt. Die Wahl von gerader oder ungerader Parität sollte im Hinblick darauf getroffen werden, ob das Nullwort (alles Nullen) oder das Einswort (alles Einsen) im Falle eines Ausfalles das ungünstigste ist. Dann ist dieses Wort ein ungültiger Code. Die Parität kann auch verwendet werden, um Adressierungsfehler zu erkennen, wenn die Parität durch die Verknüpfung des Datenwortes mit seiner Adresse berechnet wird.

Literaturhinweis: Integrierte Digitalbausteine. K. Reiß, H. Liedl, W. Spichall, Berlin, 1970.

A.5.6 RAM-Überwachung mit einem modifizierten Hammingcode oder Erkennung von Datenfehlern mit fehlererkennenden und -korrigierenden Codes (en: error-detection-correction codes, EDC)

ANMERKUNG Siehe auch A.4.1 und C.3.2. Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller ungeradzahligen Bitfehler, aller Zweibitfehler, einiger Dreibit- und einiger Mehrbitfehler.

Beschreibung: Jedes Speicherwort wird durch mehrere redundante Bits erweitert, um einen modifizierten Hammingcode mit einer Hammingdistanz von mindestens 4 zu erzeugen. Bei jedem Lesezugriff kann man durch Testung der redundanten Bits bestimmen, ob eine Verfälschung stattgefunden hat. Wenn ein Unterschied gefunden wird, wird eine Ausfallmeldung erzeugt. Das Verfahren kann auch zur Erkennung von Adressierungsfehlern verwendet werden, indem die redundanten Bits durch die Verknüpfung des Datenwortes mit seiner Adresse berechnet werden.

Literaturhinweise:

Prüfbare und korrigierbare Codes. W. W. Peterson, München, Oldenburg, 1967.

Error detecting and error correcting codes. R. W. Hamming, The Bell System Technical Journal, 29 (2), 147-160, 1950.

A.5.7 Doppeltes RAM mit Hardware- oder Softwarevergleich und Schreib-/Lesetest

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.6 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller Bitfehler.

Beschreibung: Der Adressraum wird in zwei Speichern hinterlegt. Der erste Speicher wird wie üblich betrieben. Der zweite Speicher beinhaltet die gleiche Information und wird parallel zum ersten angesprochen. Die Ausgaben werden verglichen, und wenn ein Unterschied erkannt wird, wird eine Ausfallmeldung erzeugt. Um bestimmte Arten der Abweichungen der Bits zu erkennen, müssen die Daten in einem der beiden Speicher invers abgelegt und beim Lesen erneut invertiert werden.

Literaturhinweise:

Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

Computers can now perform vital safety functions safely. Otto Berg von Linde, Railway Gazette International, Vol. 135, No. 11, 1979.

A.6 E/A-Einheiten und Schnittstellen (externe Kommunikation)

Allgemeines Ziel: Fehlererkennung in Eingabe- und Ausgabeeinheiten (digital, analog, seriell oder parallel) und Verhinderung des Sendens unzulässiger Ausgaben an den Prozess.

A.6.1 Testmuster

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.7, A.13 und A.14 der IEC 61508-2 aufgeführt.

Ziel: Erkennung statischer Ausfälle (Stuck-at-Fehler) und Übersprechen.

Beschreibung: Dies ist ein Datenfluss-unabhängiger, zyklischer Test von Ein- und Ausgabeeinheiten. Er verwendet ein definiertes Testmuster, um die beobachteten mit den zugehörigen erwarteten Werten zu ver-

gleichen. Die Testmusterinformation, der Testmusterempfang und die Testmusterbewertung müssen alle voneinander unabhängig sein. Die EUC sollte durch das Testmuster nicht unzulässig beeinflusst werden.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.6.2 Codesicherung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.7, A.15, A.15 und A.18 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von zufälligen Hardwareausfällen und systematischen Ausfällen im Eingabe- und Ausgabedatenfluss.

Beschreibung: Dieses Verfahren schützt die Eingabe- und Ausgabeinformation sowohl vor systematischen Ausfällen als auch vor zufälligen Hardwareausfällen. Die Codesicherung stellt eine Datenfluss-abhängige Ausfallerkennung der Eingabe- und Ausgabeeinheiten, basierend auf Informationsredundanz und/oder Zeitredundanz, bereit. Normalerweise werden redundante Informationen den Eingabe- und/oder Ausgabedaten überlagert. Dies stellt ein Mittel bereit, um den korrekten Betrieb der Eingabe- und Ausgabeschaltkreise zu überwachen. Viele Verfahren sind möglich, es kann zum Beispiel dem Ausgangssignal eines Sensors ein Trägerfrequenzsignal überlagert werden. Die Logikeinheit kann dann die Anwesenheit der Trägerfrequenz testen. Es können redundante Codebits einem Ausgabekanal hinzugefügt werden, um die Überwachung der Gültigkeit eines Signals zu ermöglichen, das zwischen Logikeinheit und Stellglied übertragen wird.

Literaturhinweis: Standard input/output tests and monitoring procedures – Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.6.3 Mehrkanalige parallele Ausgabe

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.7 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von zufälligen Hardwareausfällen (Stuck-at-Fehler), Ausfälle verursacht durch äußere Einflüsse, Timing-Fehler, Adressierungsfehler, Driftfehler und transiente Fehler.

Beschreibung: Dies ist eine Datenfluss-abhängige, mehrkanalige parallele Ausgabe mit unabhängigen Ausgaben für die Erkennung von zufälligen Hardwareausfällen. Die Ausfallerkennung wird durch externe Vergleiche durchgeführt. Im Falle eines Ausfalls wird die EUC direkt abgeschaltet. Diese Maßnahme ist nur wirksam, wenn sich der Datenfluss während des Diagnose-Testintervalls verändert.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.6.4 Überwachte Ausgaben

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.7 der IEC 61508-2 aufgeführt.

Ziel: Erkennung individueller Ausfälle, Ausfälle verursacht durch äußere Einflüsse, Timing-Fehler, Adressierungsfehler, Driftfehler (von analogen Signalen) und transiente Fehler.

Beschreibung: Dies ist ein Datenfluss-abhängiger Ausgabevergleich mit unabhängigen Eingaben, um Übereinstimmung mit einem definierten Toleranzbereich (Zeit, Wert) zu gewährleisten. Ein erkannter Ausfall kann nicht immer auf die defekte Ausgabe bezogen werden. Diese Maßnahme ist nur wirksam, wenn sich der Datenfluss während des Diagnose-Testintervalls verändert.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.6.5 Eingabevergleich/-entscheidung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.7 und A.13 der IEC 61508-2 aufgeführt.

Ziel: Erkennung individueller Ausfälle, Ausfälle verursacht durch äußere Einflüsse, Timing-Fehler, Adressierungsfehler, Driftfehler (von analogen Signalen) und transiente Fehler.

Beschreibung: Dies ist ein Datenfluss-abhängiger Vergleich unabhängiger Eingänge, um Übereinstimmung mit einem definierten Toleranzbereich (Zeit, Wert) zu gewährleisten. Es wird 1 aus 2, 2 aus 3 oder bessere Redundanz verwendet. Diese Maßnahme ist nur wirksam, wenn sich der Datenfluss während des Diagnose-Testintervalls verändert.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.7 Datenwege (interne Kommunikation)

Allgemeines Ziel: Erkennung von Ausfällen, die durch einen Defekt bei der Informationsübertragung verursacht werden.

A.7.1 Ein-Bit-Hardwareredundanz

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.8 der IEC 61508-2 aufgeführt.

Ziel: Erkennung aller ungeraden Bitfehler, d. h. 50 % aller möglichen Bitfehler in der Datenfolge.

Beschreibung: Der Bus wird um eine Leitung (Bit) erweitert, und diese zusätzliche Leitung (Bit) wird verwendet, um durch Prüfung der Parität Ausfälle zu erkennen.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.7.2 Mehr-Bit-Hardwareredundanz

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.8 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen während der Kommunikation über den Bus und in Verbindungen mit serieller Übertragung.

Beschreibung: Der Bus wird um zwei oder mehrere Leitungen (Bits) erweitert, und diese zusätzlichen Leitungen (Bits) werden verwendet, um unter Verwendung des Hammingcode-Verfahrens Ausfälle zu erkennen.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.7.3 Vollständige Hardwareredundanz

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.8 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen während der Kommunikation durch Vergleich der Signale auf zwei Bussen.

Beschreibung: Der Bus wird verdoppelt und die zusätzlichen Leitungen (Bits) werden zur Erkennung von Ausfällen verwendet.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.7.4 Inspektion durch Verwendung von Testmustern

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.8 der IEC 61508-2 aufgeführt.

Ziel: Erkennung statischer Ausfälle (Stuck-at-Fehler) und Übersprechen.

Beschreibung: Dies ist ein Datenfluss-unabhängiger, zyklischer Test der Datenwege. Er verwendet ein definiertes Testmuster, um die beobachteten mit den zugehörigen erwarteten Werten zu vergleichen.

Die Testmusterinformation, der Testmusterempfang und die Testmusterbewertung müssen alle voneinander unabhängig sein. Die EUC sollte nicht in unzulässiger Weise durch das Testmuster beeinflusst werden.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.7.5 Übertragungsredundanz

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.8 der IEC 61508-2 aufgeführt.

Ziel: Erkennung transienter Ausfälle in der Buskommunikation.

Beschreibung: Die Information wird mehrmalig in Folge übertragen. Die Wiederholung wirkt nur gegen transiente Ausfälle.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.7.6 Informationsredundanz

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.8 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Ausfällen in der Buskommunikation.

Beschreibung: Daten werden in Blöcken zusammen mit einer für jeden Block berechneten Prüfsumme übertragen. Der Empfänger berechnet erneut die Prüfsumme der erhaltenen Daten und vergleicht das Ergebnis mit der empfangenen Prüfsumme.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.8 Spannungsversorgung

Allgemeines Ziel: Erkennung oder Tolerierung von Ausfällen, verursacht durch Defekte in der Spannungsversorgung.

A.8.1 Überspannungsschutz mit Sicherheitsabschaltung

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.9 der IEC 61508-2 aufgeführt.

Ziel: Schutz des sicherheitsbezogenen Systems vor Überspannungen.

Beschreibung: Eine Überspannung wird früh genug erkannt, damit alle Ausgänge durch eine Abschaltoutine in einen sicheren Zustand geschaltet werden können oder zu einer zweiten Versorgungseinheit umgeschaltet werden kann.

Literaturhinweis: Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

A.8.2 Spannungsüberwachung (sekundärseitig)

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.9 der IEC 61508-2 aufgeführt.

Ziel: Überwachung der sekundärseitigen Spannungen und Einleitung eines sicheren Zustands, wenn die Spannung sich nicht im festgelegten Bereich befindet.

Beschreibung: Die sekundärseitige Spannung wird überwacht, und wenn sie sich nicht in ihrem festgelegten Bereich befindet, wird eine Abschaltung eingeleitet oder zu einer zweiten Versorgungseinheit umgeschaltet.

A.8.3 Energieabschaltung mit Sicherheitsabschaltung

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.9 der IEC 61508-2 aufgeführt.

Ziel: Abschaltung der Energie mit Speicherung aller sicherheitskritischen Informationen.

Beschreibung: Eine Über- oder Unterspannung wird früh genug erkannt, damit (wenn erforderlich) der interne Status in einem nichtflüchtigen Speicher gesichert werden kann und damit alle Ausgänge durch die Abschalt routine in einen sicheren Zustand gesetzt werden können oder damit zu einer zweiten Versorgungseinheit umgeschaltet werden kann.

A.9 Zeitliche und logische Programmlaufüberwachung

ANMERKUNG Diese Gruppe von Verfahren und Maßnahmen ist in den Tabellen A.15, A.16 und A.18 der IEC 61508-2 aufgeführt.

Allgemeines Ziel: Erkennung eines defekten Programmablaufes. Ein defekter Programmablauf liegt vor, wenn einzelne Elemente eines Programms (zum Beispiel Softwaremodule, Unterprogramme oder Befehle) in falscher Reihenfolge oder falschen Zeitabständen verarbeitet werden oder wenn der Prozessortakt fehlerhaft ist.

A.9.1 Watchdog mit separater Zeitbasis ohne Zeitfenster

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.10 und A.11 der IEC 61508-2 aufgeführt.

Ziel: Überwachung des Verhaltens und der Plausibilität des Programmablaufes.

Beschreibung: Externe Zeitglieder mit einer separaten Zeitbasis (zum Beispiel Watchdog-Timer) werden periodisch getriggert, um das Verhalten und die Plausibilität des Rechners bezüglich des Programmablaufes zu überwachen. Es ist wichtig, dass die Triggerpunkte korrekt im Programm platziert werden. Der Watchdog wird nicht in einem festen Zeitraster getriggert, aber ein maximales Intervall wird festgelegt.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.9.2 Watchdog mit separater Zeitbasis und Zeitfenster

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.10 und A.11 der IEC 61508-2 aufgeführt.

Ziel: Überwachung des Verhaltens und der Plausibilität des Programmablaufes.

Beschreibung: Externe Zeitglieder mit einer separaten Zeitbasis (zum Beispiel Watchdog-Timer) werden periodisch getriggert, um das Verhalten und die Plausibilität des Rechners bezüglich des Programmablaufes

zu überwachen. Es ist wichtig, dass die Triggerpunkte korrekt im Programm platziert werden. Für den Watchdog-Timer wird eine untere und obere Grenze festgelegt. Wenn der Programmablauf einer längere oder kürzere Zeit als erwartet dauert, wird eine Notaktion ausgeführt.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.9.3 Logische Überwachung des Programmablaufs

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.10 und A.11 der IEC 61508-2 aufgeführt.

Ziel: Überwachung des korrekten Ablaufes von einzelnen Programmabschnitten.

Beschreibung: Der korrekte Ablauf der einzelnen Programmabschnitte wird durch Software (Zählverfahren, Schlüsselverfahren) oder durch Anwendung externer Überwachungseinrichtungen überwacht. Es ist wichtig, dass die Kontrollpunkte korrekt im Programm platziert werden.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.9.4 Kombination von zeitlicher und logischer Überwachung des Programmablaufs

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.10 und A.11 der IEC 61508-2 aufgeführt.

Ziel: Überwachung des Verhaltens und des korrekten Ablaufes von einzelnen Programmabschnitten.

Beschreibung: Eine zeitliche Einrichtung (zum Beispiel Watchdog-Timer), die den Programmablauf überwacht, wird nur getriggert, wenn der Ablauf der einzelnen Programmabschnitte korrekt ausgeführt wurde.

Literaturhinweis: Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

A.9.5 Zeitliche Überwachung mit Test während des Betriebs

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.10 und A.11 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Fehlern in der zeitlichen Überwachung.

Beschreibung: Die zeitliche Überwachung wird nach dem Einschalten getestet. Ein Anlaufen ist nur möglich, wenn die zeitliche Überwachung korrekt funktioniert. Zum Beispiel könnte ein Wärmesensor durch einen erwärmten Widerstand beim Einschalten getestet werden.

A.10 Lüftung und Beheizung

ANMERKUNG Diese Gruppe von Verfahren und Maßnahmen ist in den Tabellen A.16 und A.18 der IEC 61508-2 aufgeführt.

Allgemeines Ziel: Beherrschung von Ausfällen in der Lüftung oder Heizung und/oder deren Überwachung, sofern dies sicherheitsrelevant ist.

A.10.1 Temperatursensor

Ziel: Erkennung von Über- oder Untertemperatur, bevor das System außerhalb der Spezifikation betrieben wird.

Beschreibung: Ein Temperatursensor überwacht die Temperatur an den kritischsten Stellen des sicherheitsbezogenen E/E/PE-Systems. Bevor die Temperatur den spezifizierten Bereich verlässt, wird eine Notaktion ausgeführt.

A.10.2 Lüfterkontrolle

Ziel: Erkennung des inkorrekten Betriebs eines Lüfters.

Beschreibung: Die Lüfter werden auf korrekten Betrieb überwacht. Wenn ein Lüfter nicht richtig arbeitet, wird eine Tätigkeit zur Instandhaltung (oder letztlich eine Notaktion) ausgeführt.

A.10.3 Auslösung der Sicherheitsabschaltung über eine thermische Sicherung

Ziel: Abschaltung des sicherheitsbezogenen Systems, bevor das System außerhalb seiner Temperatur-Spezifikation arbeitet.

Beschreibung: Eine Temperatursicherung wird verwendet, um das sicherheitsbezogene System abzuschalten. Für ein PES wird die Abschaltung durch eine Abschaltroutine eingeleitet, welche alle für die Notaktion erforderlichen Informationen speichert.

A.10.4 Gestaffelte Meldung von Thermosensoren und bedingter Alarm

Ziel: Anzeige, dass das sicherheitsbezogene System außerhalb seiner Temperatur-Spezifikation arbeitet.

Beschreibung: Die Temperatur wird überwacht und ein Alarm wird ausgelöst, wenn die Temperatur außerhalb des festgelegten Bereichs ist.

A.10.5 Zuschaltung von Fremdkühlung und Statusanzeige

Ziel: Verhinderung von Überhitzung durch Fremdkühlung.

Beschreibung: Die Temperatur wird überwacht und Zwangsluftkühlung eingeleitet, wenn die Temperatur höher als eine festgelegte Grenze wird. Der Anwender wird über den Status informiert.

A.11 Kommunikation und Massenspeicher

Allgemeines Ziel: Beherrschung von Ausfällen während der Kommunikation mit externen Quellen und Massenspeichern.

A.11.1 Trennung elektrischer Energieleitungen von Informationsleitungen

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.16 der IEC 61508-2 aufgeführt.

Ziel: Verringerung der Beeinflussung von Informationsleitungen durch hohe Ströme.

Beschreibung: Elektrische Versorgungsleitungen werden von den Leitungen getrennt, die die Information führen. Das elektrische Feld, das Spannungsspitzen in die Informationsleitungen induzieren könnte, nimmt mit dem Abstand ab.

A.11.2 Räumliche Trennung mehrfacher Leitungen

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.16 der IEC 61508-2 aufgeführt.

Ziel: Verringerung von Übersprechen auf Mehrfachleitungen.

Beschreibung: Leitungen, die redundante Signale übertragen, werden voneinander getrennt. Das elektrische Feld, das Spannungsspitzen in die Mehrfachleitungen induzieren könnte, nimmt mit dem Abstand ab. Diese Maßnahme reduziert auch Ausfälle infolge gemeinsamer Ursache.

A.11.3 Erhöhung der Störfestigkeit

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.16 und A.18 der IEC 61508-2 aufgeführt.

Ziel: Verringerung der elektromagnetischen Störungen auf das sicherheitsbezogene System.

Beschreibung: Entwurfsverfahren wie Schirmung und Filterung werden verwendet, um die Störfestigkeit des sicherheitsbezogenen Systems gegen elektromagnetische Störungen zu erhöhen, die eingestrahlt, über Versorgungs- oder Signalleitungen geführt werden oder aus elektrostatischen Entladungen resultieren können.

ANMERKUNG Siehe [16] und [17] für Anforderungen zur Störfestigkeit von sicherheitsbezogenen Systemen und von Betriebsmitteln, die vorgesehen sind, sicherheitsbezogene Funktionen (funktionale Sicherheit) in industriellen Anwendungen auszuführen.

Literaturhinweise:

IEC/TR 61000-5-2:1997, *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 2: Earthing and cabling*.

Principles and Techniques of Electromagnetic Compatibility. C. Christopoulos, CRC Press, 1995.

Noise Reduction Techniques in Electronic Systems. H. W. Ott, John Wiley Interscience, 2nd Edition, 1988.

Gestaltung von Maschinensteuerungen unter Berücksichtigung der elektromagnetischen Verträglichkeit. F. Börner, Sicherheitstechnisches Informations- und Arbeitsblatt 330260, BIA-Handbuch. 20. Lfg. V/93, Erich Schmidt Verlag, Bielefeld.

EMC for Product Designers. Tim Williams, Newnes, 1992, ISBN 0-7506-1264-9.

Grounding and Shielding Techniques in Instrumentation. John Wiley & Sons, New York, 1986.

A.11.4 Antivalente Signalübertragung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.7 und A.16 der IEC 61508-2 aufgeführt.

Ziel: Erkennung gleicher induzierter Spannungen in mehrfachen Signalübertragungsleitungen.

Beschreibung: Alle Informationen werden redundant mit antivalenten Signalen (zum Beispiel logisch 1 und 0) übertragen. Ausfälle infolge gemeinsamer Ursache (z. B. durch elektromagnetische Störstrahlung) können durch einen Antivalenzvergleich erkannt werden.

Literaturhinweis: Elektronik in der Sicherheitstechnik. H. Jürs, D. Reinert, Sicherheitstechnisches Informations- und Arbeitsblatt 330220, BIA-Handbuch, 20. Lfg. V/93, Erich Schmidt Verlag, Bielefeld.

A.12 Sensoren

Allgemeines Ziel: Ausfallerkennung in den Sensoren des sicherheitsbezogenen Systems.

A.12.1 Referenzsensor

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.13 der IEC 61508-2 aufgeführt.

Ziel: Erkennung des inkorrekten Betriebs eines Sensors.

Beschreibung: Ein unabhängiger Referenzsensor wird verwendet, um den Betrieb eines Prozesssensors zu überwachen. Alle Eingabesignale werden in geeigneten Zeitabständen durch den Referenzsensor getestet, um Ausfälle des Prozesssensors zu erkennen.

Literaturhinweis: Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

A.12.2 Zwangsöffnender Schalter

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.13 der IEC 61508-2 aufgeführt.

Ziel: Öffnen eines Kontaktes durch eine direkte mechanische Verbindung zwischen Stößel und Kontakt.

Beschreibung: Ein zwangsgeführter Schalter öffnet seinen Öffnerkontakt durch eine direkte mechanische Verbindung zwischen Stößel und Kontakt. Dies gewährleistet, dass jedes Mal, wenn der Stößel in der betätigten Stellung ist, der Schalterkontakt offen sein muss.

Literaturhinweis: Verriegelung beweglicher Schutzeinrichtungen. F. Kreutzkamp, K. Becker, Sicherheitstechnisches Informations- und Arbeitsblatt 330210, BIA-Handbuch, 1. Lfg. IX/85, Erich Schmidt Verlag, Bielefeld.

A.13 Stellglieder (Aktoren)

Allgemeines Ziel: Beherrschung von Ausfällen in den Stellgliedern eines sicherheitsbezogenen Systems.

A.13.1 Überwachung

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.14 der IEC 61508-2 aufgeführt.

Ziel: Erkennung des inkorrekten Betriebs eines Aktors.

Beschreibung: Der Betrieb des Aktors wird überwacht (zum Beispiel durch die zwangsöffnenden Kontakte eines Relais, siehe Überwachung von Relaiskontakten in A.1.2). Die durch diese Überwachung eingeführte Redundanz kann zum Auslösen einer Notaktion verwendet werden.

Literaturhinweise:

Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

Zusammenstellung und Bewertung elektromechanischer Sicherheitsschaltungen für Verriegelungseinrichtungen. F. Kreutzkamp, W. Hertel, Sicherheitstechnisches Informations- und Arbeitsblatt 330212, BIA-Handbuch, 17. Lfg. X/91, Erich Schmidt Verlag, Bielefeld.

A.13.2 Kreuzweise Überwachung mehrfacher Aktoren

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.14 der IEC 61508-2 aufgeführt.

Ziel: Erkennung von Fehlern in Aktoren durch Vergleich der Ergebnisse.

Beschreibung: Jeder der mehrfach vorhandenen Aktoren wird durch einen unterschiedlichen Hardwarekanal überwacht. Im Falle eines Widerspruchs wird eine Notaktion eingeleitet.

A.14 Maßnahmen gegen die Einwirkung der physikalischen Umgebung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.16 und A.18 der IEC 61508-2 aufgeführt.

Ziel: Verhindern, dass die Einflüsse der physikalischen Umgebung (Wasser, Staub, korrodierende Substanzen) Ausfälle verursachen können.

Beschreibung: Das Gehäuse des Gerätes wird so entworfen, dass es der erwarteten Umgebung standhält.

Literaturhinweis: IEC 60529:2001, *Degrees of protection provided by enclosures (IP code)*.

Anhang B (informativ)

Überblick über Verfahren und Maßnahmen für sicherheitsbezogene E/E/PE-Systeme: Vermeidung von systematischen Ausfällen (siehe IEC 61508-2 und IEC 61508-3)

ANMERKUNG Viele Verfahren in diesem Anhang sind auf Software anwendbar, werden jedoch im Anhang C nicht noch einmal aufgeführt.

B.1 Allgemeine Maßnahmen und Verfahren

B.1.1 Projektmanagement

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.1 bis B.6 der IEC 61508-2 aufgeführt.

Ziel: Vermeidung von Ausfällen durch Annahme eines organisatorischen Modells sowie von Regeln und Maßnahmen für die Entwicklung und den Test sicherheitsbezogener Systeme.

Beschreibung: Die wichtigsten und besten Maßnahmen sind

- die Erstellung eines Organisationsmodells, speziell für die Qualitätssicherung (siehe Normen wie die Serie ISO 9000-1 bis ISO 9004-1 oder ähnliches), welches in einem Qualitätssicherungshandbuch niedergelegt ist, und
- die Festlegung von Regeln und Maßnahmen für die Erstellung und Validierung von sicherheitsbezogenen Systemen in Projektplanung und projektspezifischen Richtlinien.

Mehrere wichtige Basisprinzipien werden im Folgenden genannt:

- Definition einer Entwurfsorganisation:
 - Aufgaben und Verantwortlichkeiten der organisatorischen Einheiten,
 - Befugnisse der Abteilung für die Qualitätssicherung,
 - Unabhängigkeit der Qualitätssicherung (interne Inspektion) von der Entwicklung;
- Definition des Ablaufplans (Phasenmodelle):
 - Bestimmung aller Tätigkeiten, die während der Durchführung des Projekts sachdienlich sind, einschließlich der internen Inspektionen und deren Zeitplanung,
 - Projektaktualisierung;
- Definition eines feststehenden Ablaufs einer internen Inspektion:
 - Planung, Ausführung und Überprüfung der Inspektion (Inspektionstheorie),
 - Freigabemechanismus für Teilprodukte,
 - Sicherung von Wiederholungsinspektionen;
- Konfigurationsmanagement:
 - Verwaltung und Kontrolle der Versionen,
 - Erkennung der Auswirkungen von Modifikationen,
 - Inspektion der Beibehaltung der Eigenschaften nach Modifikationen;
- Einführung einer quantitativen Beurteilung von Qualitätssicherungsmaßnahmen:
 - Festlegung der Anforderungen,
 - Ausfallstatistiken;
- Einführung von rechnerunterstützten universellen Methoden, Werkzeugen und Personalschulung.

Literaturhinweise:

Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

Dependability of Critical Computer Systems 1. F. J. Redmill, Elsevier Applied Science, 1988, ISBN 1-85166-203-0.

IEEE: Software Engineering Standards. IEEE/Wiley-Interscience, New York, 1987.

B.1.2 Dokumentation

ANMERKUNG 1 Dieses Verfahren/Maßnahme ist in den Tabellen B.1 bis B.6 der IEC 61508-2 aufgeführt.

ANMERKUNG 2 Siehe auch Abschnitt 5 und Anhang A der IEC 61508-1.

Ziel: Vermeidung von Ausfällen und Erleichterung der Beurteilung der Systemsicherheit, indem jeder Schritt während der Entwicklung dokumentiert wird.

Beschreibung: Die betriebliche Fähigkeit und Sicherheit sowie die von allen in die Entwicklung einbezogenen Parteien aufgewandte Sorgfalt muss während der Beurteilung nachgewiesen werden. Besondere Aufmerksamkeit wird auf die Dokumentation gelegt, um jederzeit die während der Entwicklung aufgewandte Sicherheit und die Sicherheitsnachweise darlegen zu können.

Wichtige allgemeine Maßnahmen sind die Einführung von Richtlinien und Rechnerhilfsmitteln, d. h.

- Richtlinien, die
 - einen Zusammenstellungsplan festlegen,
 - nach Checklisten für den Inhalt fragen und
 - die Form des Dokuments bestimmen;
- Verwaltung der Dokumentation mit Hilfe von rechnerunterstützten und -organisierten Projektbibliotheken.

Individuelle Maßnahmen sind:

- Unterteilung der Dokumentation
 - in die Anforderungen,
 - des Systems (Anwenderdokumentation) und
 - der Entwicklung (einschließlich interner Inspektion);
- Zusammenstellung der Entwicklungsdokumentation gemäß dem Sicherheitslebenszyklus;
- Definition standardisierter Dokumentationsmodule, aus denen die Dokumente zusammengestellt werden können;
- eindeutige Identifikation der Bestandteile der Dokumentation;
- formalisierte Aktualisierung der Revisionen;
- Auswahl eindeutiger und verständlicher Beschreibungsmittel:
 - formale Notation der Festlegungen;
 - natürliche Sprache für Einführungen, Rechtfertigungen und Darstellungen der Absichten;
 - graphische Darstellungen der Beispiele;
 - semantische Definition graphischer Elemente und
 - Fachwortverzeichnisse.

Literaturhinweise:

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*.

Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

EWICS European Workshop on Industrial Computer Systems, TC 7: Safety Related Computers – Software Development and Systems Documentation, Verlag TÜV Rheinland, Köln, 1985.

Entwicklungstechnik sicherheitsverantwortlicher Software in der Eisenbahn-Signaltechnik. U. Feucht, Informatik-Fachberichte 86, Springer Verlag, Berlin, 184-195, 1984.

Richtlinie zur Erstellung und Prüfung sicherheitsrelevanter Software. K. Grimm, G. Heiner, Informatik Fachberichte 86, Springer Verlag, Berlin, 277-288, 1984.

B.1.3 Trennung sicherheitsbezogener Systeme von nicht sicherheitsbezogenen Systemen

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.1 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Verhinderung, dass nicht sicherheitsbezogene Teile des Systems die sicherheitsbezogenen Teile in unerwünschter Art beeinflussen.

Beschreibung: In der Spezifikation sollte entschieden werden, ob eine Trennung der sicherheitsbezogenen Systeme und der nicht sicherheitsbezogenen Systeme möglich ist. Für Schnittstellen zwischen beiden Teilen sollten eindeutige Spezifikationen geschrieben werden. Eine eindeutige Trennung reduziert den Testaufwand für die sicherheitsbezogenen Systeme.

Literaturhinweis: Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

B.1.4 Diversitäre Hardware

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen A.15, A.16 und A.18 der IEC 61508-2 aufgeführt.

Ziel: Erkennung systematischer Ausfälle während des Betriebs der EUC, indem diversitäre Bauteile mit unterschiedlichen Ausfallraten und -arten verwendet werden.

Beschreibung: Unterschiedliche Bauteilarten werden für die diversitären Kanäle eines sicherheitsbezogenen Systems verwendet. Dies reduziert die Wahrscheinlichkeit von Ausfällen infolge gemeinsamer Ursache (zum Beispiel Überspannung, elektromagnetische Störungen) und erhöht die Wahrscheinlichkeit, solche Ausfälle zu erkennen.

Mit Hilfe von unterschiedlichen Mitteln, etwa unterschiedliche physikalische Prinzipien zur Ausführung einer geforderten Funktion, werden unterschiedliche Wege zur Problemlösung beschritten.

Literaturhinweis: Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

B.2 Spezifikation der Entwurfsanforderungen des E/E/PE-Systems

Allgemeines Ziel: Erstellung einer Spezifikation, die so weit wie möglich vollständig, frei von Irrtümern, frei von Widersprüchen und einfach zu verifizieren ist.

B.2.1 Strukturierte Spezifikation

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.1 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Reduzierung der Komplexität durch Erstellung einer hierarchischen Struktur von Teilanforderungen. Vermeidung von Ausfällen an den Schnittstellen zwischen den Anforderungen.

Beschreibung: Dieses Verfahren strukturiert die funktionale Spezifikation so in Teilanforderungen, dass zwischen ihnen nur möglichst einfache Beziehungen vorkommen. Diese Zerlegung wird so lange bereinigt, bis kleine eindeutige Teilanforderungen unterschieden werden können. Das Ergebnis der abschließenden Bereinigung ist eine hierarchische Struktur von Teilanforderungen, die einen Rahmen für die Spezifikation der Gesamtanforderungen bereitstellt. Diese Methode betont die Schnittstelle der Teilanforderungen und ist besonders wirksam zur Vermeidung von Schnittstellenausfällen.

Literaturhinweise:

ESA PSS 05-02, Guide to the user requirements definition phase, European Space Agency, 1989.

Structured Analysis and System Specification. T. De Marco, Yourdon Press, Englewood Cliffs, 1979.

B.2.2 Formale Methoden

ANMERKUNG 1 Siehe C.2.4 für Einzelheiten zu bestimmten formalen Methoden.

ANMERKUNG 2 Dieses Verfahren/Maßnahme ist in den Tabellen B.1, B.2 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Unzweideutige und lückenlose Beschreibung einer Spezifikation, so dass Irrtümer und Auslassungen erkannt werden können.

Beschreibung: Formale Methoden stellen ein Mittel zur Entwicklung einer Systembeschreibung an einigen Phasen in der Systemspezifikation oder des Systementwurfs bereit. Die resultierende Beschreibung nimmt eine mathematische Form an und kann einer mathematischen Analyse unterworfen werden, um verschiedenartige Klassen von Unstimmigkeiten oder Unrichtigkeiten zu erkennen. Außerdem kann die Beschreibung in einigen Fällen maschinell mit einer ähnlichen Strenge wie die der Syntaxüberprüfung eines Quelltextes durch einen Compiler analysiert werden. Sie kann auch animiert werden, um verschiedene Verhaltensaspekte des beschriebenen Systems anzuzeigen. Die Animation kann zusätzliches Vertrauen liefern, dass das System sowohl die wirklichen als auch die formal festgelegten Anforderungen erfüllt, weil sie die menschliche Wiedererkennung des festgelegten Verhaltens verbessert.

Eine formale Methode wird im Allgemeinen eine Notation (allgemein wird eine Form diskreter Mathematik benutzt), ein Verfahren zur Aufstellung einer Beschreibung in dieser Notation und verschiedene Formen der Analyse zur Überprüfung einer Beschreibung auf unterschiedliche Eigenschaften der Korrektheit anbieten.

Ausgehend von einer mathematischen, formalen Spezifikation kann der Entwurf durch eine Reihe von schrittweisen Verfeinerungen zu einem logischen Schaltungsentwurf übertragen werden.

Literaturhinweis: Formal Specification: Techniques and Applications. N.Nissanke, Springer-Verlag Telos, 1999, ISBN-10: 1852330023.

B.2.3 Semi-formale Methoden

ANMERKUNG 1 Tabelle B.7 des Teils 3 erweitert diese Liste des Anhangs B mit anderen semi-formalen softwarebezogenen Verfahren. Teil 3 führt auf:

- Logik-/Funktionsblockdiagramme: beschrieben in IEC 61131-3,
- Ablaufdiagramme: beschrieben in IEC 61131-3,
- Datenflussdiagramme: siehe C.2.2,
- Endliche Zustandsmaschinen/Zustandsübergangsdiagramme: siehe B.2.3.2,
- Zeitgesteuerte Petri-Netze: siehe B.2.3.3,
- Entity-Relationship-Attribut-Datenmodelle: siehe C.2.14,

- Nachrichtenverlaufstabellen: siehe C.2.15,
- Entscheidungs-/Wahrheitstabellen: siehe C.6.1.

Ziel: Unzweideutige und lückenlose Beschreibung einer Spezifikation, so dass Irrtümer, Auslassungen und fehlerhaftes Verhalten erkannt werden können.

ANMERKUNG 2 Dieses Verfahren/Maßnahme ist in den Tabellen B.1, B.2 und B.6 der IEC 61508-2 und in den Tabellen A.1, A.2, A.4, B.7, C-A.1, C-A.2, C-A.4 und C-B.7 der IEC 61508-3 aufgeführt.

B.2.3.1 Allgemeines

Ziel: Beweis, dass der Entwurf seine Spezifikation erfüllt.

Beschreibung: Semi-formale Methoden stellen Mittel zur Entwicklung einer Systembeschreibung in einigen Stufen der Systementwicklung, d. h. Spezifikation, Entwurf oder Codierung, bereit. Die Beschreibung kann in einigen Fällen maschinell analysiert oder animiert werden, um verschiedenen Aspekte des Systemverhaltens anzuzeigen. Die Animation kann zusätzliches Vertrauen liefern, dass das System sowohl die wirklichen als auch die formal festgelegten Anforderungen erfüllt.

In den folgenden Unterabschnitten werden zwei semi-formale Methoden beschrieben.

B.2.3.2 Endliche Zustandsmaschinen/Zustandsübergangsdiagramme

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.5, B.7, C-B.5 und C-B.7 der IEC 61508-3 aufgeführt.

Ziel: Gestaltung, Verifikation, Spezifikation oder Implementierung der Steuerungsstruktur eines Systems.

Beschreibung: Viele Systeme können hinsichtlich ihrer Zustände, ihrer Eingaben und ihrer Aktionen beschrieben werden. So könnte ein System im Zustand S1 nach Empfang der Eingabe E die Aktion A ausführen und in den Zustand S2 übergehen. Wir können ein System durch Beschreibung der Systemaktionen für jede Eingabe in jedem Zustand vollständig beschreiben. Das resultierende Systemmodell wird eine endliche Zustandsmaschine (oder endlicher Zustandsautomat) genannt. Es wird oft als ein so genanntes Zustandsübergangsdiagramm dargestellt, das zeigt, wie sich ein System von einem Zustand in den anderen bewegt, oder als eine Matrix, in der die Dimensionen Zustand und Eingabe sind. Die Matrix-Zellen enthalten die Aktion und den neuen Zustand, der sich aus dem Empfang der Eingabe in dem gegebenen Zustand ergibt.

Wenn ein System komplex ist oder eine natürliche Struktur hat, kann sich dies in einer geschichteten endlichen Zustandsmaschine ausdrücken.

Eine als eine endliche Zustandsmaschine beschriebene Spezifikation oder Entwurf kann geprüft werden auf

- Vollständigkeit (das System muss eine Aktion und einen neuen Zustand für jede Eingabe in jedem Zustand haben),
- Konsistenz (nur eine Zustandsänderung wird für jedes Zustands-/Eingabepaar beschrieben),
- Erreichbarkeit (ob es möglich ist, von einem Zustand zum anderen durch jede beliebige Folge von Eingaben zu gelangen) und
- Mangel an Endlosschleifen oder Dead-End-States usw.

Dies sind wichtige Eigenschaften für kritische Systeme. Werkzeuge zur Unterstützung dieser Prüfungen sind leicht zu entwickeln und verschiedene auf endliche Zustandsautomaten basierende Modelle (formale Sprachen, Petri-Netze, Markov-Graphen usw.) können verwendet werden. Es existieren auch Algorithmen, die die automatische Erzeugung von Testfällen zur Verifikation der Implementierung einer Zustandsmaschine oder zur Animation eines Modells einer Zustandsmaschine erlauben.

Sie können auch zur Berechnung der Ausfallwahrscheinlichkeit verwendet werden, siehe C.6.

Literaturhinweis: Introduction to Automata Theory, Languages, and Computation (3rd Edition). J. Hopcroft, R. Motwani, J. Ullman, Addison-Wesley Longman Publishing Co, 2006, ISBN:0321462254.

B.2.3.3 Zeitgesteuerte Petri-Netze

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.5, B.7, C-B.5 und C-B.7 der IEC 61508-3 aufgeführt.

Ziel: Modellierung von wichtigen Gesichtspunkten des Systemverhaltens, Bewertung und möglicherweise Verbesserung der Sicherheit und betrieblicher Anforderungen durch Analyse und Redesign.

Beschreibung: Petri-Netze sind ein besonderer Fall von endlichen Zustandsautomaten. Sie gehören zu einer Klasse von Modellen der Graphentheorie, die geeignet sind, Informations- und Kontrollflüsse in Systemen darzustellen, die nebeneinander laufen und asynchrones Verhalten haben.

Ein Petri-Netz ist ein Netzwerk von Stellen und Transitionen. Die Stellen können markiert oder nicht markiert sein. Eine Transition wird aktiviert, wenn alle Eingabestellen zu ihr markiert sind. Wenn sie aktiviert ist, darf sie (muss aber nicht) „feuern“. Ist dies geschehen, werden die Markierungen der Eingabestellen wieder entfernt und stattdessen alle Ausgabestellen der Transition markiert.

Mögliche Gefahren können als besondere Zustände (Markierungen) in dem Modell dargestellt werden. Das Petri-Netz-Modell kann unter Berücksichtigung von zeitlichen Eigenschaften des Systems erweitert werden. Obwohl sich „klassische“ Petri-Netze auf Aspekte des Kontrollflusses konzentrieren, sind mehrere Erweiterungen zur Einbeziehung von Datenflüssen in das Modell vorgeschlagen worden.

Sie stellen ebenfalls eine sehr effiziente Unterstützung zur Ausführung der Monte-Carlo Simulation zur Verfügung, um die Berechnungen der Ausfallwahrscheinlichkeit auszuführen, siehe C.6.

Literaturhinweise:

Timed Petri Nets: Theory and Application. Jiapun Wang, Springer, 1998, ISBN 0792382706.

Using Petri nets for safety analysis of unmanned Metro system. M. El Kursi, P. Ozello, Proc. SAFECOMP '92, 135-139, Pergamon Press, 1992.

Petri nets: Properties, analysis and applications. T. Murata, Proc. IEEE 77 (4), 541-580, April 1989.

Safety analysis using Petri nets. N. G. Leveson, J. L. Stolzy, Proc. 15th Ann. Int. Symp on Fault-Tolerant Computing, 358-363, IEEE, 1985.

Net theory and applications. W. Brauer (ed.), Lecture Notes in Computer Science, Vol. 84, Springer Verlag, 1980.

B.2.4 Rechnerunterstützte Spezifikationswerkzeuge

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.1 und B.6 der IEC 61508-2 und in den Tabellen A.1, A.2, C-A.1 und C-A.2 der IEC 61508-3 aufgeführt.

B.2.4.1 Allgemeines

Ziel: Verwendung formaler Spezifikationsverfahren, um die automatische Erkennung von Zweideutigkeiten und der Vollständigkeit zu erleichtern.

Beschreibung: Dieses Verfahren erzeugt eine Spezifikation in Form einer Datenbank, die automatisiert überprüft werden kann, um die Übereinstimmung und Vollständigkeit zu bewerten. Das Spezifikationswerkzeug kann dem Anwender verschiedene Aspekte des festgelegten Systems durch eine Animation zeigen. Im Allgemeinen unterstützt dieses Verfahren nicht nur die Erstellung der Spezifikation, sondern auch den Entwurf und andere Phasen des Projektlebenszyklus. Spezifikationswerkzeuge können nach den folgenden Unterabschnitten klassifiziert werden.

B.2.4.2 Methodenunspezifische Werkzeuge

Ziel: Unterstützung des Anwenders zur Erstellung einer geeigneten Spezifikation, indem Hinweise und Verbindungen zu zugehörigen Teilen bereitgestellt werden.

Beschreibung: Das Spezifikationswerkzeug übernimmt einige Routinearbeiten des Anwenders und unterstützt das Projektmanagement. Es erzwingt keine besonderen Spezifikationsmethoden. Die relative Unabhängigkeit im Hinblick auf die Methode gestattet dem Anwender einen hohen Freiheitsgrad, gibt ihm aber nur wenig von der zur Erstellung von Spezifikationen notwendigen Unterstützung. Dies erschwert die Einarbeitung in das System.

B.2.4.3 Modellorientierte Verfahren mit hierarchischer Analyse

Ziel: Unterstützung des Anwenders zur Erstellung einer geeigneten Spezifikation, indem die Übereinstimmung der Beschreibungen der Aktionen mit den Daten bei verschiedenen Abstraktionsgraden sichergestellt wird.

Beschreibung: Diese Methode gibt eine funktionale Darstellung des gewünschten Systems (strukturierte Analyse) bei verschiedenen Abstraktionsgraden (Genauigkeitsgrad) wieder. Die Analyse auf verschiedenen Ebenen betrifft sowohl die Aktionen als auch die Daten. Die Bewertung der Zweideutigkeit und Vollständigkeit ist zwischen hierarchischen Ebenen wie auch zwischen zwei Funktionseinheiten (Modulen) auf der gleichen Ebene möglich.

Literaturhinweise:

System requirements analysis. Jeffrey O. Grady, Academic Press, 2006, ISBN 012088514X, 9780120885145.

Structured Analysis for Requirements Definition. D.T. Ross, K.E. Schoman, IEEE Transactions on Software Engineering, vol. 3, no. 1, pp. 6-15, Jan/Feb, 1977.

B.2.4.4 Entity-Relationship-Modelle

Ziel: Unterstützung des Anwenders zur Erstellung einer geeigneten Spezifikation durch Konzentration auf Einheiten innerhalb des Systems und den Beziehungen zwischen diesen.

Beschreibung: Das gewünschte System wird als eine Ansammlung von Objekten und ihren Beziehungen beschrieben. Das Werkzeug ermöglicht es, zu bestimmen, welche Beziehungen von dem System interpretiert werden können. Die Beziehungen lassen im Allgemeinen eine Beschreibung der hierarchischen Struktur der Objekte, des Datenflusses, der Beziehungen zwischen den Daten und welche Daten bestimmten Anwendungsprozessen unterliegen zu. Das klassische Verfahren wurde für Prozesssteuerungsanwendungen erweitert. Inspektionsmöglichkeiten und Unterstützung des Anwenders hängen von der Vielfalt der dargestellten Beziehungen ab. Auf der anderen Seite macht eine große Anzahl von Darstellungsmöglichkeiten die Anwendung dieses Verfahren komplex.

Literaturhinweis: Software Requirements: Practical Techniques for Gathering and Managing Requirements Throughout the Product Development Cycle. Karl Eugene Wiegers, Microsoft Press, 2003, ISBN 0735618798, 9780735618794.

B.2.4.5 Anregung und Antwort

Ziel: Unterstützung des Anwenders zur Erstellung einer geeigneten Spezifikation durch Identifizierung von Anregung-Antwort-Beziehungen.

Beschreibung: Die Beziehungen zwischen den Objekten des Systems werden in einer Notation der „Anregung“ und „Antwort“ festgelegt. Es wird eine einfache und leicht erweiterte Sprache verwendet, die Sprach-elemente zur Darstellung von Objekten, Beziehungen, Eigenschaften und Strukturen beinhaltet.

B.2.5 Checklisten

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.1, B.2 und B.6 der IEC 61508-2 und in den Tabellen A.10, B.8, C-A.10 und C-B.8 der IEC 61508-3 aufgeführt.

Ziel: Vollständig und kritisch anhand des Sicherheitslebenszyklus alle wichtigen Systemaspekte behandeln, ohne genaue Anforderungen niederzulegen.

Beschreibung: Eine Auswahl von Fragen sind von der Person, die die Checkliste anwendet, zu beantworten. Viele Fragen sind von allgemeiner Natur, und der Beurteilende muss diese so geeignet wie möglich für das zu beurteilende System interpretieren. Checklisten können für alle Phasen des Gesamt-Sicherheitslebenszyklus, des Sicherheitslebenszyklus des E/E/PE-Systems und des Software-Sicherheitslebenszyklus verwendet werden und sind insbesondere als ein Werkzeug zur Unterstützung der Beurteilung der funktionalen Sicherheit nützlich.

Um die vielen Arten von zu validierenden Systemen zu berücksichtigen, beinhalten die meisten Checklisten Fragen, die auf viele Systemarten anwendbar sind. Deshalb mag es Fragen in den Checklisten geben, die für das zu behandelnde System nicht zutreffen und die deshalb vernachlässigt werden sollten. Ebenso mag es bei einem besonderen System notwendig sein, die Standard-Checkliste mit speziellen Fragen zu ergänzen.

Es ist einleuchtend, dass die erfolgreiche Verwendung von Checklisten von der Fachkenntnis und dem Beurteilungsvermögen des Ingenieurs abhängig ist, der die Checkliste auswählt und anwendet. Daraus resultierend sollte jede von dem Ingenieur getroffene Entscheidung zu den ausgewählten Checklisten und zusätzlichen oder überflüssigen Fragen vollständig dokumentiert und gerechtfertigt werden. Dadurch soll sichergestellt werden, dass die Anwendung der Checklisten überprüfbar ist und dass die gleichen Ergebnisse erreicht werden, sofern nicht unterschiedliche Kriterien verwendet werden.

Genauigkeit ist das Ziel bei der Erstellung einer Checkliste. Wenn eine umfassende Rechtfertigung notwendig ist, dann sollte dies durch Verweis auf zusätzliche Dokumente erfolgen. Zur Dokumentation der Ergebnisse jeder Frage sollte eine begrenzte Auswahl von Antworten wie bestanden, durchgefallen und ergebnislos oder ähnlich verwendet werden. Diese Genauigkeit vereinfacht außerordentlich das Verfahren, um ein Gesamtergebnis aus Checklistenauswertungen zu erzielen.

Literaturhinweise:

IEC 60880:2006, *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions.*

The Art of Software Testing, Second Edition. G. Myers et al., Wiley & Sons, New York, 2004, ISBN 0471469122, 9780471469124.

Software Quality Assurance: From Theory to Implementation. Daniel Galin, Pearson Education, 2004, ISBN 0201709457, 9780201709452.

IEC 61346 (alle Teile), *Industrial systems, installations and equipment and industrial products – Structuring principles and reference designation.*

Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

Risk Assessment and Risk Management for the Chemical Process Industry. H.R. Greenberg, J.J. Cramer, John Wiley and Sons, 1991, ISBN 0471288829, 9780471288824.

B.2.6 Inspektion der Spezifikation

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.1 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Vermeidung von Unvollständigkeiten und Widersprüchen in der Spezifikation.

Beschreibung: Die Inspektion ist ein allgemeines Verfahren, in der verschiedene Eigenschaften einer Spezifikation von einer unabhängigen Arbeitsgruppe bewertet werden. Die Arbeitsgruppe stellt Fragen an den Ersteller, der diese zufrieden stellend beantworten muss. Die Prüfung sollte wenn möglich von einer Arbeitsgruppe ausgeführt werden, die nicht in die Erstellung der Spezifikation eingebunden war. Der erforderliche Grad der Unabhängigkeit wird durch den für das System erforderlichen Sicherheits-Integritätslevel bestimmt. Die unabhängigen Prüfer sollten in der Lage sein, die Systemfunktion in einer zweifelsfreien Art und Weise ohne Bezug zu weiteren Spezifikationen zu rekonstruieren. Sie müssen ebenfalls prüfen, ob alle zutreffenden Sicherheits- und technischen Aspekte durch die betrieblichen und organisatorischen Maßnahmen abgedeckt werden. Dieses Verfahren hat sich in der Praxis als sehr wirksam erwiesen.

Literaturhinweise:

IEC 61160:2006, *Design review*.

The Art of Software Testing, Second Edition. G. Myers et al., Wiley & Sons, New York, 2004, ISBN 0471469122, 9780471469124.

Software Quality Assurance: From Theory to Implementation. D. Galin, Pearson Education, 2004, ISBN 0201709457, 9780201709452.

B.3 Entwurf und Entwicklung des E/E/PE-Systems

Allgemeines Ziel: Erstellung eines stabilen Entwurfs eines sicherheitsbezogenen Systems in Übereinstimmung mit der Spezifikation.

B.3.1 Beachtung von Richtlinien und Normen

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle B.2 der IEC 61508-2 aufgeführt.

Ziel: Beachtung anwendungsspezifischer Normen (nicht in dieser Norm festgelegte).

Beschreibung: Während des Entwurfs des sicherheitsbezogenen Systems sollten Richtlinien befolgt werden. Diese Richtlinien sollten erstens zu sicherheitsbezogenen Systemen führen, die praktisch frei von Ausfällen sind, und zweitens die nachfolgende Validierung bezüglich der Sicherheit erleichtern. Sie können allgemeingültig, projektspezifisch oder spezifisch für eine einzelne Phase sein.

Literaturhinweise:

Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

Deutsche Bundesbahn: Richtlinien-Entwürfe 42500 bis 42550 für das Handbuch „Grundsätze zur technischen Zulassung in der Signal- und Nachrichtentechnik“. Bundesbahn-Zentralamt München, August 1987.

EWICS European Workshop on Industrial Computer Systems, TC 7: Safety Related Computers – Software Development and Systems Documentation. Verlag TÜV Rheinland, Köln, 1985.

B.3.2 Strukturierter Entwurf

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Reduzierung der Komplexität durch Erstellung einer hierarchischen Struktur von Teilanforderungen. Vermeidung von Schnittstellenausfällen zwischen den Anforderungen. Vereinfachung der Verifikation.

Beschreibung: Während des Entwurfs der Hardware sollten bestimmte Kriterien und Methoden verwendet werden. Zum Beispiel kann Folgendes erforderlich sein:

- ein hierarchisch strukturierter Schaltungsentwurf und
- Verwendung bereits erstellter und getesteter Schaltungsteile.

Auf ähnliche Weise ermöglicht die Verwendung strukturierter Diagramme während des Entwurfs der Software eine eindeutige Struktur der Softwaremodule. Die Struktur zeigt, wie die Module zueinander in Verbindung stehen, die genauen Daten, die zwischen ihnen ausgetauscht werden, und deren Abstimmung.

Literaturhinweise:

Software Engineering for Real-time Systems. J. E. Cooling, Pearson Education, 2003, ISBN 0201596202, 9780201596205.

Software Design. D. Budgen, Pearson Education, 2003, ISBN 0201722194, 9780201722192.

IEC 61346-1 (alle Teile), *Industrial systems, installations and equipment and industrial products – Structuring principles and reference designations*.

An Overview of JSD, J. R. Cameron, IEEE Trans SE-12 No. 2, Februar 1986.

Structured Development for Real-Time Systems (3 Volumes). P. T. Yourdon, P. T. Yourdon Press, 1985.

Structured Development for Real-Time Systems (3 Volumes). P. T. Ward, S. J. Mellor, Yourdon Press, 1985.

Applications and Extensions of SADT. D. T. Ross, Computer, 25-34, April 1985.

Essential Systems Analysis. St. M. McMenamin, F. Palmer, Yourdon Inc, 1984.

System Development. M. Jackson, Prentice-Hall, 1983.

Structured Analysis for Requirements Definition. D. T. Ross, K. E. Schoman Jr, IEEE Trans. Software Eng, Vol. SE-3, 6-15, 1977.

Structured Analysis (SA): A language for communicating ideas. D. T. Ross, IEEE Trans. Software Eng, Vol. SE-3 (1), 16-34.

B.3.3 Verwendung von bewährten Bauteilen

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Reduzierung des Risikos vieler erstmaliger und unerkannter Fehler durch die Verwendung von Bauteilen mit speziellen Eigenschaften.

Beschreibung: Die Auswahl von betriebsbewährten Bauteilen erfolgt durch den Hersteller nach der Zuverlässigkeit der Bauteile im Hinblick auf die Sicherheit (zum Beispiel die Verwendung von betrieblich erprobten Einheiten, um hohe Sicherheitsanforderungen zu erfüllen, oder die Speicherung sicherheitsrelevanter Programme nur in sicheren Speichern). Die Sicherheit von Speichern kann sich sowohl auf unberechtigten Zugriff als auch auf Umgebungseinflüsse (elektromagnetische Verträglichkeit, Strahlung usw.) beziehen und auf die Reaktion der Bauteile im Falle eines auftretenden Ausfalls.

Literaturhinweise:

IEC 61163-1:2006, *Reliability stress screening – Part 1: Repairable items manufactured in lots*.

Zuverlässigkeit elektronischer Komponenten. T. Bajenescu, VDE-Verlag, Berlin, 1985.

Microcomputers in safety technique – an aid to orientation for developer and manufacturer. H. Hölscher, J. Rader, Verlag TÜV Rheinland, Köln, 1986, ISBN 3-88585-315-9.

Reliability Testing for Industrial use. W. T. Greenwood, Computer, 10 (7), 26-30, 1977.

Independent Test Labs: Caveat Emptor. E. Rubinstein, IEEE Spectrum, 14 (6), 44-50, 1977.

B.3.4 Modularisierung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Reduzierung der Komplexität und Vermeidung von Ausfällen bezogen auf Schnittstellen zwischen Teilsystemen.

Beschreibung: Auf allen Ebenen des Entwurfs wird jedes Teilsystem klar definiert und ist in der Größe beschränkt (nur wenige Funktionen). Die Schnittstellen zwischen Teilsystemen werden so einfach wie möglich gehalten und Querverbindungen (d. h. gemeinsame Daten, Informationsaustausch) werden gering gehalten. Die Komplexität der einzelnen Teilsysteme ist ebenfalls beschränkt.

Literaturhinweise:

The Art of Software Testing, Second Edition. G. Myers et al., Wiley & Sons, New York, 2004, ISBN 0471469122, 9780471469124.

Software Engineering for Real-time Systems. J. E. Cooling, Pearson Education, 2003, ISBN 0201596202, 9780201596205.

EWICS European Workshop on Industrial Computer Systems, TC 7: Safety Related Computers – Software Development and Systems Documentation. TÜV Rheinland, Köln, 1985.

Software Reliability – Principles and Practices. G. J. Myers, Wiley-Interscience, New York, 1976.

B.3.5 Rechnerunterstützte Entwurfswerkzeuge

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2 und B.6 der IEC 61508-2 und in den Tabellen A.4 und C-A.4 der IEC 61508-3 aufgeführt.

Ziel: Systematischere Ausführung des Entwurfsprozesses. Einbeziehung geeigneter automatischer Konstruktionselemente, die bereits verfügbar und getestet sind.

Beschreibung: Rechnerunterstützte Entwurfswerkzeuge (en: computer aided design, CAD) sollten, wenn verfügbar und durch die Komplexität des Systems gerechtfertigt, während des Entwurfs der Hardware und Software verwendet werden. Die Korrektheit solcher Werkzeuge sollte durch spezielle Tests, durch langfristig nachgewiesene zufrieden stellende Anwendung oder durch unabhängige Verifikation ihrer Ergebnisse im Hinblick auf das zu entwerfende sicherheitsbezogene System nachgewiesen werden.

Hilfswerkzeuge sollten nach ihrem Integrationsgrad ausgewählt werden. In diesem Zusammenhang werden Werkzeuge als integriert bezeichnet, wenn sie derart zusammenwirkend arbeiten, dass die Ausgaben des einen Werkzeugs geeigneten Inhalt und geeignetes Format zur automatischen Eingabe des nachfolgenden Werkzeugs haben. Demzufolge wird die Möglichkeit gemindert, dass menschliches Versagen beim Überarbeiten von Zwischenergebnissen eingebracht wird.

Literaturhinweise:

Overview of Technology Computer-Aided Design Tools and Applications in Technology Development, Manufacturing and Design. W. Fichtner, Journal of Computational and Theoretical Nanoscience, Volume 5, Number 6, June 2008, pp. 1089-1105(17).

The Electromagnetic Data Exchange: Much more than a Common Data Format. P.E. Frandsen et al. In *Proceeding of the 2nd European Conference on Antennas and Propagation*. The Institution of Engineering and Technology (IET), 2007, ISBN 978-0-86341-842-6.

Software engineering: Update. Ian Sommerville, Pearson Education, 2006, ISBN 0321313798, 9780321313799.

An Experience in Design and Validation of Software for a Reactor Protection System. S. Bologna, E. de Agostino et al, IFAC Workshop, SAFECOMP 1979, Stuttgart, 16-18 May 1979, Pergamon Press, 1979.

B.3.6 Simulation

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2, B.5 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Ausführung einer systematischen und vollständigen Inspektion eines elektrischen/elektronischen Schaltkreises, bezogen sowohl auf die funktionale Ausführung als auch auf die korrekte Dimensionierung der Bauteile.

Beschreibung: Die Funktion des Schaltkreises eines sicherheitsbezogenen Systems wird auf einem Rechner mittels eines softwaremäßigen Verhaltensmodells simuliert. Jedes einzelne Bauteil des Schaltkreises hat sein eigenes simuliertes Verhalten und die Reaktion des Schaltkreises, in dem dieses eingebunden ist, wird durch Beobachtung der Grenzdaten jedes Bauelements geprüft.

Literaturhinweise:

VDI-Gemeinschaftsausschuss Industrielle Systemtechnik: Software-Zuverlässigkeit. VDI-Verlag, 1993.

Using an executable specification language for an information system. S. Urban et al, IEEE Trans Software Engineering, Vol. SE-11 No. 7, July 1985.

Verification and validation of Real-time Software. W. J. Quirk (ed.), Springer Verlag, Berlin, 1985.

Proc. Working Conference on Prototyping. Namur, October 1983, Budde et al, Springer Verlag, 1984.

B.3.7 Inspektion (Überprüfungen und Analysen)

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Aufdeckung von Widersprüchen zwischen Spezifikation und Ausführung.

Beschreibung: Festgelegte Funktionen des sicherheitsbezogenen Systems werden geprüft und ausgewertet, um zu gewährleisten, dass das sicherheitsbezogene System den in der Spezifikation gegebenen Anforderungen entspricht. Jeder Punkt, der die Ausführung und die Anwendung des Produkts in Frage stellt, wird dokumentiert, so dass dieser ausgeräumt werden kann. Im Gegensatz zu einem Walkthrough ist der Autor während der Inspektion passiv und der Prüfer aktiv.

Literaturhinweise:

IEC 61160:2006, *Design Review*.

Software engineering: Update. Ian Sommerville, Pearson Education, 2006, ISBN 0321313798, 9780321313799.

The Art of Software Testing, Second Edition. G. Myers et al., Wiley & Sons, New York, 2004, ISBN 0471469122, 9780471469124.

ANSI/IEEE Std. 1028:1997, IEEE Standard for software reviews and audits.

VDI-Gemeinschaftsausschuss Industrielle Systemtechnik: Software-Zuverlässigkeit. VDI-Verlag, 1993.

Dependability of Critical Computer Systems 3. P. G. Bishop et al, Elsevier Applied Science, 1990, ISBN 1-85166-544-7.

B.3.8 Walkthrough

ANMERKUNG Dieses Verfahren/Maßnahme ist in den Tabellen B.2 und B.6 der IEC 61508-2 aufgeführt.

Ziel: Aufdeckung von Widersprüchen zwischen Spezifikation und Ausführung.

Beschreibung: Festgelegte Funktionen des Entwurfs des sicherheitsbezogenen Systems werden geprüft und ausgewertet, um zu gewährleisten, dass das sicherheitsbezogene System den in der Spezifikation gegebenen Anforderungen entspricht. Mögliche Schwachpunkte der Realisierung und der Anwendung des Produkts werden dokumentiert, so dass diese ausgeräumt werden können. Im Gegensatz zu einer Inspektion ist der Autor während der Inspektion aktiv und der Prüfer passiv.

Literaturhinweise:

Software engineering: Update. Ian Sommerville, Pearson Education, 2006, ISBN 0321313798, 9780321313799.

ANSI/IEEE Std. 1028:1997, IEEE Standard for software reviews and audits.

Dependability of Critical Computer Systems 3. P. G. Bishop et al, Elsevier Applied Science, 1990, ISBN 1-85166-544-7.

Methodisches Testen von Programmen. G. J. Myers, Oldenbourg Verlag, München, Wien, 1987.

B.4 Betriebs- und Instandhaltungsverfahren des E/E/PE-Systems

Allgemeines Ziel: Entwicklung von Verfahren, die die Ausfälle während des Betriebs und der Instandhaltung des sicherheitsbezogenen Systems zu vermeiden helfen.

B.4.1 Betriebs- und Instandhaltungsanweisungen

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle B.4 der IEC 61508-2 aufgeführt.

Ziel: Vermeidung von Irrtümern während des Betriebs und der Instandhaltung des sicherheitsbezogenen Systems.

Beschreibung: Betriebsanweisungen beinhalten wesentliche Informationen, wie das sicherheitsbezogene System anzuwenden und in Stand zu halten ist. In besonderen Fällen enthalten diese Anweisungen auch Beispiele, wie das sicherheitsbezogene System im Allgemeinen zu installieren ist. Alle Anweisungen müssen leicht verständlich sein. Bilder und Diagramme sollten verwendet werden, um komplexe Verfahren und Abhängigkeiten zu beschreiben.

Literaturhinweis: Guidelines for Safe Automation of Chemical Processes. CCPS, AIChE, New York, 1993.

B.4.2 Benutzerfreundlichkeit

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle B.4 der IEC 61508-2 aufgeführt.

Ziel: Reduzierung der Komplexität während des Betriebs des sicherheitsbezogenen Systems.

Beschreibung: Der korrekte Betrieb des sicherheitsbezogenen Systems kann zu einem bestimmten Grad von der menschlichen Handhabung abhängen. Unter Berücksichtigung des relevanten Systementwurfs und des Entwurfs des Arbeitsplatzes muss der Entwickler des sicherheitsbezogenen Systems gewährleisten, dass

- der Bedarf nach menschlichen Eingriffen auf ein absolutes Minimum beschränkt wird;
- der notwendige Eingriff so einfach wie möglich ist;