

	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (IEC 61508-7:2000) Deutsche Fassung EN 61508-7:2001	<u>DIN</u> EN 61508-7
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0803 Teil 7
ICS 25.040.40; 35.240.50 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures; (IEC 61508-7:2000); German version EN 61508-7:2001 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures; (CEI 61508-7:2000); Version allemande EN 61508-7:2001 Die Europäische Norm EN 61508-7:2001 hat den Status einer Deutschen Norm. Beginn der Gültigkeit Die EN 61508-7 wurde am 2001-07-03 angenommen. Nationales Vorwort Für die vorliegende Norm 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 zuständig. Norm-Inhalt war veröffentlicht als E DIN IEC 65A/185/CD:1996-09 (VDE 0801 Teil 7). Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet. Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2006 unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation – bestätigt, – zurückgezogen, – durch eine Folgeausgabe ersetzt oder – geändert. Fortsetzung Seite 2 bis 5 und 111 Seiten EN DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

DIN EN 61508-7 (VDE 0803 Teil 7):2003-06

Die Vornormen

DIN V VDE 0801 (VDE 0801):1990-01 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben

DIN V VDE 0801/A1 (VDE 0801/A1):1994-10 Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben; Änderung 1:1994-10

DIN V 19250:1994-05 Leittechnik – Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen und

DIN V 19251:1995-02 Leittechnik – MSR-Schutzeinrichtungen – Anforderungen und Maßnahmen zur gesicherten Funktion

enthalten Festlegungen, die den Festlegungen in den Normen der Reihe DIN EN 61508 (VDE 0803) entgegenstehen oder zu ihnen redundant sind.

Die DKE beabsichtigt daher, die oben genannten Vornormen zum 1. August 2004 zurückzuziehen.

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.

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist nachstehend wiedergegeben. Zum Zeitpunkt der Veröffentlichung dieser Norm waren die angegebenen Ausgaben gültig.

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-1:2001	IEC 61508-1:1998	DIN EN 61508-1 (VDE 0803 Teil 1):2002-11	VDE 0803 Teil 1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803 Teil 2):2002-12	VDE 0803 Teil 2
EN 61508-3:2001	IEC 61508-3:1998	DIN EN 61508-3 (VDE 0803 Teil 3):2002-12	VDE 0803 Teil 3
EN 61508-4:2001	IEC 61508-4:1998	DIN EN 61508-4 (VDE 0803 Teil 4):2002-11	VDE 0803 Teil 4
EN 61508-5:2001	IEC 61508-5:1998	DIN EN 61508-5 (VDE 0803 Teil 5):2002-11	VDE 0803 Teil 5
EN 61508-6:2001	IEC 61508-6:2000	DIN EN 61508-6 (VDE 0803 Teil 6): in Vorbereitung	VDE 0803 Teil 6
–	IEC Guide 104:1997	–	–
–	ISO/IEC Guide 51:1990	DIN 820-120:2001-10	–

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 60068-1:1994	IEC 60068-1:1988	DIN EN 60068-1:1995	–
EN 60529:1991	IEC 60529:1989	DIN EN 60529:2000	VDE 0470 Teil 1
–	IEC 60812:1985	–	–
–	IEC 60880:1986	DIN IEC 60880:1987	–
EN 61000-4-1:1994 Ersetzt durch: EN 61000-4-1:2000	IEC 61000-4-1:1992 Ersetzt durch: IEC 61000-4-1:2000	DIN EN 61000-4-1:1995 Ersetzt durch: DIN EN 61000-4-1:2001	VDE 0847 Teil 4-1
EN 61000-4-5:1995	IEC 61000-4-5:1995	DIN EN 61000-4-5:2001	VDE 0847 Teil 4-5
–	IEC 61000-5-2:1997	–	–
–	IEC 61025:1990	DIN IEC 61025:1993	–
EN 61069-5:1995	IEC 61069-5:1994	DIN EN 61069-5:1995	–
EN 61078:1993	IEC 61078:1991	DIN EN 61078:1994	–
EN 61131-3:1993	IEC 61131-3:1993	DIN EN 61131-3:1994	–
–	IEC 61160:1992	–	–
–	IEC 61163-1:1995	–	–
–	IEC 61164:1995	–	–
–	IEC 61165:1995	–	–
EN 61346-1:1996	IEC 61346-1:1996	DIN EN 61346-1:1997	–
–	IEC 61506:1997	–	–
–	IEC 61704: wird veröffentlicht	–	–
–	ISO 5807:1985	–	–
EN 27185:1992	ISO 7185:1990	DIN EN 27185:1994	–
EN 28631:1993	ISO/IEC 8631:1989	DIN EN 28631:1994	–
–	ISO 8652:1995	DIN ISO/IEC 8652:1996	–
–	ISO/IEC 8807:1989	–	–
EN 29899:1993	ISO/IEC 9899:1990	DIN EN 29899:1994	–
–	ISO/IEC/TR 10206:1991	–	–
–	ISO/IEC 10514-1:1996	–	–
–	ISO/IEC 10514-3:1998	–	–
–	ISO/IEC 13817-1:1996	–	–
–	ISO/IEC 14882:1998	–	–
–	ISO/IEC 1539-1:1997	–	–
–	ISO/IEC/TR 15942: wird veröffentlicht	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-120, *Normungsarbeit – Teil 120: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC-Guide 51:1999).*

DIN EN 61508-2 (VDE 0803 Teil 2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.*

DIN EN 61508-1 (VDE 0803 Teil 1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen.*

DIN EN 61508-2 (VDE 0803 Teil 2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme.*

DIN EN 61508-3 (VDE 0803 Teil 3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software.*

DIN EN 61508-4 (VDE 0803 Teil 4), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen.*

DIN EN 61508-5 (VDE 0803 Teil 5), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level).*

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

DIN EN 60068-1, *Umweltprüfungen – Teil 1: Allgemeines und Leitfaden.*

DIN EN 60529, *Schutzarten durch Gehäuse (IP-Code).*

DIN IEC 60880, *Software für Rechner im Sicherheitssystem von Kernkraftwerken.*

DIN EN 61000-4-1, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-1: Prüf- und Messverfahren; Übersicht über die Reihe IEC 61000-4.*

DIN EN 61000-4-5, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-5: Prüf- und Messverfahren; Prüfung der Störfestigkeit gegen Stoßspannungen.*

DIN IEC 61025, *Störungsbaumanalyse.*

DIN EN 61069-5, *Leittechnik für industrielle Prozesse – Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines Systems – Teil 5: Eignungsbeurteilung der Systemverlässlichkeit.*

DIN EN 61078, *Techniken für die Analyse der Zuverlässigkeit – Verfahren mit Zuverlässigkeitsblockdiagramm.*

DIN EN 61131-3, *Speicherprogrammierbare Steuerungen – Teil 3: Programmiersprachen.*

DIN EN 61346-1, *Industrielle Systeme, Anlagen und Ausrüstungen und Industrieprodukte – Strukturierungsprinzipien und Referenzkennzeichnung – Teil 1: Allgemeine Regeln.*

DIN EN 27185, *Programmiersprachen; Pascal.*

DIN EN 28631, *Informationstechnik – Programmkonstrukte und Regeln für ihre Anwendung.*

DIN ISO/IEC 8652, *Informationstechnik, Programmiersprachen – Ada.*

DIN EN 29899, *Programmiersprachen; C.*

– Leerseite –

Deutsche Fassung

**Funktionale Sicherheit sicherheitsbezogener
elektrischer/elektronischer/programmierbarer elektronischer Systeme
Teil 7: Anwendungshinweise über Verfahren und Maßnahmen
(IEC 61508-7:2000)**

Functional safety of
electrical/electronic/programmable electronic
safety-related systems
Part 7: Overview of techniques and measures
(IEC 61508-7:2000)

Sécurité fonctionnelle des systèmes
électriques/électroniques/électroniques
programmables relatifs à la sécurité
Partie 7: Présentation de techniques et mesures
(CEI 61508-7:2000)

Diese Europäische Norm wurde von CENELEC am 2001-07-03 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.

CENELEC

Europäisches Komitee für Elektrotechnische Normung
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Vorwort

Der Text der Internationalen Norm IEC 61508-7:2000, ausgearbeitet von dem SC 65A „System aspects“ des IEC TC 65 „Industrial-process measurement and control“, wurde dem Einstufigen Annahmeverfahren unterworfen und von CENELEC am 2001-07-03 ohne irgendeine Abänderung als EN 61508-7 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2002-08-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2004-08-01

Anhänge, die als „normativ“ bezeichnet sind, gehören zum Norminhalt.

Anhänge, die als „informativ“ bezeichnet sind, enthalten nur Informationen.

In dieser Norm ist Anhang ZA normativ und sind die Anhänge A, B, C und D informativ.

Der Anhang ZA wurde von CENELEC hinzugefügt.

Die IEC 61508 ist eine Sicherheitsgrundnorm zur funktionalen Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen sicherheitsbezogenen Systemen. Der Anwendungsbereich lautet:

„Diese Internationale Norm behandelt diejenigen Gesichtspunkte, die zu betrachten sind, wenn elektrische/elektronische/programmierbare elektronische Systeme (E/E/PES) zur Ausführung von Sicherheitsfunktionen eingesetzt werden. Ein Hauptziel dieser Norm ist es, für ein bestimmtes Anwendungsgebiet die Entwicklung einer entsprechenden Internationalen Norm durch das jeweils verantwortliche Komitee zu ermöglichen. Dies wird es erlauben, alle wichtigen Einflussgrößen dieses Anwendungsgebietes vollständig zu berücksichtigen und damit dessen besonderen Erfordernissen nachzukommen. Ein zweites Ziel dieser Norm ist es, die Entwicklung eines elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) sicherheitsbezogenen Systems, für dessen Anwendungsgebiet noch keine Internationale Norm besteht, zu ermöglichen.“

Der CENELEC-Bericht ROBT-004, der auf der 103. Sitzung des technischen Büros im März 2000 angenommen wurde, geht davon aus, dass einige IEC-Normen, die bereits veröffentlicht sind oder gerade erarbeitet werden, Implementierungen der IEC 61508 für ein bestimmtes Anwendungsgebiet darstellen, z. B.:

- IEC 61511, Functional safety – Safety instrumented systems for the process industry sector;
- IEC 62061, Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems;
- IEC 61513, Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.
- Für das Anwendungsgebiet des Eisenbahnwesens wurde ebenfalls eine Reihe Europäischer Normen erstellt (EN 50126, EN 50128 und prEN 50129).

ANMERKUNG EN 50126 und EN 50128 beruhen auf früheren Entwürfen der IEC 61508. prEN 50129 beruht auf den Grundsätzen der jetzt gültigen Fassung der IEC 61508.

Diese Aufzählung schließt nicht aus, dass weitere Implementierungen der IEC 61508 für bestimmte Anwendungsgebiete, die sich gerade in der Erarbeitung oder Veröffentlichung innerhalb IEC oder CENELEC befinden, erscheinen.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61508-7:2000 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

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

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

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

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

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

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

Einleitung

Systeme, die aus elektrischen und/oder elektronischen Bauteilen bestehen, werden seit vielen Jahren verwendet, um Sicherheitsfunktionen in vielen Anwendungsbereichen auszuführen. Auf Rechnern basierende Systeme (allgemein ausgedrückt programmierbare elektronische Systeme (PES)) 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 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 Bauteilen bestehen (elektrische/elektronische/programmierbare elektronische Systeme (E/E/PES)) 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 Schutzsystemen 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, die einzelne Teile einer Gesamtheit sind. Da sich diese Internationale Norm mit sicherheitsbezogenen elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) Systemen beschäftigt, kann sie einen Rahmen bereitstellen, innerhalb dessen sicherheitsbezogene Systeme, basierend auf anderen Technologien, betrachtet werden können.

Es ist berücksichtigt worden, dass eine große Vielfalt von E/E/PES-Anwendungen in vielfältigen Anwendungsbereichen vorliegt 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 ermöglicht.

Diese Internationale Norm:

- betrachtet alle relevanten sicherheitsbezogenen Phasen des Gesamtsystems der E/E/PES und des Software-Sicherheitslebenszyklus (zum Beispiel vom anfänglichen Konzept über Entwurf, Durchführung, Betrieb und Instandhaltung bis zur Außerbetriebnahme), wenn E/E/PES 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/PES befassen. Die Entwicklung anwendungsspezifischer Normen sollte innerhalb des Rahmens dieser Internationalen 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;
- liefert eine Methode für die Entwicklung der Spezifikation der Sicherheitsanforderungen, die notwendig ist, um die notwendige funktionale Sicherheit des sicherheitsbezogenen E/E/PE-Systems zu erreichen;
- verwendet Sicherheits-Integritätslevel für die Spezifikation der Zielvorgabe der Sicherheitsintegrität der Sicherheitsfunktionen, die in dem sicherheitsbezogenen E/E/PE-System implementiert werden;
- verwendet einen auf dem Risiko basierenden Lösungsansatz für die Festlegung der Anforderungen der Sicherheits-Integritätslevel;
- setzt numerische Ausfallgrenzwerte für sicherheitsbezogene E/E/PE-Systeme, die mit Sicherheits-Integritätsleveln verbunden sind;

- setzt eine untere Grenze des Ausfallgrenzwertes für eine gefahrbringende Ausfallart, der für ein einzelnes sicherheitsbezogenes E/E/PE-System beansprucht werden kann. Für sicherheitsbezogene E/E/PE-Systeme, die:
 - in der Betriebsart mit einer niedrigen Anforderungsrate betrieben werden, ist die untere Grenze der mittleren Wahrscheinlichkeit, die entworfene Funktion auf Anforderung nicht auszuführen, auf 10^{-5} festgelegt;
 - in der Betriebsart mit einer hohen oder ununterbrochenen Anforderungsrate betrieben werden, ist die untere Grenze der Wahrscheinlichkeit eines gefahrbringenden Ausfalls auf 10^{-9} pro Stunde festgelegt;

ANMERKUNG Ein einzelnes sicherheitsbezogenes E/E/PE-System bedeutet nicht auch notwendigerweise eine ein-kanalige Architektur.

- lässt einen weiten Bereich von Prinzipien, Techniken 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 gut 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.

Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme

Teil 7: Überblick der Verfahren und Maßnahmen

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.

ANMERKUNG 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 IEC 61508-1, IEC 61508-2, IEC 61508-3 und IEC 61508-4 sind Sicherheits-Grundnormen, dieser Status ist aber im Zusammenhang mit einfachen E/E/PE-sicherheitsbezogenen Systemen nicht anwendbar (siehe 3.4.4 der IEC 61508-4). 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 IEC 61508 ist ebenfalls zur Verwendung als eigenständige Norm vorgesehen.

Es steht in der Verantwortlichkeit eines Technischen Komitees, zur Vorbereitung und Erstellung eigener Festlegungen soweit wie 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.

ANMERKUNG 1 Die funktionale Sicherheit eines E/E/PE-sicherheitsbezogenen Systems kann nur erreicht werden, wenn alle zutreffenden Anforderungen erfüllt werden. Daher ist es wichtig, dass alle zutreffenden Anforderungen sorgfältig betrachtet und angemessenen in Bezug genommen werden.

ANMERKUNG 2 In den USA und Kanada können existierende nationale Sicherheitsnormen für den Bereich der Prozessindustrie auf der Basis der IEC 61508 (d. h. ANSI/ISA S84.01-1996) anstelle von IEC 61508 angewendet werden, bis die vorgeschlagene spezifische Umsetzung der IEC 61508 für die Prozessindustrie (d. h. IEC 61511) in den USA und Kanada als Internationale Norm veröffentlicht wurde.

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

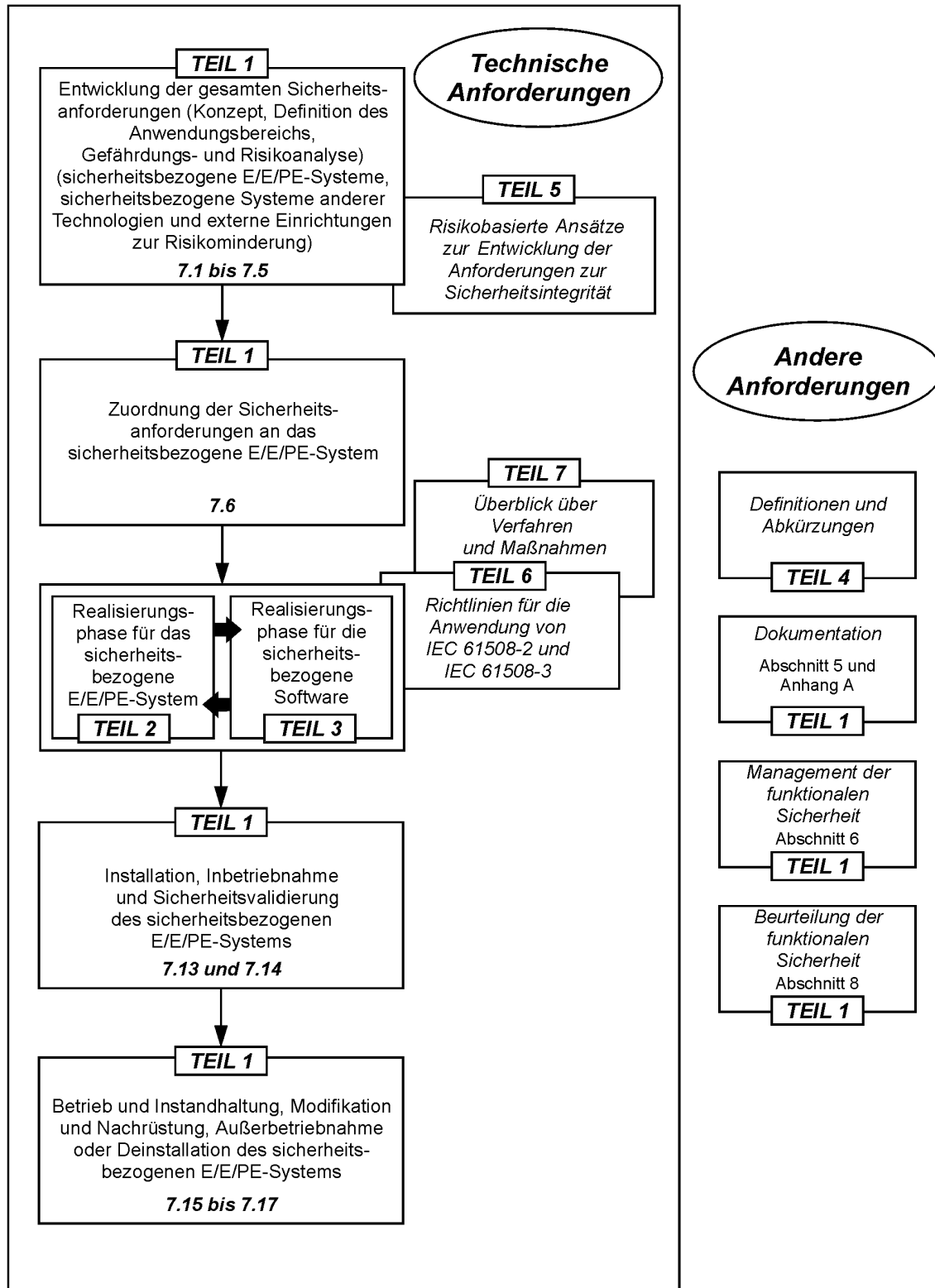


Bild 1 – Gesamtrahmen der Betrachtung der IEC 61508

2 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisung in diesem Text Bestandteil dieses Teils der IEC 61508 sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Vertragspartner, deren Vereinbarungen auf diesem Teil der IEC 61508 basieren, werden jedoch gebeten, die Möglichkeit zu prüfen, ob die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente angewendet werden können. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments. Mitglieder von ISO und IEC führen Verzeichnisse der gültigen Internationalen Normen.

IEC 61508-1:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 2: Requirements for electrical/electrical/programmable electronic safety-related system*¹⁾

IEC 61508-3:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations of terms*

IEC 61508-5:1998, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:2000, *Functional safety of electrical/electrical/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*¹⁾

IEC Guide 104:1997, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:1990 *Guidelines for the inclusion of safety aspects in standards*

3 Definitionen und Abkürzungen

Für die Anwendung dieses Teils der IEC 61508 finden die Definitionen und Abkürzungen aus **IEC 61508-4** Anwendung.

¹⁾ Wird veröffentlicht.

Anhang A (informativ)

Überblick über Verfahren und Maßnahmen für E/E/PES: 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.14 bis A.19 der IEC 61508-2 aufgeführt.

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

Beschreibung: Unter bestimmten Bedingungen können Ausfälle durch (zum Beispiel) die Verwendung von Informationen über das Zeitverhalten der EUC-Einrichtung erkannt werden. Wenn zum Beispiel ein Schalter, der Teil eines E/E/PE-sicherheitsbezogenen Systems ist und normalerweise durch die EUC-Einrichtung 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.15 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 Relaisspule nicht schließen. Daher kann die Überwachung des Schließens des Öffnerkontakts *b* bei Entregung der Relaisspule 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.2, A.9, A.14 und A.15 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 gefährlichen 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.16, A.17 und A.19 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.

Literaturhinweis: DIN V VDE 0801: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben (Principles for Computers in Safety-Related Systems), Beuth-Verlag, Berlin, 1990.

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.16 und A.19 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, der 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 Hardware mit sicherer Ausfallrichtung

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

Ziel: Überführung eines Systems in einen sicheren Zustand im Falle eines Ausfalls.

Beschreibung: In festverdrahteten Systemen wird eine Einheit als fehlersicher bezeichnet, wenn:

- eine definierte Auswahl von Fehlern zu einem sicheren Zustand führen wird und
- diese Fehler erkannt werden.

BEISPIEL Die definierte Auswahl von Fehlern könnte Stuck-at-, Stuck-open-Fehler, Kurzschlüsse innerhalb und zwischen Bauteilen und gerichtete Kurzschlüsse beinhalten.

Literaturhinweise:

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

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

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:

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

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

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-Einrichtung setzt den Betrieb nur dann weiter fort, wenn jeder Test erfolgreich gewesen ist.

Literaturhinweise:

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

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

A.2.7 Analogsignal-Überwachung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den **Tabellen A.3 und A.14 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

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 per Software: begrenzte Anzahl von Mustern (ein Kana)

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 per 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 des Watch-Dog-Prinzips 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.

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

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.

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:

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

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

A.4.2 Modifizierte Prüfsumme

ANMERKUNG Dieses Verfahren/Maßnahme ist in [Tabelle A.5 der IEC 61508-2](#) aufgeführt.

Ziel: Erkennung aller ungeradzahligen 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 bitseziellen 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:

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

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

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. Zwihehoff, 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.

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:

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.

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

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

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 Zellauswahl zu vergleichen. Die erste zu testende Zelle im ausge-

wählten 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:

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.

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

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 Ad-

ressierungsfehlern verwendet werden, indem die redundanten Bits durch die Verknüpfung des Datenwortes mit seiner Adresse berechnet werden.

Literaturhinweise:

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

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

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.14 und A.15 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 vergleichen. Die Testmusterinformation, der Testmusterempfang und die Testmustersauswertung müssen alle voneinander unabhängig sein. Die EUC-Einrichtung 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.16, A.17 und A.19 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-Einrichtung 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.

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.

MSR-Schutzeinrichtungen. Anforderungen und Maßnahmen zur gesicherten Funktion. DIN V 19251, Februar 1995.

A.6.5 Eingabevergleich/-entscheidung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den **Tabellen A.7 und A.14 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.

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.

MSR-Schutzeinrichtungen. Anforderungen und Maßnahmen zur gesicherten Funktion. DIN V 19251, Februar 1995.

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-Einrichtung 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 Abschaltoutine 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.16, A.17 und A.19 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.12 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.12 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.12 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.12 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.12 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.17 und A.19 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

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.11 der IEC 61508-2 aufgeführt.

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 E/E/PES. Bevor die Temperatur den spezifizierten Bereich verlässt, wird eine Notaktion ausgeführt.

A.10.2 Lüfterkontrolle

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.11 der IEC 61508-2 aufgeführt.

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

ANMERKUNG Dieses Verfahren/Maßnahme ist in Tabelle A.11 der IEC 61508-2 aufgeführt.

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

ANMERKUNG Dieses Verfahren/Maßnahme ist in **Tabelle A.11 der IEC 61508-2** aufgeführt.

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

ANMERKUNG Dieses Verfahren/Maßnahme ist in **Tabelle A.11 der IEC 61508-2** aufgeführt.

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.13 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 den **Tabellen A.13 und A.17 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.13, A.17 und A.19 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.

Literaturhinweise:

IEC 61000-5-2/TR3:1997, *Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 2: Earthing and cabling*.

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

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.

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

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.

A.11.4 Antivalente Signalübertragung

ANMERKUNG Dieses Verfahren/Maßnahme ist in den **Tabellen A.13 und A.17 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.14 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.14 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.15 der IEC 61508-2** aufgeführt.