DIN EN 61800-5-2 (VDE 0160-105-2)

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.

ICS 29.200

Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (IEC 61800-5-2:2007); Deutsche Fassung EN 61800-5-2:2007

Adjustable speed electrical power drive systems –
Part 5-2: Safety requirements –
Functional
(IEC 61800-5-2:2007);
German version EN 61800-5-2:2007

Entraînements électriques de puissance à vitesse variable –
Partie 5-2: Exigences de sécurité –
Fonctionnalité
(CEI 61800-5-2:2007);
Version allemande EN 61800-5-2:2007

Gesamtumfang 73 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin

Preisgr. 42 K
VDE-Vertr.-Nr. 0160015

Beginn der Gültigkeit

Die von CENELEC am 2007-10-01 angenommene EN 61800-5-2 gilt als DIN-Norm ab 2008-04-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61800-5-2 (VDE 0160-105-2):2005-12.

Für diese Norm ist das nationale Arbeitsgremium K 226 „Ausrüstung von Starkstromgeräten und -anlagen mit elektronischen Betriebsmitteln“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 22G „Adjustable speed electric drive systems incorporating semiconductor power converters“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (maintenance result date) unverändert bleiben soll, das auf der IEC-Website unter „http://webstore.iec.ch“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation
– bestätigt,
– zurückgezogen,
– durch eine Folgeausgabe ersetzt oder
– geändert.

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
EN 60204-1	IEC 60204-1	DIN EN 60204-1 (VDE 0113-1)	VDE 0113-1
EN 60529:1991 + A1:2000	IEC 60529:1989 + A1:1999	DIN EN 60529 (VDE 0470-1):2000-09	VDE 0470-1
EN 60664-1:2003	IEC 60664-1:1992 + A1:2000 + A2:2002	DIN EN 60664-1 (VDE 0110-1):2003-11	VDE 0110-1
EN 60664-3:2003	IEC 60664-3:2003	DIN EN 60664-3 (VDE 0110-1):2003-09	VDE 0110-3
–	IEC 61508 (Reihe)	–	–

Tabelle NA.1 *(fortgesetzt)*

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61508-4:2001	IEC 61508-4:1998 + Corr.:1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4
EN 61508-1:2001	IEC 61508-1:1998 + Corr.:1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803-2):2002-12	VDE 0803-2
EN 61508-3:2001	IEC 61508-3:1998 + Corr.:1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-5	IEC 61508-5	DIN EN 61508-5 (VDE 0803-5)	VDE 0803-5
EN 61508-6:2001	IEC 61508-6:2000	DIN EN 61508-6 (VDE 0803-6):2003-06	VDE 0803-6
EN 61508-7:2001	IEC 61508-7:2000	DIN EN 61508-7 (VDE 0803-7):2003-06	VDE 0803-7
–	IEC 61513	DIN IEC 61513 (VDE 0491-2)	VDE 0491-2
EN 61558-1:2005	IEC 61558-1:2005	DIN EN 61558-1 (VDE 0570-1):2006-07	VDE 0570-1
EN 61800-1	IEC 61800-1	DIN EN 61800-1 (VDE 0160-101)	VDE 0160-101
EN 61800-2	IEC 61800-2	DIN EN 61800-2 (VDE 0160-102)	VDE 0160-102
EN 61800-3	IEC 61800-3	DIN EN 61800-3 (VDE 0160-103)	VDE 0160-103
EN 61800-4	IEC 61800-4	DIN EN 61800-4 (VDE 0160-104)	VDE 0160-104
EN 61800-5-1:2003	IEC 61800-5-1:2003	DIN EN 61800-5-1 (VDE 0160-105):2003-09	VDE 0160-105
–	IEC 62061:2005 + Corr.:2005	–	–
–	IEC 62280 (Reihe)	–	–

Nationaler Anhang NB
(informativ)

Literaturhinweise

DIN EN 60204-1 (VDE 0113-1), *Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen*

DIN EN 60529 (VDE 0470-1):2000-09, *Schutzarten durch Gehäuse (IP-Code) (IEC 60529:1989 + A1:1999); Deutsche Fassung EN 60529:1991 + A1:2000*

DIN EN 60664-1 (VDE 0110-1):2003-11, *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen – Teil 1: Grundsätze, Anforderungen und Prüfungen (IEC 60664-1:1992 + A1:2000 + A2:2002); Deutsche Fassung EN 60664-1:2003*

DIN EN 60664-3 (VDE 0110-3):2003-09, *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen – Teil 3: Anwendung von Beschichtungen, Eingießen oder Vergießen zum Schutz gegen Verschmutzung (IEC 60664-3:2003); Deutsche Fassung EN 60664-3:2003*

DIN EN 61508-1 (VDE 0803-1):2002-11, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-1:2001*

DIN EN 61508-4 (VDE 0803-4):2002-11, *Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN* 61508-4*:2001*

DIN EN 61508-2 (VDE 0803-2):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508- 2:2000); Deutsche Fassung EN 61508-2:2001*

DIN EN 61508-3 (VDE 0803-3):2002-12, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-3:2001*

DIN EN 61508-5 (VDE 0803-5), *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 0803-6):2003-06, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2000); Deutsche Fassung EN 61508-6:2001*

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

DIN EN 61558-1 (VDE 0570-1):2006-07, *Sicherheit von Transformatoren, Netzgeräten, Drosseln und dergleichen – Teil 1: Allgemeine Anforderungen und Prüfungen*

DIN EN 61800-1 (VDE 0160-101), *Drehzahlveränderbare elektrische Antriebe – Teil 1: Allgemeine Anforderungen – Festlegungen für die Bemessung von Niederspannungs-Gleichstrom-Antriebssystemen*

DIN EN 61800-2 (VDE 0160-102), *Drehzahlveränderbare elektrische Antriebe – Teil 2: Allgemeine Anforderungen – Festlegungen für die Bemessung von Niederspannungs-Wechselstrom-Antriebssystemen mit einstellbarer Frequenz*

DIN EN 61800-3 (VDE 0160-103), *Drehzahlveränderbare elektrische Antriebe – Teil 3: EMV-Anforderungen einschließlich spezieller Prüfverfahren*

DIN EN 61800-4 (VDE 0160-104), *Drehzahlveränderbare elektrische Antriebe – Teil 4: Allgemeine Anforderungen – Festlegungen für die Bemessung von Wechselstrom-Antriebssystemen über 1 000 V AC und höchstens 35 kV*

DIN EN 61800-5-1 (VDE 0160-105):2003-09, *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-1: Anforderungen an die Sicherheit – Elektrische, thermische und energetische Anforderungen (IEC 61800-5-1:2003-02); Deutsche Fassung EN 61800-5-1:2003*

DIN IEC 61513, *Kernkraftwerk – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen*

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 61800-5-2

Oktober 2007

ICS 29.200; 13.110

Deutsche Fassung

Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit

(IEC 61800-5-2:2007)

Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional
(IEC 61800-5-2:2007)

Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnalité
(CEI 61800-5-2:2007)

Diese Europäische Norm wurde von CENELEC am 2007-10-01 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, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

Ref. Nr. EN 61800-5-2:2007 D

Vorwort

Der Text des Schriftstücks 22G/179/FDIS, zukünftige 1. Ausgabe von IEC 61800-5-2, ausgearbeitet von dem SC 22G „Adjustable speed electric drive systems incorporating semiconductor power converters“ des IEC/TC 22 „Power electronic systems and equipment“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2007-10-01 als EN 61800-5-2 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): 2008-07-01

– spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2010-10-01

Diese Europäische Norm wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde. Diese Europäische Norm deckt grundlegende Anforderungen einer EG-Richtlinie bzw. von EG-Richtlinien ab. Siehe Anhang ZZ.

Die Anhänge ZA und ZZ wurden von CENELEC hinzugefügt.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61800-5-2:2007 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 60300-3-1	ANMERKUNG	Harmonisiert als EN 60300-3-1:2004 (nicht modifiziert).
IEC 60664-1	ANMERKUNG	Harmonisiert als EN 60664-1:2003 (nicht modifiziert).
IEC 60664-3	ANMERKUNG	Harmonisiert als EN 60664-3:2003 (nicht modifiziert).
IEC 61025	ANMERKUNG	Harmonisiert als EN 61025:2007 (nicht modifiziert).
IEC 61078	ANMERKUNG	Harmonisiert als EN 61078:2006 (nicht modifiziert).
IEC 61165	ANMERKUNG	Harmonisiert als EN 61165:2006 (nicht modifiziert).
IEC 61508-4	ANMERKUNG	Harmonisiert als EN 61508-4:2001 (nicht modifiziert).
IEC 61511	ANMERKUNG	Harmonisiert in der Reihe EN 61511 (nicht modifiziert).
IEC 61511-1	ANMERKUNG	Harmonisiert als EN 61511-1:2004 (nicht modifiziert).
IEC 61558	ANMERKUNG	Harmonisiert in der Reihe EN 61558 (teilweise modifiziert).
IEC 61558-1	ANMERKUNG	Harmonisiert als EN 61558-1:2005 (nicht modifiziert).
IEC 62061	ANMERKUNG	Harmonisiert als EN 62061:2005 (nicht modifiziert).
ISO 13849-1	ANMERKUNG	Harmonisiert als EN ISO 13849-1:2006 (nicht modifiziert).
ISO 13849-2	ANMERKUNG	Harmonisiert als EN ISO 13849-2:2003 (nicht modifiziert).

Inhalt

Seite

Vorwort ... 2
Einleitung ... 6
1 Anwendungsbereich ... 7
2 Normative Verweisungen ... 8
3 Begriffe ... 9
4 Festgelegte *Sicherheitsfunktionen* ... 14
4.1 Allgemeines ... 14
4.2 *Sicherheitsfunktionen* ... 14
4.2.1 Grenzwerte ... 14
4.2.2 Stoppfunktionen ... 15
4.2.3 Andere *Sicherheitsfunktionen* ... 16
5 Management der *funktionalen Sicherheit* ... 17
5.1 Ziel ... 17
5.2 Sicherheitslebenszyklus eines *PDS(SR)* ... 17
5.3 Planung der *funktionalen Sicherheit* ... 18
5.4 *Spezifikation der Sicherheitsanforderungen* (SRS) für ein *PDS(SR)* ... 20
5.4.1 Allgemeines ... 20
5.4.2 Spezifikation der Anforderungen an die *Sicherheitsfunktionen* ... 20
5.4.3 Spezifikation der Anforderungen zur *Sicherheitsintegrität* ... 21
6 Anforderungen an Entwurf und Entwicklung eines *PDS(SR)* ... 21
6.1 Allgemeine Anforderungen ... 21
6.1.1 Wechsel des Betriebszustandes ... 21
6.1.2 Normen ... 22
6.1.3 Realisierung ... 22
6.1.4 *Sicherheitsintegrität* und Fehlererkennung ... 22
6.1.5 *Sicherheitsfunktionen* und nicht sicherheitsbezogene Funktionen ... 22
6.1.6 Anzuwendender *SIL* ... 22
6.1.7 Anforderungen an die Software ... 22
6.1.8 Überprüfung der Anforderungen ... 23
6.1.9 Dokumentation von Entwurf und Entwicklung ... 23
6.2 Anforderungen an den *PDS(SR)*-Entwurf ... 23
6.2.1 Anforderungen an die Wahrscheinlichkeit von gefahrbringenden zufälligen Hardwareausfällen je Stunde (PFH) ... 23
6.2.2 Strukturelle Einschränkungen ... 25
6.2.3 Abschätzung des *Anteils sicherer Ausfälle (SFF)* ... 27
6.2.4 Anforderungen an die systematische *Sicherheitsintegrität* eines *PDS(SR)* und von *PDS(SR)-Teilsystemen* ... 28
6.2.5 Anforderungen an die elektromagnetische Störfestigkeit eines *PDS(SR)* ... 30
6.3 Verhalten bei der Erkennung von Fehlern ... 31

Seite

6.3.1 Fehlererkennung ... 31
6.3.2 Fehlertoleranz größer Null ... 31
6.3.3 Fehlertoleranz von Null ... 31
6.4 Zusätzliche Anforderungen an die Datenkommunikation ... 31
6.5 Anforderungen an Integration und Prüfung des *PDS(SR)* ... 32
6.5.1 Integration der Hardware ... 32
6.5.2 Integration der Software ... 32
6.5.3 Modifikationen bei der Integration ... 33
6.5.4 Durchzuführende Integrationsprüfungen ... 33
6.5.5 Prüfprotokoll ... 33
7 Anwenderdokumentation ... 33
7.1 Informationen und Anweisungen für eine sichere Anwendung eines *PDS(SR)* ... 33
8 *Verifikation* und *Validierung* ... 35
8.1 Allgemeines ... 35
8.2 *Verifikation* ... 35
8.3 *Validierung* ... 35
8.4 Dokumentation ... 35
9 Prüfanforderungen ... 35
9.1 Prüfplanung ... 35
9.2 Prüfdokumentation ... 36
10 Modifikation ... 36
10.1 Ziel ... 36
10.2 Anforderungen ... 36
10.2.1 Anforderungen an die Modifikation ... 36
10.2.2 Einflussanalyse ... 36
10.2.3 Berechtigung ... 37
10.2.4 Dokumentation ... 37

Anhang A (informativ) Aufgabenablaufplan ... 38
Anhang B (informativ) Beispiel für die Bestimmung der *PFH* ... 42
Anhang C (informativ) Verfügbare Datenbanken für Ausfallraten ... 53
Anhang D (informativ) Fehlerlisten und Fehlerausschlüsse ... 55
Literaturhinweise ... 65
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen ... 67
Anhang ZZ (informativ) Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien ... 69
Anhang ZZA (informativ) Zusammenhang mit grundlegenden Anforderungen von Richtlinie 98/37/EG ... 69
Anhang ZZB (informativ) Zusammenhang mit grundlegenden Anforderungen von Richtlinie 2006/42/EG ... 69

Seite

Bild 1 – Funktionselemente eines *PDS(SR)* ... 8
Bild 2 – Entwicklungslebenszyklus eines *PDS(SR)* ... 18
Bild 3 – Architekturen der Datenkommunikation: a) Weißer Kanal, b) Schwarzer Kanal ... 32
Bild B.1 – Beispiel-*PDS(SR)* ... 42
Bild B.2 – *Teilsysteme* des *PDS(SR)* ... 43
Bild B.3 – Funktionsblöcke des *Teilsystems* A/B ... 44
Bild B.4 – Zuverlässigkeitsmodell (Markov) des Teilsystems A/B ... 47
Bild B.5 – Funktionsblöcke des *Teilsystems* PS/VM ... 49
Bild B.6 – Zuverlässigkeitsmodell (Markov) des Teilsystems PS/VM ... 51

Tabelle 1 – Alphabetisches Verzeichnis der Begriffe ... 9
Tabelle 2 – *Sicherheits-Integritätslevel*: Ausfallgrenzwerte für eine *Sicherheitsfunktion* eines *PDS(SR)* ... 23
Tabelle 3 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen der Architektur für sicherheitsbezogene *Teilsysteme* des Typs A ... 27
Tabelle 4 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen der Architektur für sicherheitsbezogene *Teilsysteme* des Typs B ... 27
Tabelle B.1 – Bestimmung des *DC*-Faktors des *Teilsystems* A/B ... 46
Tabelle B.2 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* A/B ... 49
Tabelle B.3 – Bestimmung des *DC*-Faktors des *Teilsystems* PS/VM ... 50
Tabelle B.4 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* PS/VM ... 52
Tabelle D.1 – Leiter/Kabel ... 56
Tabelle D.2 – Leiterplatten/Baugruppen ... 56
Tabelle D.3 – Reihenklemme ... 57
Tabelle D.4 – Mehrpoliger Steckverbinder ... 57
Tabelle D.5 – Elektromagnetische Bauelemente (z. B. Relais, Schaltrelais) ... 58
Tabelle D.6 – Transformatoren ... 58
Tabelle D.7 – Induktivitäten ... 59
Tabelle D.8 – Widerstände ... 59
Tabelle D.9 – Widerstandsnetzwerke ... 59
Tabelle D.10 – Potentiometer ... 60
Tabelle D.11 – Kondensatoren ... 60
Tabelle D.12 – Diskrete Halbleiter (z. B. Dioden, Zener-Dioden, Transistoren, Triacs, GTO-Thyristoren, IGBTs, Spannungsregler, Schwingquarze, Fototransistoren, Leuchtdioden (LEDs)) ... 60
Tabelle D.13 – Optokoppler ... 61
Tabelle D.14 – Nicht programmierbare integrierte Schaltkreise ... 61
Tabelle D.15 – Programmierbare und/oder komplexe integrierte Schaltkreise ... 62
Tabelle D.16 – Bewegungs- und Lagesensoren ... 62

Einleitung

Infolge der Automatisierung sowie der Forderung nach einer erhöhten Produktivität und einer Verringerung der Eingriffe durch Bedienpersonal spielen Steuerungssysteme für Maschinen und Betriebsanlagen eine immer bedeutendere Rolle für die allgemeine Sicherheit. Diese Steuerungssysteme werden zunehmend aus komplexen elektrischen/elektronischen/programmierbaren elektronischen Geräten und Systemen aufgebaut.

Führend unter diesen Geräten und Systemen sind elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl (PDS), die für einen Einsatz in sicherheitsbezogenen Anwendungen (*PDS(SR)*) geeignet sind.

Beispiele für industrielle Anwendungen sind:

– Werkzeugmaschinen, Roboter, Fertigungsprüfeinrichtungen, Prüfplätze;
– Papiermaschinen, Textilmaschinen, Kalander in der Gummiindustrie;
– Fertigungsstraßen bei der Produktion von Kunststoffen, Chemikalien oder Metallen, Walzwerke;
– Zerkleinerungsmaschinen in der Zementindustrie, Zementöfen, Mischer, Zentrifugen, Extrusionsmaschinen;
– Bohrmaschinen;
– Förderanlagen, Beschickungsmaschinen, Hebevorrichtungen (Krane, Portalkrane usw.);
– Pumpen, Gebläse usw.

Die vorliegende Norm kann von Entwicklern auch als Referenzdokument für *PDS(SR)* in anderen Anwendungen benutzt werden.

Anwender dieser Norm sollten sich bewusst sein, dass sich gegenwärtig einige Normen des Typs C für Maschinen auf ISO 13849-1 für sicherheitsbezogene Steuerungssysteme beziehen. In diesem Fall dürfen von Herstellern von *PDS(SR)* weitere Informationen gefordert werden (z. B. Kategorie und/oder Performance Level), um die Integration eines *PDS(SR)* in sicherheitsbezogene Steuerungssysteme solcher Maschinen zu erleichtern.

ANMERKUNG „Normen des Typs C“ sind in ISO 12100-1 als Normen für die Sicherheit von Maschinen definiert, die genaue Sicherheitsanforderungen für bestimmte Maschinen oder Gruppen von Maschinen behandeln.

In früheren Zeiten gab es aufgrund fehlender Normen Widerstand gegen den Einsatz elektronischer Geräte und Systeme – vor allem gegen programmierbare elektronische Geräte und Systeme – in sicherheitsbezogenen Funktionen, weil Unsicherheit hinsichtlich der sicherheitsbezogenen Leistungsfähigkeit dieser Technik bestand.

Es gibt viele Situationen, in denen Steuerungssysteme mit einem *PDS(SR)* beispielsweise als Teil von Sicherheitsmaßnahmen zur Risikominderung eingesetzt werden. Ein typischer Fall ist die Verriegelung einer Schutzvorrichtung zum Fernhalten von Personen von Gefahren, bei der ein Zugang zur Gefahrenzone nur möglich ist, wenn rotierende Teile einen sicheren Zustand erreicht haben. Dieser Teil von IEC 61800 legt eine Methode fest, mit der der Beitrag eines *PDS(SR)* zu bestimmten *Sicherheitsfunktion*en ermittelt werden kann und die eine geeignete Entwicklung des *PDS(SR)* ermöglicht und den Nachweis, dass diese die geforderte Leistungsfähigkeit erfüllt.

Es werden Wege zur Abstimmung der sicherheitsbezogenen Leistungsfähigkeit des *PDS(SR)* auf die vorgesehene Risikominderung unter Berücksichtigung der Wahrscheinlichkeiten und Folgen der zufälligen oder systematischen Fehler des *PDS(SR)* angegeben.

1 Anwendungsbereich

Dieser Teil von IEC 61800 legt Anforderungen fest und gibt Empfehlungen für den Entwurf und die Entwicklung, die Integration und die *Validierung* von *PDS(SR)* hinsichtlich ihrer funktionalen Sicherheit. Er gilt für elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl, die in den anderen Teilen der Normenreihe IEC 61800 behandelt werden.

ANMERKUNG 1 Der Begriff „Integration“ bezieht sich auf das *PDS(SR)* selbst und nicht auf dessen Einbau in die sicherheitsbezogene Anwendung.

Diese internationale Norm gilt nur, wenn *funktionale Sicherheit* eines *PDS(SR)* beansprucht wird und das *PDS(SR)* in einer *Betriebsart* mit hoher oder kontinuierlicher Anforderungsrate (siehe 3.10) betrieben wird. Für *Betriebsarten* mit niedriger Anforderungsrate siehe IEC 61508.

Dieser Teil von IEC 61800 ist eine Produktnorm und legt sicherheitsbezogene Betrachtungen für *PDS(SR)* im Rahmen der Norm IEC 61508 dar und führt Anforderungen an *PDS(SR)* als *Teilsysteme* eines *sicherheitsbezogenen Systems* ein. Damit wird die Umsetzung der elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) Elemente eines *PDS(SR)* unter Berücksichtigung der sicherheitsbezogenen Leistungsfähigkeit der *Sicherheitsfunktion(en)* eines PDS ermöglicht.

Hersteller und Lieferanten von *PDS(SR)* können Anwendern (d. h. Integratoren von Steuerungssystemen, Entwicklern von Maschinen und Anlagen usw.) durch die Umsetzung der normativen Festlegungen dieses Teils von IEC 61800 die sicherheitsbezogene Leistungsfähigkeit ihrer Einrichtung nachweisen. Dies ermöglicht den Einbau eines *PDS(SR)* in ein sicherheitsbezogenes Steuerungssystem unter Anwendung der Grundsätze von IEC 61508, ihrer Implementierungen in spezifischen Bereichen (z. B. IEC 61511, IEC 61513, IEC 62061) oder von ISO 13849.

Bei Übereinstimmung mit diesem Teil von IEC 61800 werden alle Anforderungen von IEC 61508 erfüllt, die für ein *PDS(SR)* gefordert werden.

Dieser Teil von IEC 61800 legt keine Anforderungen fest für:

– die Gefahren- und Risikoanalyse für eine bestimmte Anwendung;
– die Angabe von *Sicherheitsfunktionen* für diese Anwendung;
– die Zuordnung von *SILs* zu diesen *Sicherheitsfunktionen*;
– das Antriebssystem mit Ausnahme der Schnittstellen;
– Sekundärgefahren (z. B. durch Ausfälle in einem Produktionsprozess);
– elektrische, thermische und energetische Sicherheitsbetrachtungen, die in IEC 61800-5-1 behandelt werden;
– das Herstellungsverfahren des *PDS(SR)*;
– die Gültigkeit von Signalen und Befehlen für das *PDS(SR)*.

ANMERKUNG 2 Die Anforderungen an die *funktionale Sicherheit* eines *PDS(SR)* hängen von der Anwendung ab und müssen als Teil der gesamten Risikobewertung der *Anlage* betrachtet werden. Wenn der Lieferant des *PDS(SR)* nicht auch für die angetriebene Einrichtung verantwortlich ist, trägt der Entwickler der *Anlage* die Verantwortung für die Risikobewertung und das Festlegen der funktionalen Anforderungen und der *Sicherheitsintegrität* des *PDS(SR)*.

ANMERKUNG 3 Obwohl böswillige Handlungen die *funktionale Sicherheit* des *PDS(SR)* beeinflussen können, werden in der vorliegenden Norm keine Sicherheitsaspekte (en.: security, hiermit sind die Aspekte außerhalb der *funktionalen Sicherheit* gemeint) behandelt.

Dieser Teil von IEC 61800 gilt nur für *PDS(SR)*, die *Sicherheitsfunktionen* bis *SIL* 3 ausführen.

Bild 1 zeigt die Funktionselemente eines *PDS(SR)*, die in diesem Teil von IEC 61800 behandelt werden.

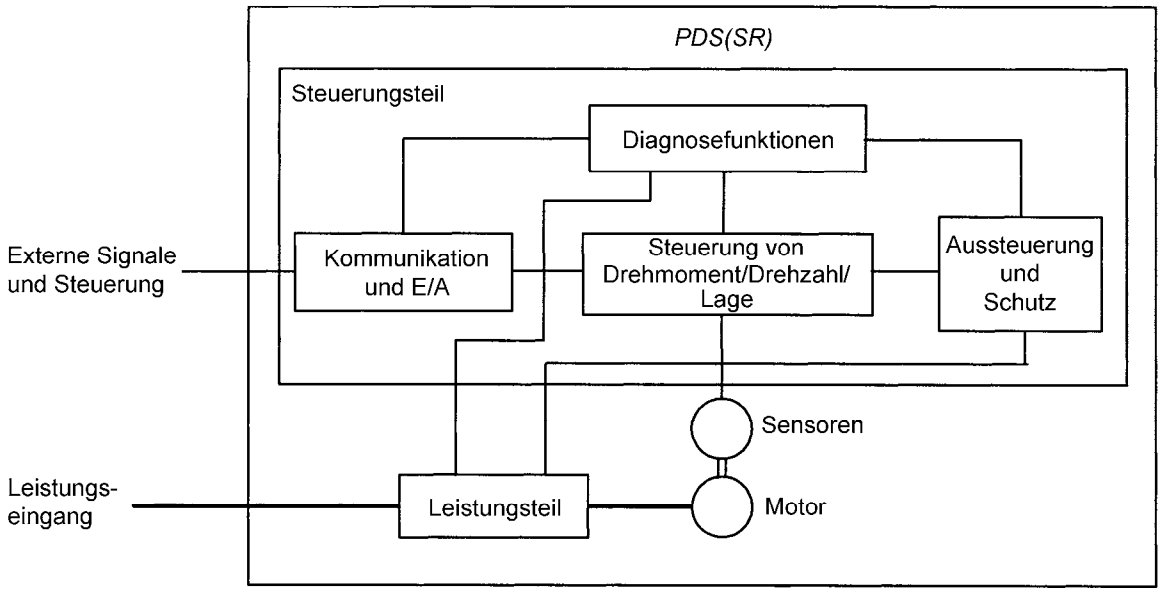


Bild 1 – Funktionselemente eines *PDS(SR)*

ANMERKUNG 4 Bild 1 zeigt eine eher logische Darstellung eines *PDS(SR)* als eine physikalische Beschreibung.

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).

ANMERKUNG 1 Das bedeutet nicht, dass Übereinstimmung mit allen Abschnitten des Referenzdokumentes bestehen muss, sondern dass das vorliegende Dokument eine Verweisung enthält, die ohne das Referenzdokument unverständlich ist.

ANWERKUNG 2 Verweisungen auf verschiedene Teile von IEC 61508 sind nicht datiert, außer wenn bestimmte Abschnitte angegeben sind.

IEC 60204-1, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61508 (alle Teile), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

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

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

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

IEC 61508-5, *Functional safety of electrical/electronic/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/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

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

IEC 61800-1, *Adjustable speed electrical power drive systems – Part 1: General requirements – Rating specifications for low voltage adjustable speed d.c. power drive systems*

IEC 61800-2, *Adjustable speed electrical power drive systems – Part 2: General requirements – Rating specifications for low voltage adjustable frequency a.c. power drive systems*

IEC 61800-3, *Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods*

IEC 61800-4, *Adjustable speed electrical power drive systems – Part 4: General requirements – Rating specifications for a.c. power drive systems above 1 000 V a.c. and not exceeding 35 kV*

IEC 61800-5-1:2003, *Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy*

IEC 62280 (alle Teile), *Railway applications – Communication, signalling and processing systems*

3 Begriffe

Für die Anwendung dieses Dokuments gelten folgende Begriffe.

ANMERKUNG 1 Tabelle 1 enthält ein alphabetisches Verzeichnis der Begriffe.

Tabelle 1 – Alphabetisches Verzeichnis der Begriffe

Begriff	Abschnitt	Begriff	Abschnitt
Ausfall infolge gemeinsamer Ursache	3.1	*sicherer Ausfall*	3.14
gefahrbringender Ausfall	3.2	*Anteil sicherer Ausfälle (SFF)*	3.15
Diagnosedeckungsgrad (DC)	3.3	*Sicherheitsfunktion(en) (eines PDS(SR))*	3.16
Diagnosetest	3.4	*Sicherheitsintegrität*	3.17
Fehlerreaktionsfunktion	3.5	*Sicherheits-Integritätslevel (SIL)*	3.18
funktionale Sicherheit	3.6	*sicherheitsbezogenes System*	3.19
Gefährdung	3.7	*Spezifikation der Sicherheitsanforderungen (SRS)*	3.20
Anlage	3.8	*SIL-Fähigkeit*	3.21
Gebrauchsdauer	3.9	*Teilsystem*	3.22
Betriebsart	3.10	*Versagen, systematischer Ausfall*	3.23
PDS(SR)	3.11	*systematische Sicherheitsintegrität*	3.24
PFH	3.12	*Validierung*	3.25
Proof-Test	3.13	*Verifikation*	3.26

ANMERKUNG 2 In der gesamten vorliegenden internationalen Norm sind die definierten Begriffe kursiv geschrieben.

3.1
Ausfall infolge gemeinsamer Ursache
(en: common cause failure)

Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitige Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen System verursachen und zu einem Ausfall der *Sicherheitsfunktion* führen

[IEC 61508-4:1998, Begriff 3.6.10]

3.2
gefahrbringender Ausfall
Ausfall mit dem Potential, das *sicherheitsbezogene System* in einen gefährlichen oder funktionsunfähigen Zustand zu versetzen

[IEC 61508-4:1998, Begriff 3.6.7]

3.3
Diagnosedeckungsgrad
DC (en: diagnostic coverage)
teilweise Verminderung der Wahrscheinlichkeit von gefahrbringenden Hardwareausfällen aufgrund der Anwendung automatischer *Diagnosetests*

[IEC 61508-4:1998, Begriff 3.8.6]

ANMERKUNG 1 Die Definition kann auch als das Verhältnis der Summe von erkannten *gefahrbringenden Ausfällen* λ_{DD} zur Summe aller *gefahrbringenden Ausfälle* λ_D angegeben werden: $DC = \Sigma\lambda_{DD}/\Sigma\lambda_D$.

ANMERKUNG 2 Der *Diagnosedeckungsgrad* kann für das gesamte System oder Teile eines *sicherheitsbezogenen Systems* gelten. Zum Beispiel kann der *Diagnosedeckungsgrad* für Sensoren und/oder Logiksysteme und/oder Stellglieder existieren.

3.4
Prüfung(en)
Prüfung(en) zur Erkennung von Fehlern oder Ausfällen, die zu einer festgelegten Ausgangsinformation oder zu einer Handlung führen, wenn ein Fehler oder Ausfall erkannt wird

3.5
Fehlerreaktionsfunktion
Funktion, die ausgelöst wird, wenn ein Fehler oder Ausfall im *PDS(SR)* erkannt wird, der einen Verlust der *Sicherheitsfunktion* zur Folge haben kann, und die dazu bestimmt ist, den sicheren Zustand der *Anlage* aufrechtzuerhalten oder das Entstehen gefahrbringender Zustände in der *Anlage* zu verhindern

3.6
funktionale Sicherheit
Teil der Gesamtsicherheit, bezogen auf die zu steuernde Einrichtung (en: equipment under control, EUC) und die EUC-Steuerung, der von der korrekten Funktion der E/E/PE- (elektrischen/elektronischen/programmierbaren elektronischen) *sicherheitsbezogenen Systeme*, der *sicherheitsbezogenen Systeme* anderer Technologien und externer Einrichtungen zur Risikominderung abhängt

[IEC 61508-4:1998, Begriff 3.1.9]

ANMERKUNG In der vorliegenden Norm werden nur diejenigen Aspekte in der Definition der *funktionalen Sicherheit* betrachtet, die von der korrekten Funktion des *PDS(SR)* abhängen.

3.7
Gefährdung
potentielle Schadensquelle

[ISO/IEC Guide 51:1999, Begriff 3.5]

ANMERKUNG 1 Der Begriff schließt *Gefährdung*en von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (z. B. durch Feuer und Explosion), und auch diejenigen, die eine Langzeitwirkung auf die Gesundheit einer Person haben (z. B. durch Freisetzung einer giftigen Substanz).

ANMERKUNG 2 IEC 61508-4:1998 (modifiziert) definiert eine Gefährdungssituation wie folgt: Umstände unter denen Personen, Eigentum oder die Umgebung einer oder mehreren *Gefährdungen* oder gefährlichen Ereignissen ausgesetzt sind.

3.8
Anlage
Ausrüstung oder Ausrüstungen, die mindestens das *PDS(SR)* und die angetriebene Ausrüstung enthalten

ANMERKUNG Der englische Begriff „installation“ wird in der vorliegenden internationalen Norm auch zur Bezeichnung der Installation eines *PDS(SR)* benutzt. In diesen Fällen wird der Begriff nicht kursiv geschrieben.

3.9
Gebrauchsdauer
festgelegte kumulierte Betriebsdauer des *PDS(SR)* während seiner Gesamtlebensdauer

3.10
Betriebsart
Verwendung, für die ein *sicherheitsbezogenes System* hinsichtlich seiner Anforderungsrate bestimmungsgemäß vorgesehen ist

[IEC 61508-4:1998, Begriff 3.5.12, modifiziert]

ANMERKUNG 1 In IEC 61508 werden zwei *Betriebsart*en betrachtet:

– ***Betriebsart* mit niedriger Anforderungsrate**: wobei die Anforderungsrate an ein *sicherheitsbezogenes System* nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Häufigkeit der *Proof-Tests* ist;

– ***Betriebsart* mit hoher Anforderungsrate oder kontinuierlicher Anforderung**: wobei die Anforderungsrate an ein *sicherheitsbezogenes System* mehr als einmal pro Jahr beträgt oder größer als die doppelte Häufigkeit der *Proof-Test*s ist.

Die *Betriebsart* mit niedriger Anforderungsrate wird für *PDS(SR)*-Anwendungen im Allgemeinen nicht in Betracht gezogen. Aus diesem Grund werden *PDS(SR)* in der vorliegenden Norm nur in der *Betriebsart* mit hoher Anforderungsrate oder mit kontinuierlicher Anforderung behandelt.

ANMERKUNG 2 *Betriebsart* mit Anforderungsrate bedeutet, dass eine *Sicherheitsfunktion* nur auf Verlangen (Anforderung) durchgeführt wird, um die *Anlage* in einen festgelegten Zustand zu überführen.

ANMERKUNG 3 *Betriebsart* mit kontinuierlicher Anforderung bedeutet, dass eine *Sicherheitsfunktion* dauernd ausgeführt wird, d. h., das *PDS(SR)* steuert die *Anlage* ununterbrochen und ein *(gefahrbringender) Ausfall* seiner Funktion kann zu einer *Gefährdung* führen.

3.11
PDS(SR)
elektrisches Leistungsantriebssystem mit einstellbarer Drehzahl, das für den Einsatz in sicherheitsbezogenen Anwendungen geeignet ist

3.12
PFH
Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls pro Stunde

ANMERKUNG In IEC 62061:2005 wird die Abkürzung PFH_D verwendet.

3.13
Proof-Test
wiederkehrende Prüfung zur Erkennung von Fehlern in einem *sicherheitsbezogenen System*, so dass nötigenfalls das System in einen „Wie-Neu“-Zustand gebracht oder so nah wie unter praktischen Gesichtspunkten möglich an diesen Zustand herangebracht werden kann

ANMERKUNG *Proof-Tests* werden normalerweise durchgeführt, um gefahrbringende Fehler aufzudecken, die durch *Diagnosetests* nicht erkannt werden. Die Wirksamkeit des *Proof-Tests* wird davon abhängig sein, wie nah das System an den „Wie-Neu“-Zustand gebracht wird. Damit der *Proof-Test* vollständig wirksam ist, ist es notwendig, alle gefahrbringenden Fehler zu erkennen. Obwohl dies in der Praxis für andere als einfache Systeme nicht leicht erreichbar ist, sollte dies aber das Ziel sein.

[IEC 61508-4:1998, Begriff 3.8.5, modifiziert]

3.14
sicherer Ausfall
Ausfall ohne das Potential, das *sicherheitsbezogene System* in einen gefährlichen oder funktionsunfähigen Zustand zu setzen

[IEC 61508-4:1998, Begriff 3.6.8]

3.15
Anteil sicherer Ausfälle
SFF (en: safe failure fraction)
Verhältnis der mittleren Rate *sicherer Ausfälle* zuzüglich erkannter *gefahrbringender Ausfälle* eines *PDS(SR)-Teilsystem*s zur gesamten mittleren Ausfallrate dieses *Teilsystems*

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$

ANMERKUNG Siehe IEC 61508-2:2000, Anhang C.

3.16
Sicherheitsfunktion(en) (eines PDS(SR))
Funktion(en) mit einer bestimmten sicherheitsbezogenen Leistungsfähigkeit, die insgesamt oder teilweise von einem *PDS(SR)* ausgeführt wird (werden) und mit der (denen) der sichere Zustand der *Anlage* aufrechterhalten oder das Entstehen gefahrbringender Zustände in der *Anlage* verhindert wird

3.17
Sicherheitsintegrität
Wahrscheinlichkeit, dass ein *PDS(SR)* eine geforderte *Sicherheitsfunktion* unter allen festgelegten Bedingungen anforderungsgemäß ausführt

ANMERKUNG 1 Je höher der *Sicherheits-Integritätslevel* des *PDS(SR)* ist, umso geringer ist die Wahrscheinlichkeit, dass das *PDS(SR)* die geforderte *Sicherheitsfunktion* nicht ausführen kann.

ANMERKUNG 2 Die *Sicherheitsintegrität* muss nicht für jede vom *PDS(SR)* ausgeführte *Sicherheitsfunktion* gleich sein.

[IEC 61508-4:1998, Begriff 3.5.2, modifiziert]

3.18
Sicherheits-Integritätslevel
SIL (en: safety integrity level)
diskrete Stufe (eine von vier möglichen) zur Spezifizierung der Anforderung für die *Sicherheitsintegrität* einer *Sicherheitsfunktion*, die einem *PDS(SR)* (ganz oder teilweise) zugeordnet ist

ANMERKUNG 1 *SIL* 4 hat die höchste Stufe der *Sicherheitsintegrität* und *SIL* 1 die niedrigste Stufe.

ANMERKUNG 2 *SIL* 4 wird in der vorliegenden Norm nicht betrachtet, da es für die Anforderungen an die Risikominderung, die gewöhnlich mit einem *PDS(SR)* verknüpft sind, nicht verwendet wird. Für Anforderungen, die für *SIL* 4 anwendbar sind, siehe IEC 61508.

[IEC 61508-4:1998, Begriff 3.5.6, modifiziert]

3.19
sicherheitsbezogenes System
System, dass sowohl

– die erforderlichen *Sicherheitsfunktionen* ausführt, die notwendig sind, um einen sicheren Zustand für die EUC zu erreichen oder aufrechtzuerhalten, als auch
– dazu vorgesehen ist, selbst oder mit anderen E/E/PE-*sicherheitsbezogenen Systemen*, *sicherheitsbezogenen Systemen* anderer Technologie oder externen Einrichtungen zur Risikominderung die notwendige *Sicherheitsintegrität* für die geforderten *Sicherheitsfunktionen* zu erreichen

3.20
Spezifikation der Sicherheitsanforderungen
SRS (en: safety requirements specification)
Spezifikation, die alle Anforderungen der *Sicherheitsfunktionen* enthält, die vom *PDS(SR)* auszuführen sind

3.21
SIL-Fähigkeit
höchstes *SIL*, das durch den Entwurf eines *PDS(SR)* hinsichtlich der *systematischen Sicherheitsintegrität* und der strukturellen Einschränkungen für die *Sicherheitsintegrität* der Hardware als erreicht betrachtet werden kann

ANMERKUNG Jeder der bezeichneten *Sicherheitsfunktionen*, die ein *PDS(SR)* ausführen soll, kann eine andere *SIL-Fähigkeit* zugeordnet werden.

3.22
Teilsystem
Teil des Architektur-Entwurfs eines *sicherheitsbezogenen Systems* auf oberster Ebene, dessen Ausfall zu einem Ausfall einer *Sicherheitsfunktion* führt

ANMERKUNG 1 Ein *PDS(SR)* kann selbst ein *Teilsystem* sein oder aus einer Anzahl von einzelnen *Teilsystemen* aufgebaut sein, die nach dem Zusammenfügen die betrachtete *Sicherheitsfunktion* ausführen. Ein *Teilsystem* kann mehr als einen Kanal besitzen.

ANMERKUNG 2 Beispiele für *Teilsysteme* eines *PDS(SR)* sind Geber, Leistungsteil, Steuerungsteil (siehe Bild 1).

3.23
systematischer Ausfall
Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Veränderung des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betreibens, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann

ANMERKUNG Beispiele von Ursachen für *systematische Ausfälle* schließen menschliches Versagen ein:

– bei der *Spezifikation der Sicherheitsanforderungen*;
– beim Entwurf, der Herstellung, dem Einbau, dem Betrieb der Hardware;
– beim Entwurf, der Implementierung der Software.

[IEC 61508-4:1998, Begriff 3.6.6]

3.24
systematische Sicherheitsintegrität
Teil der *Sicherheitsintegrität* von *sicherheitsbezogenen Systemen*, der sich auf *systematische Ausfälle* mit gefahrbringender Ausfallart bezieht

[IEC 61508-4:1998, Begriff 3.5.4]

ANMERKUNG Die *systematische Sicherheitsintegrität* kann üblicherweise nicht quantifiziert werden.

3.25
Validierung
Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung erfüllt worden sind

[IEC 61508-4:1998, Begriff 3.8.2]

ANMERKUNG Die *Validierung* ist die Tätigkeit, die darlegt, dass das *PDS(SR)* vor und nach der Installation in jeder Hinsicht der Spezifikation der Sicherheitsanforderungen entspricht.

3.26
Verifikation
Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die Anforderungen erfüllt worden sind

[IEC 61508-4:1998, Begriff 3.8.1]

4 Festgelegte *Sicherheitsfunktionen*

4.1 Allgemeines

In diesem Abschnitt werden Funktionen eines *PDS(SR)* beschrieben, die vom *PDS(SR)*-Lieferanten als sicherheitsbezogen festgelegt sind. Die Auflistung der angegebenen *Sicherheitsfunktionen* wird nicht als vollständig betrachtet. In einigen Fällen können zum *PDS(SR)* weitere externe *sicherheitsbezogene Systeme* (z. B. eine mechanische Bremse) erforderlich sein, um den sicheren Zustand aufrechtzuerhalten, wenn die elektrische Energie abgeschaltet ist.

Die technischen Maßnahmen, die zur Umsetzung dieser Funktionen erforderlich sind, hängen von der *SIL-Fähigkeit* und der geforderten Wahrscheinlichkeit gefahrbringender Hardwareausfälle ab, die in der *Spezifikation der Sicherheitsanforderungen* angegeben ist. Die technischen Maßnahmen sind im Abschnitt 6 beschrieben.

Jede *Sicherheitsfunktion* kann eine sichere Signalgabe am Eingang und/oder Ausgang erfordern, damit die notwendige Kommunikation mit (oder die Aktivierung von) anderen Funktionen, *Teilsystemen* oder Systemen (die sicherheitsbezogen sein können oder nicht) erfolgen kann. Die Sicherheitsintegrität der Schnittstellen muss in die Festlegung des *SIL* der zugehörigen *Sicherheitsfunktion* aufgenommen werden.

Einige der *Sicherheitsfunktionen* führen nur Überwachungsaufgaben aus, andere eine sicherheitsbezogene Steuerung oder andere Handlungen. Deshalb muss unterschieden werden zwischen:

– einer Reaktion auf die Überschreitung von Grenzwerten (gilt nur für Überwachungsfunktionen):

  die Reaktionsfunktion, wenn eine Überschreitung von Grenzwerten während des bestimmungsgemäßen Betriebs der *Sicherheitsfunktion* erkannt wird, und

– einer *Fehlerreaktionsfunktion*:

  die Reaktionsfunktion, wenn durch Diagnose ein Fehler innerhalb der *Sicherheitsfunktion* erkannt wird.

Bei beiden Reaktionsfunktionen müssen die möglichen sicheren Zustände für die Anwendung berücksichtigt werden.

Bei der Auswahl der geeigneten Reaktionsfunktion muss in Betracht gezogen werden, dass Teile des *PDS(SR)* möglicherweise nicht funktionsfähig sind.

Anforderungen an den Zeitablauf für die Handlungen, die nach der Erkennung eines Fehlers erforderlich sind, sind in der *Spezifikation der Sicherheitsanforderungen* angegeben (siehe 5.4.2).

Die Bezeichnungen für die *Sicherheitsfunktionen* beinhalten das Wort „sicher“, um anzuzeigen, dass diese Funktionen aufgrund einer Einschätzung (d. h. einer Risikoanalyse) dieser bestimmten Anwendung in einer sicherheitsbezogenen Anwendung eingesetzt werden können und zu sicherheitsbezogenen Funktionen und deren Integrität führen, die vom *PDS(SR)* auszuführen sind.

4.2 *Sicherheitsfunktionen*

4.2.1 Grenzwerte

Wenn eine *Sicherheitsfunktion* auf einem Grenzwert (Grenzwerten) für einen oder mehrere Parameter beruht, muss (müssen) die höchste(n) Toleranz(en) für den (die) Grenzwert(e) festgelegt werden.

ANMERKUNG Bei der Festlegung von Grenzwerten sollte eine mögliche Überschreitung des Grenzwertes bei einer Übertretung berücksichtigt werden. Zum Beispiel sollte(n) bei der Festlegung des (der) Lagegrenzwerte(s) in 4.2.3.8 der (die) maximal zulässige(n) Nachlaufweg(e) berücksichtigt werden.

Eine bestimmte *Sicherheitsfunktion* kann einen oder mehrere festgelegte Grenzwerte besitzen, die während des Betriebs ausgewählt werden können.

4.2.2 Stoppfunktionen

4.2.2.1 Allgemeines

Für jeden Typ eines PDS stehen eine Vielzahl von Verfahren zum Stillsetzen zur Verfügung.

Die Steuerungsanforderungen für das Auslösen des Stopp-Vorgangs und die Aufrechterhaltung eines Haltebetriebs nach dem Erreichen des Stillstands sind anwendungsspezifisch. Um die gewünschten Stoppfunktionen zu realisieren, können einzelne Betätigungen von Hand und Verbindungen mit den Steuerkreisen erforderlich sein.

Jede besondere Anforderung an die Realisierung einer Stoppfunktion sollte vom Anlagenentwickler festgelegt werden. In der Praxis werden häufig folgende Beispiele für Stoppfunktionen eingesetzt.

4.2.2.2 Sicher abgeschaltetes Moment (Safe torque off, STO)

Dem Motor wird keine Energie zugeführt, die eine Drehung (oder bei einem Linearmotor eine Bewegung) verursachen kann. Das *PDS(SR)* liefert keine Energie an den Motor, die ein Drehmoment (oder bei einem Linearmotor eine Kraft) erzeugen kann.

ANMERKUNG 1 Diese *Sicherheitsfunktion* entspricht einem ungesteuerten Stillsetzen nach IEC 60204-1, Stopp-Kategorie 0.

ANMERKUNG 2 Diese *Sicherheitsfunktion* kann verwendet werden, wenn die Abschaltung der Energie zur Verhinderung eines unerwarteten Anlaufs erforderlich ist.

ANMERKUNG 3 Unter Umständen, bei denen äußere Einflüsse (z. B. Herabfallen hängender Lasten) vorliegen, können zur Verhinderung von *Gefährdungen* weitere Maßnahmen (z. B. mechanische Bremsen) erforderlich sein.

ANMERKUNG 4 Elektronische Einrichtungen und Schütze bilden keinen ausreichenden Schutz gegen elektrischen Schlag und es können zusätzliche Maßnahmen zur galvanischen Trennung erforderlich sein.

4.2.2.3 Sicherer Stopp 1 (Safe stop 1, SS1)

Das *PDS(SR)* führt eine dieser Funktionen aus:

a) entweder Auslösen und Steuern der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der STO-Funktion (siehe 4.2.2.2), wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

b) Auslösen und Überwachen der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

c) Auslösen der Motorverzögerung und nach einer anwendungsspezifischen Zeitverzögerung Auslösen der STO-Funktion.

ANMERKUNG Diese *Sicherheitsfunktion* entspricht einem gesteuerten Stillsetzen nach IEC 60204-1, Stopp-Kategorie 1.

4.2.2.4 Sicherer Stopp 2 (Safe stop 2, SS2)

Das *PDS(SR)* führt eine dieser Funktionen aus:

a) entweder Auslösen und Steuern der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der SOS-Funktion (siehe 4.2.3.1), wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

b) Auslösen und Überwachen der Größe der Motorverzögerung innerhalb festgelegter Grenzen und Auslösen der SOS-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt, oder

c) Auslösen der Motorverzögerung und nach einer anwendungsspezifischen Zeitverzögerung Auslösen der SOS-Funktion.

ANMERKUNG Diese *Sicherheitsfunktion* entspricht einem gesteuerten Stillsetzen nach IEC 60204-1, Stopp-Kategorie 2.

4.2.3 Andere *Sicherheitsfunktionen*

4.2.3.1 Sicherer Betriebshalt (Safe operating stop, SOS)

Die SOS-Funktion verhindert, dass der Motor um mehr als einen festgelegten Betrag von der Halteposition abweicht. Das *PDS(SR)* liefert dem Motor die Energie, die ermöglicht, dass er dem Angreifen äußerer Kräfte standhält.

ANMERKUNG Diese Beschreibung der Funktion eines Betriebshalts beruht auf der Ausführung eines *PDS(SR)* ohne äußere (z. B. mechanische) Bremsen.

4.2.3.2 Sicher begrenzte Beschleunigung (Safely-limited acceleration, SLA)

Die SLA-Funktion verhindert, dass der Motor die festgelegte Begrenzung der Beschleunigung überschreitet.

4.2.3.3 Sicherer Beschleunigungsbereich (Safe acceleration range, SAR)

Die SAR-Funktion hält die Motorbeschleunigung und/oder -abbremsung innerhalb festgelegter Grenzwerte.

4.2.3.4 Sicher begrenzte Geschwindigkeit (Safely-limited speed, SLS)

Die SLS-Funktion verhindert, dass der Motor die festgelegte Begrenzung der Geschwindigkeit überschreitet.

4.2.3.5 Sicherer Geschwindigkeitsbereich (Safe speed range, SSR)

Die SSR-Funktion hält die Motorgeschwindigkeit innerhalb festgelegter Grenzwerte.

4.2.3.6 Sicher begrenztes Moment (Safely-limited torque, SLT)

Die SLT-Funktion verhindert, dass der Motor das festgelegte Drehmoment (oder bei Anwendung eines Linearmotors die festgelegte Kraft) überschreitet.

4.2.3.7 Sicherer Momentenbereich (Safe torque range, STR)

Die STR-Funktion hält das Motordrehmoment (oder bei Anwendung eines Linearmotors die festgelegte Kraft) innerhalb festgelegter Grenzwerte.

4.2.3.8 Sicher begrenzte Position (Safely-limited position, SLP)

Die SLP-Funktion verhindert, dass die Motorwelle die festgelegte(n) Lagebegrenzung(en) überschreitet.

4.2.3.9 Sicher begrenztes Schrittmaß (Safely-limited increment, SLI)

Die SLI-Funktion verhindert, dass die Motorwelle die festgelegte Begrenzung eines Lageschrittmaßes überschreitet.

ANMERKUNG Bei dieser Funktion steuert das *PDS(SR)* die Schrittbewegungen eines Motors wie folgt:

– ein Eingangssignal (z. B. Start) löst eine Schrittbewegung mit einem festgelegten Maximalweg aus;

– nach dem Zurücklegen des Weges, der für dieses Schrittmaß erforderlich ist, wird der Motor angehalten und bleibt in diesem Zustand, wie für die Anwendung angemessen.

4.2.3.10 Sichere Bewegungsrichtung (Safe direction, SDI)

Die SDI-Funktion verhindert, dass sich die Motorwelle in die unbeabsichtigte Richtung bewegt.

4.2.3.11 Sichere Motortemperatur (Safe motor temperature, SMT)

Die SMT-Funktion verhindert, dass die Motortemperatur(en) (einen) festgelegte(n) obere(n) Grenzwert(e) überschreitet.

4.2.3.12 Sichere Bremsenansteuerung (Safe brake control, SBC)

Die SBC-Funktion liefert (ein) sichere(s) Ausgangssignal(e) zur Ansteuerung einer (von) externen Bremse(n).

4.2.3.13 Sicherer Nocken (Safe cam, SCA)

Die SCA-Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Lage der Motorwelle innerhalb eines festgelegten Bereiches ist.

4.2.3.14 Sichere Geschwindigkeitsüberwachung (Safe speed monitor, SSM)

Die SSM-Funktion liefert ein sicheres Ausgangssignal, um anzuzeigen, ob die Motordrehzahl unterhalb eines festgelegten Grenzwertes liegt.

5 Management der *funktionalen Sicherheit*

5.1 Ziel

In diesem Abschnitt sind die Managementaktivitäten und Informationen angegeben, die für den gesamten Entwicklungsprozess des *PDS(SR)* erforderlich sind, damit sichergestellt ist, dass die Ziele für die *funktionale Sicherheit* erfüllt werden.

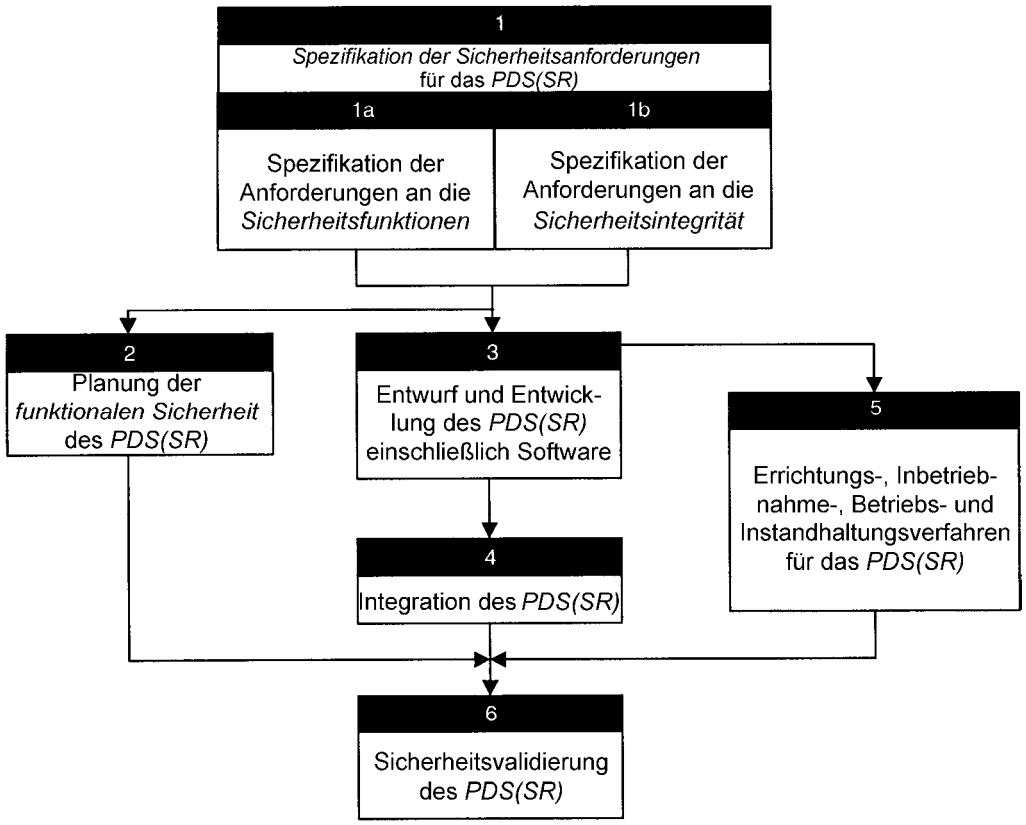
ANMERKUNG Dieser Abschnitt dient ausschließlich dem Erreichen der *funktionalen Sicherheit* des *PDS(SR)* und steht nicht im Zusammenhang mit allgemeinen Gesundheits- und Sicherheitsmaßnahmen für das Erreichen der Sicherheit am Arbeitsplatz.

5.2 Sicherheitslebenszyklus eines *PDS(SR)*

Bild 2 zeigt den Entwicklungslebenszyklus eines *PDS(SR)* mit Verweisungen auf die entsprechenden Abschnitte dieser Norm.

ANMERKUNG Dies entspricht der Realisierungsphase (Phase 9) des gesamten Sicherheitslebenszyklus nach IEC 61508-1.

Anhang A enthält diese Informationen in Form eines Aufgabenablaufplanes.



Phase 1 siehe 5.4	Phase 1a siehe 5.4.2	Phase 1b siehe 5.4.3	Phase 2 siehe 5.3
Phase 3 siehe Abschnitt 6	Phase 4 siehe 6.5	Phase 5 siehe Abschnitt 7	Phase 6 siehe 8.3

Bild 2 – Entwicklungslebenszyklus eines *PDS(SR)*

5.3 Planung der *funktionalen Sicherheit*

Es ist ein Plan für die *funktionale Sicherheit* aufzustellen und im Verlauf der gesamten Entwicklung des *PDS(SR)* gegebenenfalls zu aktualisieren. Der Plan muss die nach den Abschnitten 5 bis 10 notwendigen Aktivitäten und die Personen, Abteilungen oder Organisationen festlegen, die für die Ausführung dieser Aktivitäten verantwortlich sind. Der Plan für die *funktionale Sicherheit* kann als Abschnitt unter dem Titel „Plan für die *funktionale Sicherheit*“ in den Gesamtqualitätsplan für das *PDS(SR)* aufgenommen oder unter diesem Titel als Einzeldokument erstellt werden.

Der Plan für die *funktionale Sicherheit* muss im Einzelnen Folgendes berücksichtigen oder beinhalten, wie es für die Komplexität des *PDS(SR)* angemessen ist:

a) Aufstellung der *Spezifikation der Sicherheitsanforderungen* (siehe 5.4) einschließlich Faktoren wie:
   - Berücksichtigung der Anforderungen aus Richtlinien und Normen für bestimmte Zielanwendungen des *PDS(SR)*;
   - Auswahl der Verfahren, damit Fehler bei der Aufstellung der *Spezifikation der Sicherheitsanforderungen* vermieden werden;
   - verantwortliche Personen für die Erstellung und Pflege der *Spezifikation der Sicherheitsanforderungen*;
   - verantwortliche Personen für die Überprüfung der *Spezifikation der Sicherheitsanforderungen*;
   - Prozess der Änderung der *Spezifikation der Sicherheitsanforderungen* nach Beginn der Entwicklung;
b) Entwurf und Entwicklung der *Sicherheitsfunktion(en)* im *PDS(SR)* einschließlich (gegebenenfalls) Faktoren wie:

- Berücksichtigung von geltenden Richtlinien und Normen für die *funktionale Sicherheit* bei Entwurf und Entwicklung von Prozess- oder Maschinensteuerungen, deren Bestandteil das *PDS(SR)* ist;
- Auswahl der Verfahren für die Produktentwicklung und das Projektmanagement (siehe IEC 61508-7:2000, B.1.1);
- für Entwurf und Entwicklung verantwortliche Personen;
- Verfahren für die Projektdokumentation (siehe IEC 61508-7:2000, B.1.2);
- Anwendung strukturierter Entwurfstechniken (siehe IEC 61508-7:2000, B.3.2);
- Einsatz von Simulation oder anderer computergestützter Entwurfswerkzeuge;
- Verfahren der Entwurfsüberprüfung;
- Integrationstechniken und Funktionsprüfverfahren, Regressionstests und verantwortliche Personen;
- Management von Entwurfsänderungen (sowohl für Hardware als auch für Software);

c) Verifikationsplan für die *Sicherheitsfunktion(en)* einschließlich Faktoren wie:

- Auswahl der Verifikationsstrategien und -techniken;
- Auswahl der Verifikationsaktivitäten;
- für die *Verifikation* verantwortliche Personen;
- Auswahl und Einsatz der Prüfeinrichtungen;
- Auswertung der Verifikationsergebnisse, die sich aus der Verifikationseinrichtung und den Prüfungen ergeben;

d) Validierungsplan für die *Sicherheitsfunktion(en)* mit:

- den für die Validierungsprüfung verantwortlichen Personen;
- Angabe der entsprechenden *Betriebsarten* des *PDS(SR)*;
- der technischen Strategie der *Validierung*, z. B. analytische Verfahren oder statistische Prüfungen;
- Annahmekriterien;
- Handlungen, die bei Nichterfüllung der Annahmekriterien erfolgen müssen;

e) Plan für die Installation und die Inbetriebnahme mit (wenn anwendbar):

- besonderen Anweisungen für die Installation und deren Reihenfolge;
- für die Installation und Inbetriebnahme verantwortlichen Personen;
- Aktivitäten und Prüfungen bei der Inbetriebnahme bezogen auf die *funktionale Sicherheit*;
- Protokollierung von Inbetriebnahmeprüfungen und deren Ergebnisse;
- Verfahren für die Lösung von Prüfausfällen und -problemen;

f) Plan für eine sicherheitsbezogene Anwenderdokumentation mit:

- einer Liste wichtiger sicherheitsbezogener Informationen, die angegeben werden müssen;
- für die Anwenderdokumentation verantwortliche Personen;
- Überprüfungsverfahren zur Sicherstellung der Korrektheit der Dokumentation;

g) wenn eine Beurteilung gefordert wird (siehe IEC 61508-1:1998, Abschnitt 8), muss ein Beurteilungsplan für die *funktionale Sicherheit* zur Verfügung stehen mit:

- dem Umfang der Beurteilung der *funktionalen Sicherheit*;
- Personen, die die funktionale Beurteilung vornehmen;
- den Schritten, bei denen die Beurteilung der *funktionalen Sicherheit* vorzunehmen ist (z. B. nachdem die *Spezifikation der Sicherheitsanforderungen* erstellt wurde, nachdem das sicherheitsbezogene Steuerungssystem entworfen wurde);
- den Informationen, die als Ergebnis der Aktivitäten der Beurteilung der *funktionalen Sicherheit* angegeben werden müssen;
- den Betriebsmitteln, die zur Beurteilung der *funktionalen Sicherheit* erforderlich sind;
- dem Grad der Unabhängigkeit des Beurteilungteams;
- den Mitteln, mit denen die Beurteilung der *funktionalen Sicherheit* nach Modifikationen des *PDS(SR)* erneut durchgeführt werden muss.

5.4 *Spezifikation der Sicherheitsanforderungen* (SRS) für ein *PDS(SR)*

5.4.1 Allgemeines

Es ist eine *Spezifikation der Sicherheitsanforderungen* für ein *PDS(SR)* zu erstellen, die Folgendes enthalten muss:

– eine Spezifikation der Anforderungen an die *Sicherheitsfunktionen* (siehe 5.4.2) und

– eine Spezifikation der Anforderungen an die *Sicherheitsintegrität* (siehe 5.4.3).

Diese sind so zu verfassen, dass sie:

– deutlich;

– genau;

– eindeutig;

– durchführbar;

– verifizierbar;

– prüfbar;

– pflegbar sind.

Um Fehler bei der Erarbeitung dieser Spezifikationen zu vermeiden, sind geeignete Techniken und Maßnahmen anzuwenden (siehe IEC 61508-2:2000, Tabelle B.1).

5.4.2 Spezifikation der Anforderungen an die *Sicherheitsfunktionen*

Die Spezifikation der Anforderungen an die *Sicherheitsfunktionen* muss umfassende, genaue Anforderungen enthalten, die für den Entwurf und die Entwicklung des *PDS(SR)* ausreichend sind.

Die Spezifikation der Anforderungen an *Sicherheitsfunktionen* muss beschreiben:

a) alle auszuführenden *Sicherheitsfunktionen*;

b) alle möglichen Zustände des *PDS(SR)*, die zum Erreichen eines sicheren Zustands für die vorgesehene Anwendung verwendet werden können;

c) die *Betriebsarten* des *PDS(SR)* – z. B. Einstellung, Inbetriebnahme, Instandhaltung, bestimmungsgemäß vorgesehener Betrieb;

d) alle geforderten Arten des Verhaltens des *PDS(SR)*;

e) die Priorität derjenigen Funktionen, die gleichzeitig aktiv sind und miteinander im Widerspruch stehen können;

f) die erforderliche(n) Reaktion(en), wenn eine Verletzung der Grenzwerte beim ordnungsgemäßen Betrieb einer *Sicherheitsfunktion* erkannt wird (siehe 4.1);

g) die *Fehlerreaktionsfunktion(en)* (siehe 4.1 und 6.3);

h) die maximale Fehlerreaktionszeit, damit die entsprechende *Fehlerreaktionsfunktion* durchgeführt wird, bevor eine *Gefährdung* in der vorgesehenen Anwendung eintritt (nur erforderlich, wenn *Fehlererkennung* verwendet wird, um die *SIL-Fähigkeit* zu erreichen);

i) die maximale Antwortzeit jeder sicherheitsbezogenen Funktion (d. h. sowohl *Sicherheitsfunktionen* als auch *Fehlerreaktionsfunktionen* (siehe 6.3));

j) die Signifikanz aller Wechselwirkungen zwischen Hardware und Software – soweit zutreffend müssen alle geforderten Einschränkungen zwischen Hardware und Software angegeben und dokumentiert werden;

ANMERKUNG Wenn diese Wechselwirkungen vor dem Abschluss des Entwurfs nicht bekannt sind, können nur allgemeine Einschränkungen angegeben werden.

k) alle Mittel, über die der Bediener mit dem *PDS(SR)* interagiert und die die sicherheitsbezogenen Funktionen beeinflussen können (d. h. sowohl *Sicherheitsfunktionen* als auch *Fehlerreaktionsfunktionen*);

l) alle Schnittstellen zwischen dem *PDS(SR)* und einem anderen System (entweder direkt innerhalb oder außerhalb der *Anlage*).

5.4.3 Spezifikation der Anforderungen zur *Sicherheitsintegrität*

Die Spezifikation der Anforderungen zur *Sicherheitsintegrität* für ein *PDS(SR)* muss umfassen:

a) für jede sicherheitsbezogene Funktion (oder Gruppe gleichzeitig angewendeter *Sicherheitsfunktionen*) sowohl die *SIL-Fähigkeit* als auch die höchste Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls;

ANMERKUNG 1 Die *SIL-Fähigkeit* ist entscheidend, wenn das *PDS(SR)* als Komponente betrachtet wird, die eine *Sicherheitsfunktion* zusammen mit anderen Komponenten realisiert.

ANMERKUNG 2 Die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls des *PDS(SR)* muss in der Regel geringer sein als der Maximalwert, der dem *SIL* für die gesamte *Sicherheitsfunktion* entspricht. Dies ist erforderlich, um die Wahrscheinlichkeit *gefahrbringender Ausfälle* anderer beteiligter Komponenten mit aufnehmen zu können. Sie darf höher sein, wenn das *PDS(SR)* als Redundanz für andere Komponenten einer *Sicherheitsfunktion* benutzt wird.

ANMERKUNG 3 Wenn ein *PDS(SR)* eine *Sicherheitsfunktion* vollständig eigenständig ausführt, gibt die Spezifikation der Anforderungen zur *Sicherheitsintegrität* einen *SIL* an und nicht eine *SIL-Fähigkeit*.

ANMERKUNG 4 Wenn zur Ausführung von mehreren *Sicherheitsfunktionen* gemeinsame Hardware angewendet wird und die *Sicherheitsfunktionen* gleichzeitig benutzt werden, sollte die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls der gemeinsamen Hardware bei der Bestimmung der gesamten Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls nur einmal betrachtet werden.

ANMERKUNG 5 Wenn bei einem mehrachsigen *PDS(SR)* eine *Sicherheitsfunktion* für mehr als eine Achse gefordert wird, sollte die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls der gemeinsamen Hardware bei der Bestimmung der gesamten Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls nur einmal betrachtet werden.

b) die Extremwerte aller Umgebungsbedingungen (einschließlich elektromagnetischer Bedingungen), die möglicherweise bei Lagerung, Transport, Prüfung, Installation, Inbetriebnahme, Betrieb und Instandhaltung des *PDS(SR)* auftreten;

ANMERKUNG 6 Diese Informationen sind möglicherweise bereits berücksichtigt worden, um die Anforderungen von IEC 61800-1, IEC 61800-2 oder IEC 61800-4 zu erfüllen und sie müssen in diesem Fall nicht noch einmal dokumentiert werden.

c) alle Anforderungen an eine erhöhte elektromagnetische Störfestigkeit (siehe 6.2.5).

6 Anforderungen an Entwurf und Entwicklung eines *PDS(SR)*

6.1 Allgemeine Anforderungen

6.1.1 Wechsel des Betriebszustandes

Jeder Wechsel in einen Betriebszustand eines *PDS(SR)*, der zu einer gefahrbringenden Situation führen kann (z. B. durch einen unerwarteten Anlauf), darf nur durch eine beabsichtigte Aktion des Bedieners ausgelöst werden.

ANMERKUNG Beispielsweise sollte kein Ausfall eines *PDS(SR)* in einem Haltezustand zu einem unerwarteten Anlauf der Maschinen und/oder Anlagen führen.

6.1.2 Normen

Ein *PDS(SR)* muss nach IEC 61800-5-1 und gegebenenfalls anderen geltenden Normen der Normenreihe IEC 61800 entworfen und entwickelt werden.

6.1.3 Realisierung

Die Realisierung eines *PDS(SR)* muss nach seiner *Spezifikation der Sicherheitsanforderungen* erfolgen (siehe 5.4).

6.1.4 *Sicherheitsintegrität* und Fehlererkennung

Das *PDS(SR)* muss alle Punkte a) bis c) erfüllen:

a) die Anforderungen an die Hardware-*Sicherheitsintegrität* mit:
   - den strukturellen Einschränkungen für die Hardware-*Sicherheitsintegrität* (siehe 6.2.2) und
   - den Anforderungen an die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls je Stunde (siehe 6.2.1);

b) die Anforderungen an die systematische *Sicherheitsintegrität* mit:
   - den Anforderungen an die Fehlervermeidung (siehe 6.2.4.1) und den Anforderungen an die Beherrschung systematischer Fehler (siehe 6.2.4.2) oder
   - dem Nachweis dafür, dass verwendete Bauteile „betriebsbewährt“ sind. In diesem Fall müssen die Bauteile die entsprechenden Anforderungen von IEC 61508-2 erfüllen;

c) die Anforderungen an das Verhalten bei der Erkennung eines Fehlers (siehe 6.3).

6.1.5 *Sicherheitsfunktionen* und nicht sicherheitsbezogene Funktionen

Wenn ein *PDS(SR)* sowohl *Sicherheitsfunktionen* als auch nicht sicherheitsbezogene Funktionen ausführen muss, muss die gesamte Hardware und Software als sicherheitsbezogen behandelt werden, wenn nicht nachgewiesen werden kann, dass die Ausführung der *Sicherheitsfunktionen* und der nicht sicherheitsbezogenen Funktionen ausreichend unabhängig voneinander ist (d. h., dass der Ausfall einer nicht sicherheitsbezogenen Funktion keinen *gefahrbringenden Ausfall* der sicherheitsbezogenen Funktionen verursacht).

ANMERKUNG Eine ausreichende Unabhängigkeit kann angenommen werden, wenn nachgewiesen wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen nicht sicherheitsbezogenen und sicherheitsbezogenen Teilen im Vergleich zur Wahrscheinlichkeit eines *gefahrbringenden Ausfalls* für den höchsten *Sicherheits-Integritätslevel*, der mit den betreffenden *Sicherheitsfunktionen* verbunden ist, ausreichend gering ist.

6.1.6 Anzuwendender *SIL*

Die Anforderungen an die Hardware und die Software müssen mit dem *Sicherheits-Integritätslevel* der *Sicherheitsfunktion* mit dem höchsten *Sicherheits-Integritätslevel* bestimmt werden, wenn nicht nachgewiesen werden kann, dass die Ausführung der *Sicherheitsfunktionen* mit unterschiedlichen *Sicherheits-Integritätslevel* ausreichend unabhängig ist.

ANMERKUNG Eine ausreichende Unabhängigkeit kann angenommen werden, wenn nachgewiesen wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen Teilen, die *Sicherheitsfunktionen* unterschiedlicher Integritätslevel ausführen, im Vergleich zur Wahrscheinlichkeit eines *gefahrbringenden Ausfalls* für den höchsten *Sicherheits-Integritätslevel*, der mit den betreffenden *Sicherheitsfunktionen* verbunden ist, ausreichend gering ist.

6.1.7 Anforderungen an die Software

Wenn zur Ausführung einer *Sicherheitsfunktion* eines *PDS(SR)* mit einem bestimmten *SIL* oder einer bestimmten *SIL-Fähigkeit* (siehe 5.4.3) Software benutzt wird, muss diese Software nach den Anforderungen in IEC 61508-3 für diesen spezifischen *SIL* realisiert werden.

6.1.8 Überprüfung der Anforderungen

Die Anforderungen für die sicherheitsbezogene Hardware und Software müssen überprüft werden, um sicherzustellen, dass die Festlegungen ausreichend sind. In erster Linie muss Folgendes betrachtet werden:

a) *Sicherheitsfunktionen*;

b) Anforderungen an die *Sicherheitsintegrität*;

c) Geräte- und Bedienerschnittstellen.

6.1.9 Dokumentation von Entwurf und Entwicklung

Neben der Dokumentierung des Entwurfs und der Realisierung muss die *PDS(SR)*-Entwurfsdokumentation die Techniken und Maßnahmen angeben, die zum Erreichen des angestrebten *SIL* verwendet wurden (z. B. Ausfalleffektanalyse, Fehlerbaumanalyse).

6.2 Anforderungen an den *PDS(SR)*-Entwurf

6.2.1 Anforderungen an die Wahrscheinlichkeit von gefahrbringenden zufälligen Hardwareausfällen je Stunde (PFH)

6.2.1.1 Allgemeine Anforderungen

6.2.1.1.1 *PFH* für jede *Sicherheitsfunktion*

Die *PFH* jeder *Sicherheitsfunktion* (oder einer Gruppe von gleichzeitig verwendeten *Sicherheitsfunktionen*), die vom *PDS(SR)* auszuführen ist und die nach 6.2.1.1.2 und Anhang B ermittelt wird, muss gleich oder kleiner als der in der Spezifikation der Anforderungen an die *Sicherheitsintegrität* festgelegte Ausfallgrenzwert (siehe Tabelle 2) sein (siehe 5.4.3).

Der PFH-Wert, wie durch den *SIL* definiert, bezieht sich auf eine vollständige Sicherheitsfunktion. Wenn ein *PDS(SR)* nur einen Teil einer *Sicherheitsfunktion* in einem sicherheitsbezogenen Steuerungssystem ausführt, dann sollte die *PFH* des Antriebs ausreichend kleiner sein als der durch den *SIL* definierte Wert.

ANMERKUNG 1 Der Ausfallgrenzwert, der als *PFH* angegeben wird, wird durch den *SIL* der *Sicherheitsfunktion* bestimmt (siehe 61508-1:1998, Tabelle 3), wenn in der Spezifikation der Anforderungen an die *Sicherheitsintegrität* des *PDS(SR)* (siehe 5.4.3) für die *Sicherheitsfunktion* nicht gefordert wird, dass ein spezifischer Ausfallgrenzwert anstelle eines bestimmten *SIL* zu erfüllen ist.

Tabelle 2 – *Sicherheits-Integritätslevel*: Ausfallgrenzwerte für eine *Sicherheitsfunktion* eines *PDS(SR)*

Sicherheits-Integritätslevel	***PFH***
3	$\geq 10^{-8}$ bis $<10^{-7}$
2	$\geq 10^{-7}$ bis $<10^{-6}$
1	$\geq 10^{-6}$ bis $<10^{-5}$
ANMERKUNG Die *PFH* wird manchmal als Häufigkeit *gefahrbringender Ausfälle* oder gefahrbringende Ausfallrate mit der Einheit *gefahrbringende Ausfälle* je Stunde bezeichnet.	

Die *PFH* muss für jede *Sicherheitsfunktion* (oder jede Gruppe gleichzeitig verwendeter *Sicherheitsfunktionen*) des *PDS(SR)* ermittelt werden.

ANMERKUNG 2 Unterschiedliche *Sicherheitsfunktionen* können gemeinsame Komponenten und/oder eigene Komponenten besitzen, was zu unterschiedlichen *PFH* für jede *Sicherheitsfunktion* (oder jede Gruppe gleichzeitig verwendeter *Sicherheitsfunktionen*) führt.

ANMERKUNG 3 Es stehen eine Anzahl von Modellierungsverfahren zur Verfügung und das am besten geeignete Verfahren wird vom Analysten ausgewählt und hängt von den Umständen ab. Verfügbare Verfahren sind:

– Fehlerbaumanalyse (siehe IEC 61025);

– Markov-Modell (siehe IEC 61165);

– Zuverlässigkeits-Blockdiagramme (siehe IEC 61078).

Siehe auch IEC 60300-3-1.

ANMERKUNG 4 Bei der mittleren Dauer bis zur Wiederherstellung (siehe IEV 191-13-08), die im Zuverlässigkeitsmodell betrachtet wird, müssen das Diagnose-Testintervall, das *Proof-Test*-Intervall, die Reparaturdauer und jede andere Verzögerung vor der Wiederherstellung berücksichtigt werden.

ANMERKUNG 5 *Ausfälle infolge gemeinsamer Ursache* und infolge von Datenkommunikationsprozessen können durch andere Effekte als den tatsächlichen Ausfall der Hardware-Komponente verursacht werden (z. B. Decodierungsfehler). Diese Ausfälle werden jedoch für die Anwendung dieser Norm als zufällige Hardwareausfälle betrachtet. (Siehe IEC 61508-6:2000, Anhang D.)

ANMERKUNG 6 IEC 61508-6:2000, Anhang B, beschreibt einen vereinfachten Ansatz, der zur Ermittlung der Wahrscheinlichkeit eines *gefahrbringenden Ausfalls* einer *Sicherheitsfunktion* aufgrund zufälliger Hardwareausfälle benutzt werden kann, um zu ermitteln, ob eine Architektur den geforderten Ausfallgrenzwert einhält.

6.2.1.1.2 Abschätzung der *PFH*

Die *PFH* in Folge zufälliger Hardwareausfälle muss für jede *Sicherheitsfunktion* (oder jede Gruppe von gleichzeitig verwendeten *Sicherheitsfunktion*en), die vom *PDS(SR)* ausgeführt wird, nach IEC 61508-2:2000, Anhang A, unter Berücksichtigung von Folgendem abgeschätzt werden:

a) der Architektur des *PDS(SR)* in Bezug zur betrachteten Sicherheitsfunktion;

b) der geschätzten Ausfallrate jedes Teilsystems des *PDS(SR)* in allen Modi, die zu einem gefahrbringenden Ausfall des *PDS(SR)* führen, jedoch durch *Diagnosetests* erkannt werden;

c) der geschätzten Ausfallrate jedes Teilsystems des *PDS(SR)* in allen Modi, die zu einem gefahrbringenden Ausfall des *PDS(SR)* führen und welche durch Diagnosetests nicht erkannt werden;

d) der Anfälligkeit des *PDS(SR)* für *Ausfälle infolge gemeinsamer Ursache* (siehe IEC 61508-6:2000, Anhang D);

e) des *Diagnosedeckungsgrads* der *Diagnosetests* (bestimmt gemäß IEC 61508-2:2000, Anhänge A und C) und dem zugehörigen Diagnose-Testintervall;

ANMERKUNG 1 Bei der Festlegung des Diagnose-Testintervalls ist es notwendig, die Zeitabstände aller Tests, die zum *Diagnosedeckungsgrad* beitragen, zu berücksichtigen.

f) des Intervalls, innerhalb der *Proof-Tests* ausgeführt werden müssen, um gefahrbringende Fehler zu erkennen, die durch *Diagnosetests* nicht erkannt werden;

ANMERKUNG 2 In der Praxis kann die Ausführung von *Proof-Tests* für bestimmte Teile des *PDS(SR)* schwierig sein. In diesen Fällen darf als Intervall für *Proof-Tests* die Gebrauchsdauer dieser Teile oder des *PDS(SR)* selbst angenommen werden. Es sollte beachtet werden, dass für viele Anwendungen von Maschinen eine Gebrauchsdauer von 20 Jahren erforderlich sein kann.

g) die Reparaturzeiten für erkannte Ausfälle;

ANMERKUNG 3 Die Reparaturzeit bildet einen Teil der mittleren Zeit bis zur Wiederherstellung (siehe IEV 191-13-08), die auch die Zeit bis zur Erkennung eines Ausfalls und jede Zeit, in der eine Reparatur nicht möglich ist, einschließt (siehe IEC 61508-6:2000, Anhang B für ein Beispiel, wie die mittlere Zeit bis zur Wiederherstellung in der Berechnung der Wahrscheinlichkeit eines Ausfalls verwendet werden kann). In Fällen, in denen eine Reparatur nur während einer speziellen Zeitspanne ausgeführt werden kann, zum Beispiel während die EUC abgeschaltet ist und sich in einem sicheren Zustand befindet, ist es besonders wichtig, dass die Zeitdauer, in der keine Reparatur durchgeführt werden kann, vollständig berücksichtigt wird. Besonders wichtig ist dies, wenn diese Zeitspanne relativ groß ist.

h) die Wahrscheinlichkeit eines gefahrbringenden Ausfalls irgendeines Datenkommunikationsprozesses (siehe 6.4).

6.2.1.1.3 Ausfallraten

Die Daten der Ausfallrate eines Bauteils müssen entnommen werden:

– einer anerkannten Quelle oder

– Schätzungen auf der Basis derjenigen Bauteile, die als „betriebsbewährt“ betrachtet werden (siehe IEC 61508-2:2000, 7.4.7.6 bis 7.4.7.12).

Zur Ermittlung der Ausfallrate sollte die erwartete mittlere Betriebstemperatur eines Bauteils verwendet werden.

Alle verwendeten Ausfallraten sollten einen Vertrauensgrad von mindestens 60 % besitzen.

ANMERKUNG 1 Daten können einer Vielzahl von Veröffentlichungen der Industrie entnommen werden (siehe Anhang C).

ANMERKUNG 2 Falls Ausfalldaten des Herstellers zur Verfügung stehen, werden diese bevorzugt. Ist das nicht der Fall, dürfen allgemeingültige Daten benutzt werden.

ANMERKUNG 3 Obwohl bei den meisten Wahrscheinlichkeitsberechnungen eine konstante Ausfallrate angenommen wird, gilt diese nur unter der Voraussetzung, dass die Gebrauchsdauer des Bauteils nicht überschritten wird. Über die Gebrauchsdauer hinaus (d. h. wenn die Ausfallwahrscheinlichkeit mit der Zeit stark ansteigt) sind die Ergebnisse der meisten Wahrscheinlichkeitsberechnungsverfahren deshalb bedeutungslos. Folglich sollte jede Wahrscheinlichkeitsschätzung eine Spezifikation der Gebrauchsdauer des Bauteils beinhalten. Die Gebrauchsdauer hängt stark vom Bauteil selbst und seinen Betriebsbedingungen ab – vor allem von der Temperatur (z. B. können Elektrolytkondensatoren sehr empfindlich sein). Erfahrungen haben gezeigt, dass die Gebrauchsdauer oft in einem Bereich von 8 bis 12 Jahren liegt. Sie kann jedoch auch wesentlich geringer sein, wenn Bauteile nahe ihrer Spezifikationsgrenzwerte betrieben werden.

ANMERKUNG 4 Die in Anhang D angegebenen Fehlerlisten können zur Ermittlung der Ausfallarten benutzt werden.

6.2.1.1.4 Diagnose-Testintervall

Das Diagnose-Testintervall für jedes *Teilsystem* des *PDS(SR)* muss ermöglichen, dass das *PDS(SR)* die Anforderungen an die *PFH* erfüllen kann (siehe 6.2.1.1.1).

Wenn ein gefahrbringender Fehler zum Verlust der *Sicherheitsfunktion* führen kann, sind zur Vermeidung einer *Gefährdung* eine Erkennung dieses Fehlers innerhalb der *DC*-Grenzen und das Auslösen einer Fehlerreaktion erforderlich. Diagnose- und *Fehlerreaktionsfunktionen* müssen innerhalb der maximalen Fehlerreaktionszeit ausgeführt werden (siehe 5.4.2).

6.2.1.1.5 Diagnose-Testintervall bei einer Hardware-Fehlertoleranz von Null

Das Diagnose-Testintervall jedes *Teilsystems* eines *PDS(SR)* mit einer Hardware-Fehlertoleranz von Null, von dem eine *Sicherheitsfunktion* vollständig abhängt, muss so festgelegt werden, dass die Summe aus dem Diagnose-Testintervall und der Zeit zur Ausführung der festgelegten Aktion (*Fehlerreaktionsfunktion*) zum Erreichen oder Aufrechterhalten eines sicheren Zustandes kleiner ist als die festgelegte längste Fehlerreaktionszeit.

6.2.2 Strukturelle Einschränkungen

6.2.2.1 Grenzen des *SIL*

Im Zusammenhang mit der Hardware-*Sicherheitsintegrität* ist der höchste *Sicherheits-Integritätslevel*, der für eine *Sicherheitsfunktion* beansprucht werden kann, durch die Hardware-Fehlertoleranz und den *Anteil sicherer Ausfälle* des *Teilsystems* eines *PDS(SR)*, das diese *Sicherheitsfunktion* ausführt, begrenzt. Eine Hardware-Fehlertoleranz von N bedeutet, dass $N + 1$ Fehler einen Verlust der *Sicherheitsfunktion* verursachen könnte. Die Tabellen 3 und 4 legen den höchsten *Sicherheits-Integritätslevel* fest, der für die *Sicherheitsfunktion*, die dieses *Teilsystem* verwendet, beansprucht werden kann, wobei die Hardware-Fehlertoleranz und der *Anteil sicherer Ausfälle* dieses *Teilsystems* berücksichtigt werden (siehe IEC 61508-2:2000,

Anhang C). Die Anforderungen der Tabellen 3 oder 4, je nachdem, welche anwendbar ist, müssen auf jedes *Teilsystem* angewendet werden, das eine *Sicherheitsfunktion* ausführt, und folglich auf jedes Teil des *PDS(SR)*. In 6.2.2.2.1 und 6.2.2.2.2 wird festgelegt, welche der Tabellen 3 oder 4 für ein bestimmtes *Teilsystem* gilt. Im Hinblick auf diese Anforderungen gilt:

a) bei der Bestimmung der Hardware-Fehlertoleranz dürfen keine anderen Maßnahmen (wie Diagnose) in Betracht gezogen werden, die die Auswirkungen von Fehlern beherrschen können;

b) wenn ein Fehler direkt zum Auftreten eines oder mehrerer Folgefehler führt, werden diese als ein Einzelfehler betrachtet;

c) bei der Bestimmung der Hardware-Fehlertoleranz dürfen bestimmte Fehler ausgeschlossen werden, sofern die Wahrscheinlichkeit ihres Auftretens sehr gering im Verhältnis zu den Anforderungen an die *Sicherheitsintegrität* des *Teilsystems* ist. Der Ausschluss solcher Fehler muss begründet und dokumentiert werden (siehe Anmerkung 3).

ANMERKUNG 1 Die strukturellen Einschränkungen wurden aufgenommen, damit eine ausreichend widerstandsfähige Architektur unter Berücksichtigung der Komplexität des *Teilsystems* erreicht wird. Der Hardware-*Sicherheits-Integritätslevel* des *PDS(SR)*, der unter Anwendung dieser Anforderungen abgeleitet wird, ist der höchste Level, der beansprucht werden kann, selbst wenn in einigen Fällen theoretisch ein höherer *Sicherheits-Integritätslevel* abgeleitet werden könnte, wenn für das *PDS(SR)* der rein mathematische Ansatz angewendet werden würde.

ANMERKUNG 2 Bei der Festlegung der Architektur des *Teilsystems*, das die Anforderungen an die Hardware-Fehlertoleranz erfüllt, werden bestimmungsgemäße Betriebsbedingungen vorausgesetzt. Die Anforderungen an die Fehlertoleranz dürfen abgeschwächt werden, wenn das *PDS(SR)* während des Betriebs repariert wird. Die wichtigsten Parameter, die mit einer Abschwächung zusammenhängen, müssen jedoch vorher evaluiert worden sein (z. B. mittlere Zeit bis zur Wiederherstellung in Relation zur Anforderungswahrscheinlichkeit).

ANMERKUNG 3 Dies ist aus folgendem Grund erforderlich: Wenn ein Bauteil aufgrund von Eigenschaften seiner Ausführung und Konstruktion offensichtlich eine sehr geringe Ausfallwahrscheinlichkeit besitzt (z. B. ein Gestänge eines mechanischen Stellgliedes), ist es normalerweise nicht notwendig, die *Sicherheitsintegrität* einer *Sicherheitsfunktion*, die dieses Bauteil benutzt, einzuschränken (auf der Basis der Hardware-Fehlertoleranz).

6.2.2.2 *Teilsysteme* des Typs A und des Typs B

6.2.2.2.1 Typ A

Ein *Teilsystem* gehört zum Typ A, wenn für die Bauteile, die zum Erreichen der *Sicherheitsfunktion* erforderlich sind, Folgendes gilt:

a) das Ausfall aller eingesetzten Bauteile ausreichend definiert ist und

b) das Verhalten des *Teilsystems* unter Fehlerbedingungen vollständig bestimmt werden kann und

c) verlässliche Ausfalldaten durch Felderfahrung für das *Teilsystem* existieren, um zu zeigen, dass die angenommenen Ausfallraten für erkannte und unerkannte gefahrbringende Ausfälle erreicht werden.

ANMERKUNG Anhang D enthält Fehler und Fehlerausschlüsse, die in Betracht gezogen werden können.

6.2.2.2.2 Typ B

Ein *Teilsystem* gehört zum Typ B, wenn für die Bauteile, die zum Erreichen der *Sicherheitsfunktion* erforderlich sind, ein Kriterium oder mehrere Kriterien von 6.2.2.2.1 nicht erfüllt werden.

ANMERKUNG 1 Das bedeutet, dass, wenn mindestens ein Bauteil eines *Teilsystems* die Bedingungen für ein *Teilsystem* des Typs B erfüllt, das gesamte *Teilsystem* als Typ B und nicht als Typ A betrachtet werden muss.

ANMERKUNG 2 Der Steuerungsteil aus Mikrocontrollern usw. kann beispielsweise als *Teilsystem* des Typs B betrachtet werden.

ANMERKUNG 3 Anhang D enthält Fehler und Fehlerausschlüsse, die in Betracht gezogen werden können.

6.2.2.3 Strukturelle Einschränkungen

Es gelten die strukturellen Einschränkungen der Architektur nach Tabelle 3 oder Tabelle 4: Tabelle 3 gilt für jedes *Teilsystem* des Typs A, das Teil des *PDS(SR)* ist; Tabelle 4 gilt für jedes *Teilsystem* des Typs B, das Teil des *PDS(SR)* ist.

Tabelle 3 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen der Architektur für sicherheitsbezogene *Teilsysteme* des Typs A

Anteil sicherer Ausfälle [a]	**Hardware-Fehlertoleranz *N* (siehe 6.2.2.1)**		
	0	**1**	**2**
< 60 %	*SIL* 1	*SIL* 2	*SIL* 3
60 % bis < 90 %	*SIL* 2	*SIL* 3	*SIL* 3[b]
90 % bis < 99 %	*SIL* 3	*SIL* 3[b]	*SIL* 3[b]
≥ 99 %	*SIL* 3	*SIL* 3[b]	*SIL* 3[b]

[a] Einzelheiten über die Ermittlung des *Anteils sicherer Ausfälle* siehe 6.2.3.

[b] Dieser Teil von IEC 61800 gilt nur für *Sicherheitsfunktionen* mit einem *SIL* von höchstens 3. Für *Sicherheitsfunktionen* mit *SIL* 4 gelten die Anforderungen von IEC 61508.

Tabelle 4 – Hardware-*Sicherheitsintegrität*: Strukturelle Einschränkungen der Architektur für sicherheitsbezogene *Teilsysteme* des Typs B

Anteil sicherer Ausfälle [a]	**Hardware-Fehlertoleranz *N* (siehe 6.2.2.1)**		
	0	**1**	**2**
< 60 %	nicht zulässig	*SIL* 1	*SIL* 2
60 % bis < 90 %	*SIL* 1	*SIL* 2	*SIL* 3
90 % bis < 99 %	*SIL* 2	*SIL* 3	*SIL* 3[b]
≥ 99 %	*SIL* 3	*SIL* 3[b]	*SIL* 3[b]

[a] Einzelheiten über die Ermittlung des *Anteils sicherer Ausfälle* siehe 6.2.3.

[b] Dieser Teil von IEC 61800 gilt nur für *Sicherheitsfunktionen* mit einem *SIL* von höchstens 3. Für *Sicherheitsfunktionen* mit *SIL* 4 gelten die Anforderungen von IEC 61508.

6.2.3 Abschätzung des *Anteils sicherer Ausfälle (SFF)*

6.2.3.1 Analyseverfahren

Zur Abschätzung der *SFF* eines *Teilsystems* muss eine Analyse (z. B. Fehlerbaumanalyse, Ausfalleffektanalyse) durchgeführt werden, bei der alle zutreffenden Fehler und deren entsprechende Ausfallarten bestimmt werden. Die Wahrscheinlichkeit jeder Ausfallart des *Teilsystems* muss auf der Basis der Wahrscheinlichkeit der zugehörigen Fehler ermittelt werden.

6.2.3.2 Datenbasis

Die Ermittlung der *SFF* muss erfolgen aufgrund:

– statistisch signifikanter Daten der Ausfallrate, die aus der Felderfahrung gewonnen wurden, oder
– Ausfalldaten der Bauteile aus einer anerkannten Quelle.

Siehe auch 6.2.1.1.3.

ANMERKUNG Eine informative Liste bekannter Quellen ist im Anhang C enthalten.

6.2.3.3 Sicherheitsrelais

In einem *Teilsystem* mit einer Hardware-Fehlertoleranz von Null, bei dem ein Sicherheitsrelais mit einem zwangsgeführten Rückmeldekontakt verwendet wird, um eine *Sicherheitsfunktion* und einen *Diagnose-deckungsgrad* dieser Funktion bereitzustellen, ist der Anspruch der *Sicherheitsintegrität* infolge der strukturelle Einschränkungen der Architektur dieses *Teilsystems* auf *SIL* 2 beschränkt.

6.2.3.4 Berechnung der *SFF*

Der *Anteil sicherer Ausfälle* eines *Teilsystems* muss nach IEC 61508-2:2000, Anhänge A und C, berechnet werden.

6.2.4 Anforderungen an die systematische *Sicherheitsintegrität* eines *PDS(SR)* und von *PDS(SR)-Teilsystemen*

6.2.4.1 Anforderungen an die Vermeidung von Ausfällen

6.2.4.1.1 Allgemeines

Um Fehler beim Entwurf und bei der Entwicklung der Hardware des *PDS(SR)* zu verringern, müssen bestimmte Techniken und Maßnahmen angewendet werden.

Es sind die nach 6.2.4.1.4 geplanten Prüfungen durchzuführen. Siehe auch Abschnitt 9.

6.2.4.1.2 Auswahl des Entwurfsverfahrens

In Übereinstimmung mit dem geforderten *Sicherheits-Integritätslevel* muss das gewählte Entwurfsverfahren folgende Kriterien fördern:

a) Transparenz, Modularität und andere Eigenschaften, die die Komplexität verringern und das Verständnis des Entwurfs fördern;

b) eine eindeutige und genaue Spezifikation
   - der Funktionalität;
   - der Schnittstellen der *Teilsysteme*;
   - der Ablaufreihenfolgen und zeitbezogener Informationen;
   - von Gleichzeitigkeit und Synchronisation;

c) eine eindeutige und genaue Dokumentation und Weiterleitung der Informationen;

d) *Verifikation* und *Validierung*.

6.2.4.1.3 Entwurfsmaßnahmen

Es sind folgende Entwurfsmaßnahmen umzusetzen:

a) genauer Entwurf des *PDS(SR)* und/oder der *Teilsysteme* einschließlich:
   - der Anwendung der Bauteile innerhalb der Spezifikationen des Herstellers wie z. B. von Temperatur, Belastung, Stromversorgung, Leistungsbemessung und Zeitverhalten;
   - Herabsetzung von Parametern zur Erhöhung der Zuverlässigkeit, wenn dies zum Erreichen von Ausfallgrenzwerten erforderlich ist;
   - ordnungsgemäßer Zusammenbau der *Teilsysteme* einschließlich Verdrahtung und sämtlicher Anschlussverbindungen;
   - Überprüfungen für eine frühe Erkennung von Entwurfsfehlern;

b) Verträglichkeit:
   – Einsatz von *Teilsystemen* mit verträglichen Betriebskennwerten;
c) Beständigkeit gegen festgelegte Umgebungsbedingungen:
   – Entwurf des *PDS(SR)* in einer Weise, dass in allen festgelegten Umgebungen wie z. B. Temperatur, Feuchte, Vibrationen, EM Phänomene, Verschmutzungsgrad, Überspannungskategorie, Höhe ein sicherer Betrieb möglich ist.

6.2.4.1.4 Prüfplanung

Je nach Notwendigkeit müssen beim Entwurf folgende verschiedene Arten von Prüfungen geplant werden:

a) Prüfung des *Teilsystems*;
b) Prüfung der Integration;
c) Validierungsprüfung;
d) Konfigurationsprüfung (siehe 7.1).

Die Dokumentation der Prüfplanung muss umfassen:

a) Arten von durchzuführenden Prüfungen und anzuwendende Verfahren;
b) Prüfumgebung, -werkzeuge, -aufbau und -programme;
c) Annahme-/Ablehnungskriterien.

Soweit anwendbar müssen automatische Prüfwerkzeuge und integrierte Entwicklungswerkzeuge benutzt werden.

ANMERKUNG Die Integrität solcher Werkzeuge kann durch spezifische Prüfungen, durch langen zufrieden stellenden Einsatz oder durch unabhängige *Verifikation* ihrer Ergebnisse für das zu entwickelnde *PDS(SR)* nachgewiesen werden.

6.2.4.1.5 Anforderungen an die Behandlung von Revisionen während Entwurf und Entwicklung

In der Phase Entwurf und Entwicklung muss ein Prozess für die Behandlung von Revisionen und für erneute Tests festgelegt werden, um sicherzustellen, dass nach einer Überarbeitung die *Sicherheitsintegrität* des *PDS(SR)* auf dem geforderten Level bleibt.

6.2.4.2 Anforderungen an die Beherrschung systematischer Fehler

6.2.4.2.1 Entwurfsmerkmale

Zur Beherrschung von *systematischen Ausfällen* muss der Entwurf Eigenschaften aufweisen, die das *PDS(SR)* und seine *Teilsysteme* unanfällig machen gegen:

a) Restfehler in der Hardware, wenn die Möglichkeit von Fehlern im Entwurf der Hardware nicht durch Anwendung von IEC 61508-2:2000, A.3 und Tabelle A.16 ausgeschlossen werden kann;
b) Beanspruchungen durch Umgebungsbedingungen einschließlich elektromagnetischer Störungen durch Anwendung von IEC 61508-2:2000, A.3 und Tabelle A.17;
c) Fehler durch den Bediener des *PDS(SR)* (siehe IEC 61508-2:2000, A.3 und Tabelle A.18);
d) Restfehler in der Software des Entwurfs (siehe IEC 61508-2:2000, 7.4.3 und zugehörige Tabelle);
e) Fehler und andere Effekte durch Datenkommunikation (siehe 6.4).

6.2.4.2.2 Prüfbarkeit und Instandhaltbarkeit

Bei den Entwurfs- und Entwicklungsaktivitäten müssen Prüfbarkeit und Instandhaltbarkeit betrachtet werden, um die Umsetzung dieser Eigenschaften im endgültigen *PDS(SR)* zu ermöglichen.

6.2.4.2.3 Einschränkungen durch den Menschen

Der Entwurf des *PDS(SR)* muss die Fähigkeiten und Einschränkungen des Menschen berücksichtigen und er muss für Handlungen durch Bediener und Instandhaltungspersonal geeignet sein. Der Entwurf sämtlicher Bedienerschnittstellen muss unter Berücksichtigung einer üblichen Bedienung durch den Menschen erfolgen und mögliche Ausbildung und Kenntnisse der Bediener berücksichtigen.

6.2.4.2.4 Schutz gegen unbeabsichtigte Modifikation

Das *PDS(SR)* muss Maßnahmen zum Schutz gegen unbeabsichtigte Modifikationen von sicherheitsbezogener Software, Hardware, Parametrierung und Konfiguration des *PDS(SR)* umfassen.

ANMERKUNG Siehe IEC 61508-7:2000, B.4.8.

6.2.4.2.5 Eingabebestätigung und Bedienfehler

Der Entwurf des *PDS(SR)* muss eine Bestätigung einer Eingabe zur Beherrschung von Eingabefehlern umfassen. Der Entwurf muss außerdem durch Plausibilitätsprüfungen gegen Bedienfehler (bezogen auf *Sicherheitsfunktionen* des *PDS(SR)*) absichern.

ANMERKUNG IEC 61508-7:2000, B.4.6 und B.4.9.

6.2.4.2.6 Verlust der Energieversorgung

Das *PDS(SR)* muss unter Berücksichtigung der Auswirkungen des Verlustes der Energieversorgung ausgelegt und entwickelt werden.

6.2.5 Anforderungen an die elektromagnetische Störfestigkeit eines *PDS(SR)*

6.2.5.1 Allgemeines

In 6.2.5.3 wird ein Leistungskriterium festgelegt, das bei der Durchführung von elektromagnetischen Störfestigkeitsprüfungen am *PDS(SR)* angewendet werden muss. Dieses Kriterium gilt nicht für normale (nicht sicherheitsbezogene) Funktionen der Einrichtung (funktionale elektromagnetische Verträglichkeit (EMV) des *PDS(SR)* ist erreicht, wenn das *PDS(SR)* den Anforderungen von IEC 61800-3 entspricht).

6.2.5.2 Vorgesehene Umgebung

Bei der Ermittlung der Prüfschärfe für die elektromagnetische Störfestigkeit muss die festgelegte elektromagnetische Umgebung für den vorgesehenen Einsatz eines *PDS(SR)* berücksichtigt werden.

Wenn dem *PDS(SR)*-Hersteller die elektromagnetische Umgebung nicht bekannt ist, müssen für die Störfestigkeitsprüfungen die Prüfschärfen von IEC 61800-3 angewendet werden.

6.2.5.3 Leistungskriterium

Folgendes Leistungskriterium muss von den festgelegten *Sicherheitsfunktionen* eines *PDS(SR)* erfüllt werden. Das Verhalten aller nicht sicherheitsbezogenen Funktionen des *PDS(SR)* wird nicht betrachtet, sofern nicht 6.2.5.4 gilt.

(FS) Funktionen des *PDS(SR)*, die für Sicherheitsanwendungen vorgesehen sind:

– müssen innerhalb ihrer festgelegten Grenzwerte für die *funktionale Sicherheit* bleiben oder
– dürfen zeitweise oder dauerhaft ihre festgelegten Grenzwerte für die *funktionale Sicherheit* überschreiten, wenn das *PDS(SR)* auf die elektromagnetische Störung so reagiert, dass ein definierter sicherer Zustand des *PDS(SR)* aufrechterhalten bleibt oder innerhalb der festgelegten längsten Fehlerreaktionszeit erreicht wird.

Eine dauerhafte Verschlechterung der *Sicherheitsfunktion* oder eine Zerstörung der Bauteile ist zulässig, sofern ein sicherer Zustand aufrechterhalten bleibt oder innerhalb der festgelegten längsten Fehlerreaktionszeit erreicht wird.

Dieses Kriterium gilt für alle elektromagnetischen Phänomene, die für das *PDS(SR)* in seiner vorgesehenen Anwendung von Bedeutung sind.

6.2.5.4 Entstehung von *Gefährdungen*

Wenn eine elektromagnetische Störfestigkeitsprüfung durchgeführt wird, dürfen durch das *PDS(SR)* keine gefährlichen Zustände oder *Gefährdungen* entstehen.

6.2.5.5 *Verifikation*

Bei der Durchführung von elektromagnetischen Störfestigkeitsprüfungen müssen die festgelegten Entstörmaßnahmen vorhanden sein.

Abhängig von der Analyse der elektromagnetischen Umgebung für die vorgesehene Anwendung des *PDS(SR)* werden zum Nachweis einer erhöhten Störfestigkeit (nach den Forderungen in IEC 61508-2) entweder:

– soweit erforderlich (abhängig vom elektromagnetischen Phänomen und dem geforderten *SIL*) die Prüfschärfe und/oder die Prüfdauer und/oder die Anzahl der Prüfzyklen erhöht oder

– die Wirksamkeit aller zusätzlichen Entstörmaßnahmen nachgewiesen (siehe IEC 61508-7:2000, A.11.3), die festgelegt wurden.

6.3 Verhalten bei der Erkennung von Fehlern

6.3.1 Fehlererkennung

Fehler innerhalb eines *PDS(SR)* können durch *Diagnosetests* erkannt werden.

Wenn ein gefahrbringender Fehler erkannt wird, der zu einem Verlust der *Sicherheitsfunktion* führen kann, muss eine *Fehlerreaktionsfunktion* ausgelöst werden, um eine *Gefährdung* zu verhindern. Diagnose- und *Fehlerreaktionsfunktion* müssen innerhalb der längsten Fehlerreaktionszeit durchgeführt werden.

6.3.2 Fehlertoleranz größer Null

Die Erkennung eines gefahrbringenden Fehlers (durch *Diagnosetests* oder andere Mittel) in einem *Teilsystem* mit einer Hardware-Fehlertoleranz größer Null muss zu folgenden Reaktionen führen:

a) einer *Fehlerreaktionsfunktion* oder

b) der Abtrennung des fehlerhaften Teils des *Teilsystems*, damit einer weiterer sicherer Betrieb der Maschinen und/oder der Anlagen möglich ist, während der fehlerhafte Teil repariert wird. Ist die Reparatur innerhalb der mittleren Dauer bis zur Wiederherstellung (MTTR), die bei der Berechnung der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls ermittelt wird (siehe 6.2.1), noch nicht abgeschlossen, muss eine *Fehlerreaktionsfunktion* ausgelöst werden.

6.3.3 Fehlertoleranz von Null

Die Erkennung eines gefahrbringenden Fehlers (durch *Diagnosetests* oder andere Mittel) in einem *Teilsystem* mit einer Hardware-Fehlertoleranz von Null, von dem eine *Sicherheitsfunktion* vollständig abhängt, muss zu einer *Fehlerreaktionsfunktion* führen.

6.4 Zusätzliche Anforderungen an die Datenkommunikation

Wenn zur Ausführung einer *Sicherheitsfunktion* Datenkommunikation angewendet wird, dann muss die Wahrscheinlichkeit des unerkannten Ausfalls des Kommunikationsprozesses unter Berücksichtigung von Übertragungsfehlern, Wiederholungen, Verlust, Einfügungen, falsche Abfolge, Verfälschung, Verzögerung und

Maskerade ermittelt werden. Diese Wahrscheinlichkeit muss bei der Abschätzung der *PFH* der *Sicherheitsfunktion* durch zufällige Ausfälle (siehe 6.2.1.1.2) berücksichtigt werden.

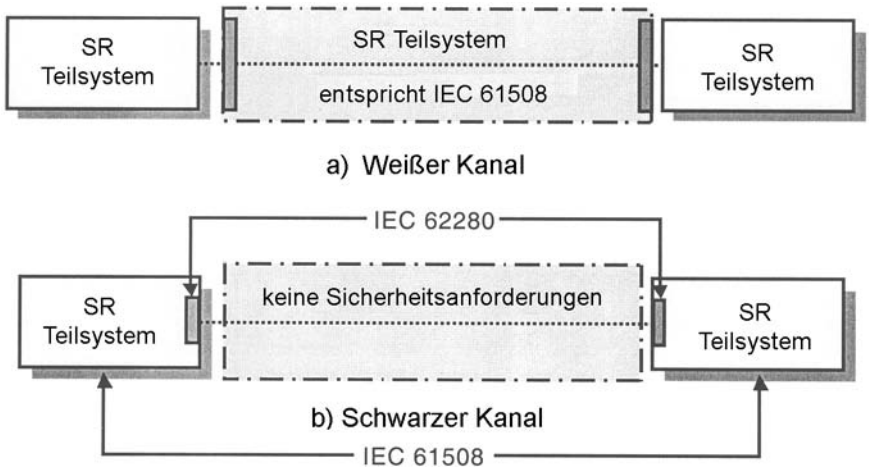
ANMERKUNG Maskerade bedeutet, dass der wahre Inhalt einer Nachricht nicht richtig identifiziert wird. Eine Nachricht von einer nicht sicheren Komponente wird beispielsweise als Nachricht von einer Sicherheitskomponente identifiziert.

Die erforderlichen Maßnahmen zur Sicherung des geforderten Ausfallwertes des Kommunikationsprozesses müssen nach den Anforderungen von IEC 61508-2 und IEC 61508-3 realisiert werden. Es gibt zwei mögliche Ansätze:

a) der Kommunikationskanal muss nach der gesamten Norm IEC 61508 entworfen, ausgeführt und validiert werden (so genannter „weißer Kanal“, siehe Bild 3a)) oder

b) Teile des Kommunikationskanals wurden nicht nach IEC 61508 entworfen oder validiert (so genannter „schwarzer Kanal“, siehe Bild 3b)). In diesem Fall müssen die erforderlichen Maßnahmen zur Sicherung der Leistungsfähigkeit im Fehlerfall des Kommunikationsprozesses in den sicherheitsbezogenen Bauteilen des *PDS(SR)* realisiert werden, die mit dem Kommunikationskanal verbunden sind. Die Realisierung muss nach IEC 62280 in angemessener Weise erfolgen.

Wenn die Datenkommunikation dazu benutzt wird, sicherheitsbezogene Daten mit *Teilsystemen* außerhalb des *PDS(SR)* auszutauschen, gelten für das *PDS(SR)* zusammen mit dem betreffenden *Teilsystem* die oben angegebenen Anforderungen.



SR: sicherheitsbezogen (en: safety related)

Bild 3 – Architekturen der Datenkommunikation: a) Weißer Kanal, b) Schwarzer Kanal

6.5 Anforderungen an Integration und Prüfung des *PDS(SR)*

6.5.1 Integration der Hardware

Das *PDS(SR)* muss wie in seinem Entwurf spezifiziert integriert werden. Als Teil der Integration sämtlicher *Teilsysteme* und Bauteile in das *PDS(SR)* muss dieses mit den festgelegten Integrationsprüfungen geprüft werden. Diese Prüfungen sind im Verifikationsplan festgelegt und müssen nachweisen, dass alle Module ordnungsgemäß in Wechselwirkung miteinander stehen und ihre vorgesehene Funktion und keine nicht vorgesehenen Funktionen ausführen.

Alternativ sind die Anforderungen an die Hardware-Integration erfüllt, wenn die Typprüfung des *PDS(SR)* nach 6.2.5 und IEC 61800-5-1 und zusätzlich nach IEC 61800-1 oder IEC 61800-2 oder IEC 61800-4 (wie zutreffend) bestanden wurden.

6.5.2 Integration der Software

Die Integration eines sicherheitsbezogenen Softwareteils/-moduls in das *PDS(SR)* muss nach IEC 61508-3 erfolgen. Dazu gehören Prüfungen, die im Software-Verifikationsplan festgelegt sind, um sicherzustellen,

dass die Verträglichkeit der Software mit der Hardware in einem Umfang besteht, dass die Anforderungen an die funktionale und sicherheitsbezogene Leistungsfähigkeit erfüllt werden.

ANMERKUNG Dazu gehört nicht die Prüfung aller Kombinationen von Eingangswerten. Die Prüfung aller Äquivalenzklassen (siehe IEC 61508-7:2000, B.5.2) kann ausreichen. Die statische Analyse (siehe IEC 61508-7:2000, B.6.4), die dynamische Analyse (siehe IEC 61508-7:2000, B.6.5) oder die Ausfallanalyse (siehe IEC 61508-7:2000, B.6.6) können die Anzahl der Testfälle auf einen annehmbaren Umfang verringern.

6.5.3 Modifikationen bei der Integration

Bei der Integration müssen sämtliche Modifikationen oder Änderungen des *PDS(SR)* einer Einflussanalyse unterzogen werden, die alle beeinflussten Komponenten identifiziert, und einer zusätzlichen *Verifikation*.

6.5.4 Durchzuführende Integrationsprüfungen

Die Integrationsprüfung(en) muss (müssen) in einem Verifikationsplan festgelegt werden. Es muss eine Funktionsprüfung mit Eingangswerten oder Sollwerten durchgeführt werden, die den bestimmungsgemäß erwarteten Betrieb des PDS(SR) angemessen nachbilden. Die *Sicherheitsfunktion* wird angefordert (z. B. durch Aktivierung von STO oder Überschreitung der Drehzahlbegrenzung für SLS) und das sich ergebende Verhalten wird beobachtet und mit den Angaben in der Spezifikation verglichen (siehe auch Abschnitt 9).

6.5.5 Prüfprotokoll

Bei der *PDS(SR)*-Integrationsprüfung muss Folgendes dokumentiert werden:

a) die Version des verwendeten Prüfplanes;

b) die Kriterien für die Abnahme der Integrationsprüfungen;

c) der Typ und die Version des zu prüfenden *PDS(SR)*;

d) die verwendeten Werkzeuge und Einrichtungen zusammen mit den Kalibrierdaten;

e) die Ergebnisse jeder Prüfung;

f) jeder Widerspruch zwischen erwarteten und tatsächlichen Ergebnissen.

7 Anwenderdokumentation

7.1 Informationen und Anweisungen für eine sichere Anwendung eines *PDS(SR)*

Die folgenden Informationen müssen vom Hersteller angegeben und dem Anwender zur Verfügung gestellt werden.

a) Eine funktionale Spezifikation jeder Funktion und Schnittstelle, die zur Realisierung der *Sicherheitsfunktionen* zur Verfügung steht. Dazu gehört:
   - eine genaue Beschreibung der *Sicherheitsfunktion* (einschließlich der Reaktion(en) auf eine Verletzung der Grenzwerte);
   - die *Fehlerreaktionsfunktion*;
   - die Antwortzeit jeder sicherheitsbezogenen Funktion und der zugehörigen *Fehlerreaktionsfunktionen*;
   - die Bedingung(en) (z. B. *Betriebsart*), unter denen die *Sicherheitsfunktion* aktiv oder gesperrt ist(sind);
   - die Priorität derjenigen Funktionen, die gleichzeitig aktiv sind und miteinander im Widerspruch stehen können.

b) Die Information der *Sicherheitsintegrität* für jede *Sicherheitsfunktion* einschließlich:
   - *SIL-Fähigkeit*;
   - *PFH*-Wert.

c) Die Umgebungs- und Betriebsbedingungen (einschließlich elektromagnetischer Bedingungen), unter denen der Einsatz des *PDS(SR)* vorgesehen ist (siehe auch IEC 61800-1 oder IEC 61800-2 oder IEC 61800-4, IEC 61800-3 und IEC 61800-5-1). Dabei sind Lagerung, Transport, Installation, Inbetriebnahme, Prüfung, Betrieb und Instandhaltung zu berücksichtigen.

d) Die Angabe aller Einschränkungen für das *PDS(SR)* für:

- die Umgebung, die beachtet werden sollte, um die Gültigkeit der ermittelten Ausfallraten aufrechtzuerhalten;
- die *Gebrauchsdauer* des *PDS(SR)* und das (die) Intervall(e) des (der) *Proof-Test*s, falls zutreffend;
- alle Anforderungen an Prüfungen, Kalibrierung oder Instandhaltung;
- alle Grenzen der Anwendung des *PDS(SR)*, die beachtet werden sollten, um *systematische Ausfälle* zu verhindern;
- die *SIL-Fähigkeit* jeder *Sicherheitsfunktion*;
- alle Informationen, die zur Kennzeichnung der Hardware- und Softwarekonfiguration des *PDS(SR)* erforderlich sind, um das Konfigurationsmanagement nach Abschnitt 4 zu ermöglichen.

e) Installations- und Inbetriebnahmerichtlinien (siehe IEC 61800-5-1:2003, Abschnitt 6) einschließlich Einstellungen und Parametrisierung.

f) Anforderungen an die Konfigurationsprüfung der *Sicherheitsfunktionen* in Fällen, in denen die Integrität der Konfigurationsmittel einer *Sicherheitsfunktion* nicht gewährleistet werden kann (z. B. PC-Werkzeuge zur Konfiguration).

Die Konfigurationsprüfung wird nach der Inbetriebnahme oder der Modifikation einer Anwendung durchgeführt, um sicherzustellen, dass die verwendeten *Sicherheitsfunktionen* des *PDS(SR)* wie vorgesehen konfiguriert wurden. Die Prüfung bestätigt in erster Linie die vorgesehenen Parameterwerte innerhalb des *PDS(SR)*. Die Prüfung wird gewöhnlich von der für die Inbetriebnahme des *PDS(SR)* verantwortlichen Stelle unter Anwendung von Prüfverfahren durchgeführt, die vom *PDS(SR)*-Hersteller zur Verfügung gestellt werden.

Im Handbuch der Konfigurationsprüfung müssen mindestens die folgenden Punkte aufgezeichnet werden:

- Beschreibung der Anwendung einschließlich eines Bildes;
- Beschreibung der sicherheitsbezogenen Bauteile (einschließlich Software-Versionen), die in der Anwendung benutzt werden;
- Liste der verwendeten *Sicherheitsfunktion*en des *PDS(SR)*;
- Ergebnisse aller Prüfungen dieser *Sicherheitsfunktion*en unter Anwendung der angegebenen Prüfverfahren;
- Liste aller sicherheitsbezogenen Parameter und ihrer Werte im *PDS(SR)*;
- Prüfsumme, Prüfdatum und Bestätigung durch das Prüfpersonal.

Konfigurationsprüfungen für *PDS(SR)* in baugleichen Anwendungen dürfen als eine einzelne Typprüfung der baugleichen Anwendung durchgeführt werden, sofern sichergestellt werden kann, dass die *Sicherheitsfunktionen* wie in allen Geräten vorgesehen konfiguriert wurden.[N1)]

g) Die *Diagnosetests*, die entweder vom Anwender oder durch Teile einer *Anlage*, die ein *PDS(SR)* enthalten, durchzuführen sind (z. B. PLC, Überwachungs-Controller).

h) Es sind Betriebs- und Instandhaltungsverfahren für das *PDS(SR)* anzugeben, die Folgendes festlegen müssen:

- die Routinevorgänge, die zur Aufrechterhaltung der *funktionalen Sicherheit* des *PDS(SR)* durchgeführt werden müssen, einschließlich Austausch von Bauelementen mit begrenzter Lebensdauer (z. B. Lüfter, Batterien usw.);
- die Aktionen und Einschränkungen, die zur Verhinderung eines gefährlichen Zustandes erforderlich sind und/oder die Folgen eines gefährlichen Vorfalls abschwächen;
- die anzuwendenden Instandhaltungsverfahren, wenn Fehler oder Ausfälle im *PDS(SR)* auftreten, einschließlich

---

[N1)] Die Konfigurationsprüfung entspricht der in Deutschland bisher als Abnahmetest bezeichneten Prüfung.

  - Verfahren der Fehlerdiagnose und Reparatur und
  - Verfahren der erneuten *Validierung*;
- für die Instandhaltung und die erneute *Validierung* notwendigen Werkzeuge und Verfahren für die Instandhaltung der Werkzeuge und Einrichtungen.

ANMERKUNG Die Betriebs- und Instandhaltungsverfahren des *PDS(SR)* sollten ständig verbessert werden, z. B. durch:

- Audits der *funktionalen Sicherheit*;
- Prüfungen am *PDS(SR)*.

8 *Verifikation* und *Validierung*

8.1 Allgemeines

Das Ziel dieses Abschnittes ist die Sicherstellung der Einhaltung des Planes der *funktionalen Sicherheit* (siehe 5.3).

8.2 *Verifikation*

Im Entwurfs-/Entwicklungsprozess muss nach jeder Entwurfs-/Entwicklungsphase nachgewiesen werden, dass die Anforderungen dieser Entwurfs-/Entwicklungsphase erfüllt worden sind. Eine *Verifikation* kann durch Bewertung, Analyse, Überprüfung und/oder Prüfung durchgeführt werden.

8.3 *Validierung*

Nach dem Entwurfs-/Entwicklungsprozess muss überprüft werden, ob das *PDS(SR)* alle Anforderungen erfüllt, die in der *Spezifikation der Sicherheitsanforderungen* angegeben sind. Eine *Validierung* kann durch Bewertung, Analyse, Überprüfung und/oder Prüfung erfolgen. IEC 61508-2:2000, Tabelle B.5, enthält Empfehlungen zur Vermeidung von Fehlern bei der *Validierung*.

8.4 Dokumentation

Es ist eine geeignete Dokumentation der entsprechenden *Verifikation* oder *Validierung* des *PDS(SR)* zu erstellen, die Folgendes enthält:

a) die Version(en) des (der) verwendeten Verifikations- und Validierungsplanes (-pläne);

b) die zu prüfende(n) (oder zu analysierende(n)) *Sicherheitsfunktion(en)* zusammen mit Verweisungen auf die Anforderung(en), die bei der Planung der Sicherheitsverifikation und -validierung des *PDS(SR)* festgelegt wurde(n);

c) verwendete Werkzeuge und Einrichtungen;

d) die Ergebnisse jeder *Verifikation* und *Validierung*.

9 Prüfanforderungen

9.1 Prüfplanung

Die Prüfung der *Sicherheitsfunktionen* des *PDS(SR)* muss gleichzeitig in jeder Phase des Entwicklungsprozesses geplant werden.

Der Prüfplan muss dokumentiert werden und eine genaue Beschreibung folgender Einzelheiten enthalten:

a) Funktionsprüfung jeder *Sicherheitsfunktion*;

b) Funktionsprüfung jeder Diagnosefunktion für eine *Sicherheitsfunktion*;

c) Annahmekriterien.

Prüfungen können entweder als „Blackbox“ durchgeführt werden, wobei die interne Realisierung der *Sicherheitsfunktion* unberücksichtigt bleibt, oder als „Whitebox“, wobei die besondere Kenntnis der Realisierung dazu benutzt wird, die Prüfung genau festzulegen (z. B. Einfügung von Fehlern).

Wenn es durch entsprechende Anforderungen zulässig ist, darf auf die Prüfung verzichtet werden oder sie darf durch andere Verifikations- oder Validierungsverfahren ersetzt werden.

9.2 Prüfdokumentation

Bei der Prüfung der *Sicherheitsfunktionen* des *PDS(SR)* müssen folgende Einzelheiten dokumentiert werden:

– die Version des verwendeten Prüfplanes;
– die Annahmekriterien der Prüfungen;
– der Typ und die Version des zu prüfenden *PDS(SR)*;
– die verwendeten Werkzeuge und Einrichtungen zusammen mit den Kalibrierdaten;
– die Prüfbedingungen;
– das Prüfpersonal;
– die genauen Ergebnisse jeder Prüfung;
– jeder Widerspruch zwischen erwarteten und tatsächlichen Ergebnissen;
– die Schlussfolgerung aus der Prüfung: entweder das Bestehen der Prüfung oder die Gründe für das Versagen.

10 Modifikation

10.1 Ziel

Das Ziel dieses Abschnittes ist die Sicherstellung, dass die *funktionale Sicherheit* des *PDS(SR)* noch gegeben ist, wenn nach der Freigabe der ursprünglichen Entwicklung für die Produktion Bauartänderungen erfolgt sind.

10.2 Anforderungen

Vor der Ausführung einer Modifikation müssen die Verfahren geplant werden. Modifikationen müssen mit mindestens dem gleichen Sachverstand, den gleichen automatisierten Werkzeugen, der gleichen Planung und dem gleichen Management durchgeführt werden, wie die ursprüngliche Entwicklung des *PDS(SR)*. Modifikationen müssen nach Plan durchgeführt werden.

10.2.1 Anforderungen an die Modifikation

Die Modifikation darf nur durch Ausgabe einer Modifikationsforderung nach den Verfahren für das Management der *funktionalen Sicherheit* ausgelöst werden (siehe Abschnitt 5). Diese Forderung muss Folgendes umfassen:

a) die Begründung der Änderung;
b) die vorgeschlagene Änderung (sowohl der Hardware als auch der Software).

10.2.2 Einflussanalyse

Es muss eine Bewertung der Auswirkung der vorgeschlagenen Modifikation auf die *funktionale Sicherheit* des *PDS(SR)* vorgenommen werden. Die Bewertung muss in einer angemessenen Analyse bestehen und den Umfang ermitteln, in dem eine Rückkehr zu den entsprechenden Entwicklungsstufen nach 5.2 vorgenommen werden muss.

10.2.3 Berechtigung

Die Berechtigung zur Durchführung der geforderten Modifikation muss vom Ergebnis der Einflussanalyse abhängen.

10.2.4 Dokumentation

Für jede *PDS(SR)*-Modifikation muss eine angemessene Dokumentation aufgestellt und geführt werden. Diese Dokumentation muss enthalten:

a) die genaue Spezifikation der Modifikation;

b) Ergebnisse der Einflussanalyse;

c) sämtliche Freigaben für die Änderung;

d) Testfälle für Komponenten einschließlich Daten zur erneuten *Validierung*;

e) Verlauf des *PDS(SR)*-Konfigurationsmanagements (Hardware und Software);

f) Abweichungen vom früheren Betrieb und von früheren Bedingungen;

g) notwendige Änderungen für die Anwenderdokumentation;

h) sämtliche anzuwendenden Entwicklungsstufen nach 5.2.

Anhang A
(informativ)

Aufgabenablaufplan

Entsprechend dem in IEC 61508 beschriebenen Lebenszyklus ist das folgende Entwurfs-/Entwicklungsverfahren für ein *PDS(SR)* geeignet. Es wird die Reihenfolge der erforderlichen Entwicklungsstufen angegeben und auf die zutreffenden Abschnitte in der vorliegenden Norm oder in der IEC 61508 verwiesen.

ANMERKUNG 1 Die Phase „Entwurf und Entwicklung“ des Lebenszyklus wurde nach der allgemeinen Entwurfspraxis in „Konzept“ und in „Entwurf und Entwicklung“ unterteilt.

ANMERKUNG 2 Wenn eine Zertifizierung durch Dritte gewünscht wird, sollte am Beginn des Entwurfsverfahrens ein Kontakt zwischen dem *PDS(SR)*-Hersteller und der Zertifizierungsstelle hergestellt werden.

ANMERKUNG 3 In der folgenden Tabelle gelten die Verweise auf die IEC 61508 für die erste Ausgabe des angegebenen Teils. In den nachfolgenden Ausgaben können sich die Abschnittsnummern verändert haben.

	Aufgaben	Verweisungen
1	**Allgemeine Anforderungen**	
	Alle zutreffenden Dokumente unterliegen einem geeigneten Dokumentenkontrollverfahren. Beschreibung des Projektmanagements Zertifizierung des QM-Systems	IEC 61508-1:1998, Abschnitt 5 IEC 61508-2:2000, 7.3, 7.7, 7.8, 7.9 IEC 61508-3:1998, 6, 7.3, 7.4.2.1, 7.7, 7.8, 7.9
2	***Spezifikation der Sicherheitsanforderungen* für das *PDS(SR)***	Phase 1 des *PDS(SR)*-Sicherheitslebenszyklus (siehe 5.2 dieser Norm)
	Erstellen einer *Spezifikation der Sicherheitsanforderungen (SRS)* einschließlich der Anforderungen an die *Sicherheitsfunktionen* und an die *Sicherheitsintegrität*	siehe 5.4 dieser Norm IEC 61508-1:1998, 7.6 IEC 61508-2:2000, 7.2, Tabellen B.1, B.6 IEC 61508-2:2000, 7.4.4-6, Anhang A IEC 61508-3:1998, 7.2, Tabellen A.1, B.7 IEC 61508-3:1998, 7.4.2/4, Tabellen A.3, B.1 IEC 61508-7:2000, Tabelle C.1 Beispiele in IEC 61508-5 Beispiele in IEC 61508-6:2000, Anhang A
3	***Verifikation* der *Spezifikation der Sicherheitsanforderungen* für das *PDS(SR)***	
	a) Überprüfung der *Spezifikation der Sicherheitsanforderungen* b) Kontrolle durch eine unabhängige Person oder eine unabhängige Abteilung, wenn gefordert	a) siehe 9.2 dieser Norm b) IEC 61508-2:2000 und IEC 61508-3:1998, 7.9
4	**Konzept**	Phase 3 des *PDS(SR)*-Sicherheitslebenszyklus (siehe 5.2 dieser Norm)
	a) Hardware-Entwurf auf Architekturebene mit: – Blockdiagrammen der sicherheitsbezogenen Hardware	a) siehe Abschnitt 6 dieser Norm

	Aufgaben	Verweisungen
	– Anwender- und Prozessschnittstellen – sicherheitsbezogenen Signalpfaden – Stromversorgung – Trennung unabhängiger Kanäle zum Erreichen der Fehlertoleranz – Kommunikationsverbindungen zwischen den unabhängigen Kanälen zum Erreichen des *Diagnosedeckungsgrad*es	IEC 61508-2:2000, 7.4, Anhang A, Tabellen B.2, B.6 Beispiele in IEC 61508-6:2000, Anhänge A und D
	b) Software-Entwurf auf Architekturebene mit: – Beschreibung der Funktionen, die durch die sicherheitsbezogene Software ausgeführt werden – Wechselwirkungen mit der Hardware – Diagramme der Zustandsmaschine mit dem vorgesehenen Verhalten der Software – Anwender- und Prozessschnittstellen – Möglichkeiten der Fehlererkennung und Fehlerreaktionen – Überblick über die Softwarestruktur, z. B. mit einem Blockdiagramm – Handhabung und Speicherung sicherheitsbezogener Daten – Versionsverwaltung – verwendete Werkzeuge, z. B. Compiler zur Codeprüfung usw.	b) IEC 61508-2:2000, 7.2.3.1 h) IEC 61508-3:1998, 7.2.2.8, 7.2.2.10, 7.4.2/3, Tabellen A.2, B.1, B.7, B.9 IEC 61508-7:2000, Tabelle C.1
	c) Empfehlung: Vor-Abschätzung der Ausfallwahrscheinlichkeit von *Sicherheitsfunktionen* durch zufällige Hardwareausfälle auf Ebene der funktionalen Blockdiagramme	c) IEC 61508-1:1998, Tabelle 2 IEC 61508-2:2000, 7.4.3, Tabellen 3, A.1, Anhang C IEC 61508-3:1998, Tabelle B.4 (FMEA) Beispiele in IEC 61508-6:2000, Anhänge C und D
5	***Verifikation* des Konzeptes**	
	a) Überprüfung des Systementwurfs b) Kontrolle durch unabhängige Person oder Abteilung, wenn gefordert	a) siehe 8.2 dieser Norm b) IEC 61508-2:2000 und IEC 61508-3:1998, 7.9
6	**Planung der *Validierung***	Phase 2 des *PDS(SR)*-Sicherheitslebenszyklus (siehe 5.2 dieser Norm)
	a) detaillierte Planung der *Validierung* des sicherheitsbezogenen *PDS(SR)* b) Der Validierungsplan muss parallel zu Phase 9.3, Entwurf und Entwicklung, erstellt werden.	a) siehe 8.3 dieser Norm b) IEC 61508-2:2000, 7.3, Tabelle B.5 IEC 61508-3:1998, 7.3, Tabellen A.7, B.3, B.5
7	***Verifikation* des Validierungsplans**	
	a) Überprüfung des Validierungsplans b) Kontrolle durch unabhängige Person oder Abteilung, wenn gefordert	a) siehe 8.2 dieser Norm b) IEC 61508-2:2000 und IEC 61508-3:1998, 7.9

	Aufgaben	Verweisungen
8	**Entwurf und Entwicklung**	Phase 3 des *PDS(SR)*-Sicherheitslebenszyklus (siehe 5.2 dieser Norm)
		siehe Abschnitt 6 dieser Norm
	a) Entwurf der Hardware b) Entwurf der Software c) Zuverlässigkeitsvorhersage (Berechnung der Ausfallwahrscheinlichkeit von *Sicherheitsfunktionen* durch zufällige Hardwareausfälle) mit: – Typ des *PDS(SR)* – *SFF* – Funktionsblockdiagramm – Zuverlässigkeitsmodell – Datenbasis für das Modell (Stückliste) – *PFH*-Berechnung – *Gebrauchsdauer* – Reparaturzeiten, Intervall für die *Proof-Test*s (falls zutreffend)	a) IEC 61508-2:2000, 7.4, Anhang A, Tabelle B.2, B.3, B.6 b) IEC 61508-3:1998, 7.4.5, 7.4.6, Tabelle A.4 c) IEC 61508-1:1998, Tabelle 2 IEC 61508-2:2000, 7.4.3, 7.4.7, Tabelle 3, A.1, Anhang C IEC 61508-3:1998, Tabelle B.4 (FMEA) Beispiele in IEC 61508-6:2000, Anhänge C und D
9	***Verifikation* des Entwurfs**	
	a) Überprüfung des Systementwurfs b) Funktionsprüfungen auf Modulebene c) Kontrolle durch unabhängige Person oder Abteilung, wenn gefordert	a) siehe 8.2 dieser Norm c) IEC 61508-2:2000, 7.9 IEC 61508-3:1998, 7.4.7, 7.4.8, 7.5, 7.9, Tabellen A.5, A.9
10	**Integration des *PDS(SR)***	Phase 4 des *PDS(SR)*-Sicherheitslebenszyklus (siehe 5.2 dieser Norm)
	Integration und Test des sicherheitsbezogenen *PDS(SR)*	siehe 6.5 dieser Norm
11	***Verifikation* der Integration**	
	Überprüfung der Testergebnisse und der Dokumentation für die HW-/SW-Integration	siehe 8.2 dieser Norm IEC 61508-2:2000, 7.5, 7.9, Tabellen B.3, B.6 IEC 61508-3:1998, 7.4.3.2 f), 7.4.5.5, 7.4.6.2, 7.4.7, 7.5, 7.9, Tabellen A.5, A.6, A.9
12	**Installation, Inbetriebnahme und Betrieb (Anwenderdokumentation)**	Phase 5 des *PDS(SR)*-Sicherheitslebenszyklus (siehe 5.2 dieser Norm)
	Erstellen der Anwenderdokumentation, die Installation, Inbetriebnahme, Betrieb und Instandhaltung des *PDS(SR)* beschreibt	siehe Abschnitt 7 dieser Norm IEC 61508-2:2000, 7.6, Tabelle B.4
13	***Verifikation* der Anwenderdokumentation**	
	a) Überprüfung der Anwenderdokumentation, die Installation, Inbetriebnahme, Betrieb und Instandhaltung des *PDS(SR)* beschreibt b) Kontrolle durch unabhängige Person oder Abteilung, wenn gefordert	a) siehe 8.2 dieser Norm b) IEC 61508-2:2000 und IEC 61508-3:1998, 7.9

	Aufgaben	Verweisungen
14	***Validierung* des *PDS(SR)***	Phase 6 des *PDS(SR)*-Sicherheitslebenszyklus (siehe Abschnitt 5.2 dieser Norm)
	a) Bereitstellung aller erforderlichen Informationen für die *Validierung* des *PDS(SR)*	a) siehe 8.3 dieser Norm
	b) vollständige Software und die dazugehörige Dokumentation	
	c) Validierungsprüfungen und -verfahren gemäß Validierungsplan	c) IEC 61508-2:2000, 7.7, Tabellen B.5, B.6 IEC 61508-3:1998, 7.5.2.7, 7.7, 7.9, Tabelle A.7
	d) Dokumentation der Ergebnisse der Validierungsprüfungen	
	e) Zusammenstellen einer geeigneten Dokumentation für eine *Validierung* durch Dritte, falls erforderlich	
15	***PDS(SR)*-Modifikationsverfahren**	
	a) Modifikationsanforderung und Einflussanalyse	a) siehe Abschnitt 10 dieser Norm
	b) geeignete Dokumentation zu allen modifizierten Teilen des *PDS(SR)*	b) IEC 61508-1:1998, 7.16 IEC 61508-2:2000, 7.5.2.5, 7.8 Beispiele in IEC 61508-1:1998, Bild 9
	c) erneute *Verifikation* der modifizierten Teile	
	d) Aktualisierung der Zuverlässigkeitsvorhersage, falls die Modifikation einen Einfluss auf die Fehlertoleranz, die Wahrscheinlichkeit gefahrbringender Fehler, den *Diagnosedeckungsgrad* oder *Ausfälle infolge gemeinsamer Ursache* hat	
	e) erneute *Validierung* mindestens der modifizierten Teile des *PDS(SR)*	
	f) Software-Modifikation	f) IEC 61508-3:1998, 7.1.2.8, 7.5.2.6, 7.6.2, 7.8.2, Tabelle A.8

Anhang B
(informativ)

Beispiel für die Bestimmung der *PFH*

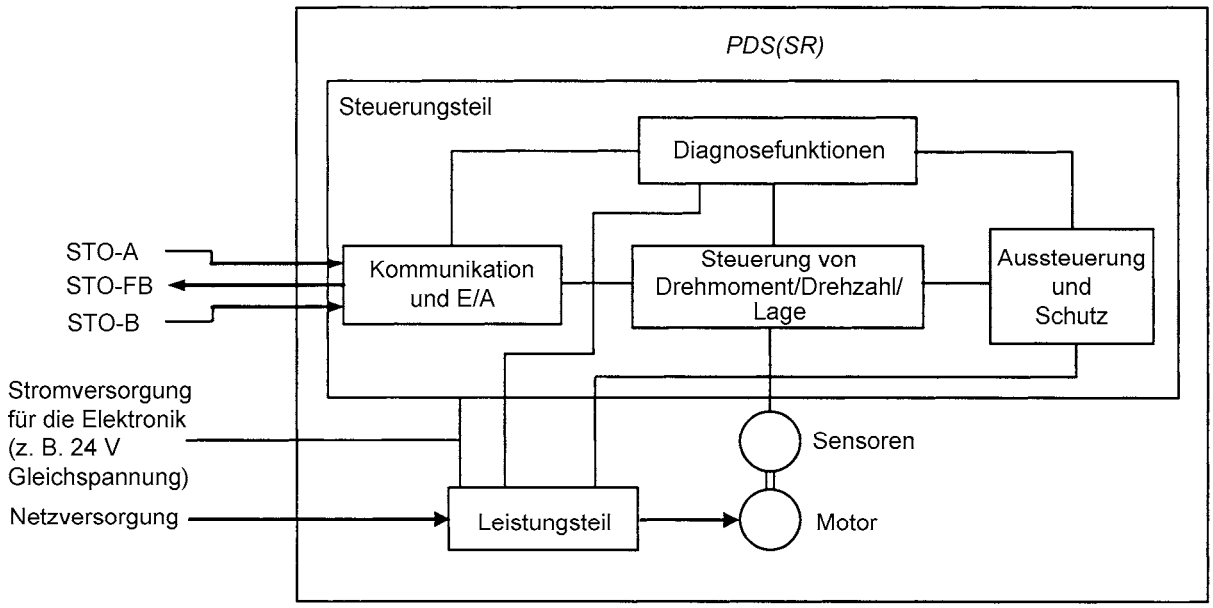
B.1 Allgemeines

In diesem Abschnitt wird die Bestimmung der *PFH* an einem Beispiel-*PDS(SR)* mit der *Sicherheitsfunktion* „Sicher abgeschaltetes Moment (STO)“ beschrieben. Es werden alle notwendigen Anforderungen an das *PDS(SR)* und an die Einzelheiten der internen Struktur des *PDS(SR)* angegeben, damit genau ersichtlich wird, wie der *PFH*-Wert errechnet werden kann.

B.2 Aufbau des Beispiel-*PDS(SR)*

B.2.1 Allgemeines

Das in diesem Abschnitt beschriebene *PDS(SR)* umfasst die *Sicherheitsfunktion* STO, die durch zwei redundante digitale Eingangsschnittstellen ausgelöst wird und ein einzelnes Rückkopplungssignal über eine digitale Ausgangsschnittstelle abgibt (siehe Bild B.1).



ANMERKUNG STO-A: STO-Trigger-Eingangskanal A; STO-B: STO-Trigger-Eingangskanal B; STO-FB: STO-Rückkopplungsausgang

Bild B.1 – Beispiel-*PDS(SR)*

Die Beispielanforderungen sind:

– *SIL* 2;
– Betriebsart mit kontinuierlicher Anforderung.

Innerhalb des *PDS(SR)* wird die *Sicherheitsfunktion* STO zusammen mit der Standardfunktionalität des *PDS(SR)* mit nur wenigen, ausschließlich die *Sicherheitsfunktion* betreffenden Komponenten realisiert.

Durch die interne einkanalige Stromversorgung wird das *PDS(SR)* in zwei unabhängige *Teilsysteme* unterteilt, und zwar in das zweikanalige *Teilsystem* A/B und das *Teilsystem* Stromversorgung/Spannungsüberwachung PS/VM (siehe Bild B.2).

Der *PFH*-Wert der *Sicherheitsfunktion* STO für dieses Beispiel-*PDS(SR)* wird folgendermaßen berechnet:

$$PFH_{PDS(SR)} = PFH_{A/B} + PFH_{PS/VM}$$

Dabei sind $PFH_{A/B}$ und $PFH_{PS/VM}$ die *PFH*-Werte der *Teilsysteme* A/B bzw. PS/VM.

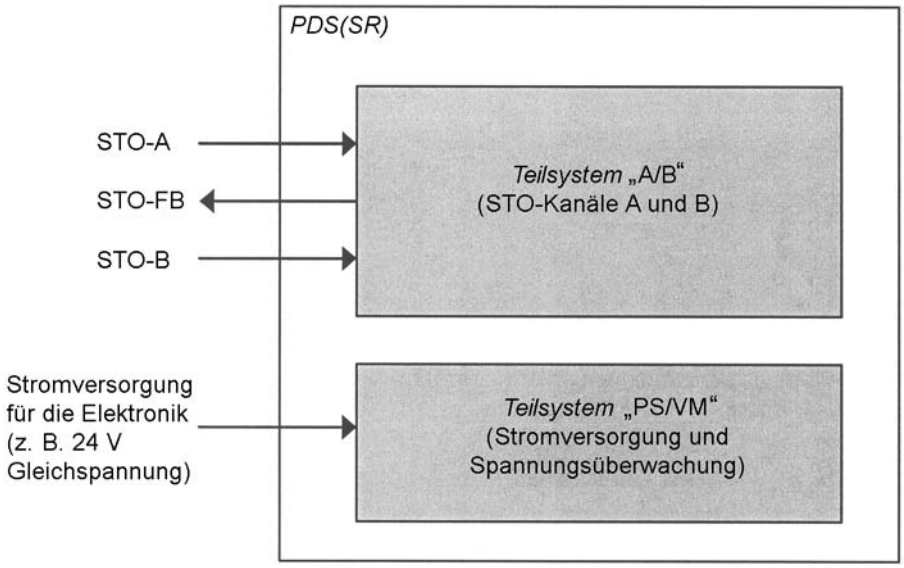


Bild B.2 – *Teilsysteme* des *PDS(SR)*

B.2.2 *Teilsystem* A/B

Die *Sicherheitsfunktion* STO wird mit zwei Kanälen realisiert, um eine Hardware-Fehlertoleranz von 1 zu erreichen, und durch das *Teilsystem* „A/B“ modelliert, für das ein unabhängiger *PFH*-Wert berechnet wird. Die Ausführung des *Teilsystems* führt zu folgenden Systemeigenschaften hinsichtlich der *Sicherheitsfunktion*:

– Typ B (komplexe Hardware);
– Hardware-Fehlertoleranz von 1 (zweikanalige Ausführung).

Aufgrund der Randbedingungen der Architektur des *Teilsystems* des Typs B (siehe 6.2.2.3) muss für *SIL* 2 und eine Hardware-Fehlertoleranz von 1 der *Anteil sicherer Ausfälle (SFF)* mindestens 60 % betragen.

B.2.3 *Teilsystem* PS/VM

Da die interne Stromversorgung (PS) nur einkanalig ausgeführt ist, wird eine Spannungsüberwachung (VM) implementiert. Die interne Stromversorgung und die Spannungsüberwachung werden als getrenntes *Teilsystem* „PS/VM“ modelliert, für das ein unabhängiger *PFH*-Wert berechnet wird. Die Ausführung des *Teilsystems* führt zu folgenden Systemeigenschaften hinsichtlich der *Sicherheitsfunktion*:

– Typ B (komplexe Hardware);
– Hardware-Fehlertoleranz von 0 (einkanalige Ausführung).

Aufgrund der Randbedingungen der Architektur des *Teilsystems* des Typs B (siehe 6.2.2.3) muss für *SIL* 2 und eine Hardware-Fehlertoleranz von 0 der *Anteil sicherer Ausfälle (SFF)* mindestens 90 % betragen.

B.3 Beispielhafte Bestimmung des *PFH*-Wertes eines *PDS(SR)*

B.3.1 *Teilsystem* „A/B“ (Haupt-*Teilsystem*)

B.3.1.1 Zerlegung in Funktionsblöcke

Innerhalb des *PDS(SR)* ist das *Teilsystem* A/B Bestandteil der Ausführung der *Sicherheitsfunktion* STO und besteht aus 2 Kanälen, wie für die Hardware-Fehlertoleranz von 1 erforderlich. Bild B.3 zeigt das Blockdiagramm für das *PDS(SR)*, bei dem die Teile hervorgehoben sind, die an der Ausführung der *Sicherheitsfunktion* STO beteiligt sind.

Zur Berechnung des *PFH*-Wertes wird das *Teilsystem* A/B weiter in Funktionsblöcke zerlegt und die Ausfallrate jedes Funktionsblockes bestimmt. Aufgrund der sehr geringen Anzahl der Bauteile der digitalen Auslöse-Eingangsschaltung und der Abschalt-Schaltung sind nur zwei Funktionsblöcke erforderlich.

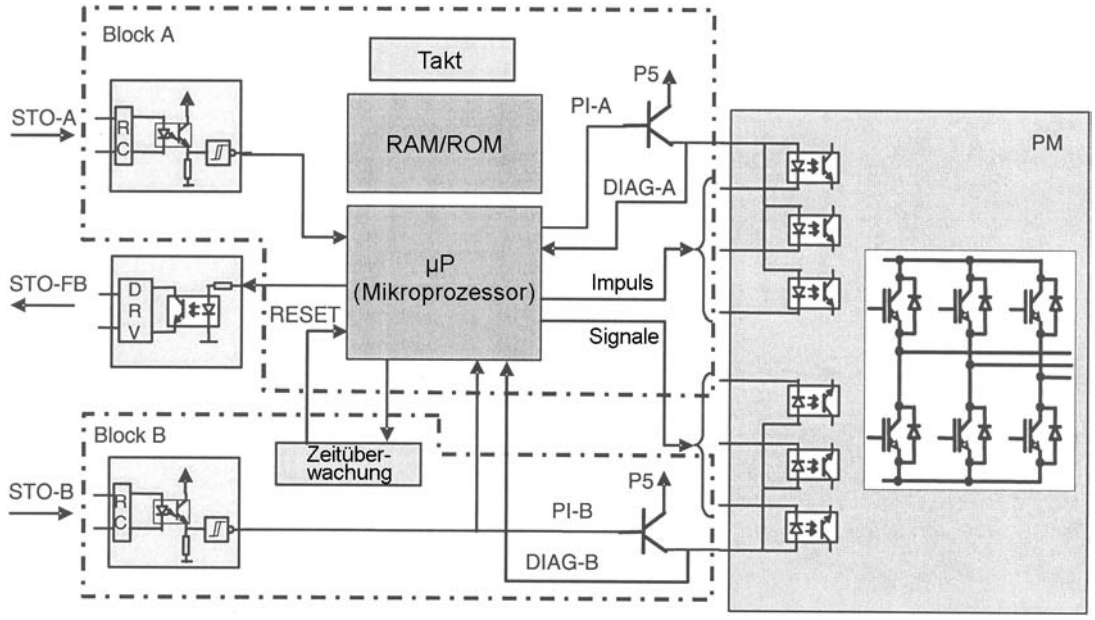


Bild B.3 – Funktionsblöcke des *Teilsystems* A/B

ANMERKUNG 1 P5: Versorgungsspannung 5 V; PI-A(B): Impulssperrkanal A(B); DIAG-A(B): Diagnosesignalkanal A(B); RC: Widerstands-Kondensator-Filter; DRV: Ausgangstreiber; PM: Leistungsteil.

ANMERKUNG 2 Ausfälle von Bauteilen innerhalb des Leistungsteils selbst verursachen keinen Verlust der *Sicherheitsfunktion*. Deshalb darf das Leistungsmodul nicht in ein *Teilsystem* einbezogen werden, das zum *PFH*-Wert beiträgt.

B.3.1.2 Bestimmung der Ausfallraten der Funktionsblöcke

B.3.1.2.1 Analyse der Funktionsblöcke

Für jeden Funktionsblock muss definiert werden, welche Ausfallarten als *gefahrbringende Ausfälle* betrachtet werden müssen. Das Ergebnis liefert Hilfsmittel für die folgende Fehlzustandsart- und -auswirkungsanalyse (en: failure mode and effects analysis, FMEA) der Bauteile des Funktionsblockes.

B.3.1.2.2 FMEA des Bauteils

Mit der FMEA der Bauteile der Schaltung des Funktionsblockes wird ermittelt, welche Bauteile als relevant für die *Sicherheitsfunktion* betrachtet werden, und anschließend muss jeder Ausfallart jedes sicherheitsrelevanten Bauteils unter Anwendung der Kriterien, die bei der Analyse der Funktionsblöcke nach B.3.1.2.1 bestimmt werden, das Attribut „sicher“ oder „gefahrbringend“ zugeordnet werden. Wenn für einfache Bauteile

keine zuverlässigen Daten über den Anteil sicherer oder gefährlicher Ausfallarten vorliegen, führt eine einzelne gefahrbringende Ausfallart dazu, dass jeglicher Ausfall des Bauteils als gefahrbringend betrachtet wird. Nach IEC 61508-6:2000, Anhang C, wird für komplexe Bauteile angenommen, dass ein Anteil von 50 % sicherer und ein Anteil von 50 % gefahrbringender Ausfallarten vorliegt.

Außerdem kennzeichnet die FMEA den Anteil der gefahrbringenden Ausfallrate jedes Bauteils, die durch die zur Verfügung stehende Diagnosefunktionalität ermittelt wird. Für komplexe Bauteile muss der Anteil der erkannten *gefahrbringenden Ausfälle* mit den Tabellen in IEC 61508-2 festgelegt werden. Dieser Anteil definiert die Ausfallrate λ_{DD} (gefahrbringend, erkennbar) und die Ausfallrate λ_{DU} (gefahrbringend, nicht erkennbar) des Bauteils.

Durch Zusammenfassung der sicheren Ausfallraten, der erkennbaren, gefahrbringenden Ausfallraten und der nicht erkennbaren, gefahrbringenden Ausfallraten sämtlicher sicherheitsbezogenen Bauteile des Funktionsblockes wird die Gesamtausfallrate des Funktionsblockes (λ_S, λ_{DD}, λ_{DU}) erzeugt.

B.3.1.2.3 Vereinfachtes Verfahren der Bestimmung der unterschiedlichen Ausfallraten

In Schaltungen mit komplexer Hardware mit einer großen Anzahl von Bauteilen ist die FMEA auf Bauteilbasis nicht immer durchführbar. Dann kann nach einem allgemein anerkannten, vereinfachten Verfahren nach IEC 61508-6:2000, Anhang C, vorgegangen werden.

Die Ausfallrate eines gesamten Funktionsblockes mit einer komplexen Schaltung, die aus der Summe der Ausfallraten aller Bauteile berechnet wird, wird geteilt in einen Anteil von 50 % *sicherer Ausfälle* und einen Anteil von 50 % *gefahrbringender Ausfälle*. Der Anteil der erkannten Ausfälle wird mit den Tabellen in IEC 61508-2 ermittelt.

Dieses Verfahren führt auch zu den Ausfallraten λ_S, λ_{DD} und λ_{DU} des Funktionsblockes.

B.3.1.3 *Anteil sicherer Ausfälle*

Die Ausfallraten der Funktionsblöcke werden nach dem vereinfachten Verfahren in B.3.1.2.3 folgendermaßen ermittelt:

– *Anteil sicherer Ausfälle* an den Ausfällen auf einer Leiterplatte: 50 % (siehe Anmerkung).

ANMERKUNG Der Anteil der *gefahrbringenden Ausfälle* auf einer Leiterplatte beträgt dann auch 50 %.

Der *Diagnosedeckungsgrad (DC)* wird mit den Tabellen in IEC 61508-2 ermittelt.

Tabelle B.1 – Bestimmung des *DC*-Faktors des *Teilsystems* A/B

Verfahren (IEC 61508-2)	Anspruch an den *DC*	Ausführung *Diagnosetests*
Tabelle A.3, Ausfallerkennung durch Überwachung während des Betriebs	90 %	Prüfung redundanter Kanäle durch zyklische Prüfungen
Tabelle A.3, Überwachte Redundanz	99 %/90 %	Prüfung redundanter Kanäle durch zyklische Prüfungen
Tabelle A.4, Selbsttest durch Software (Walking Bit) (ein Kanal)	90 %	Selbsttest des Mikroprozessors
Tabelle A.6, RAM-Prüfung „GALPAT“	90 %	wird vom Mikroprozessor durchgeführt
Tabelle A.10, Programmlauf-Überwachungseinheit (watchdog) mit getrennter Zeitbasis und Zeitfenster (siehe auch Tabelle A.12)	90 %	Entwurf der Programmlauf-Überwachungseinheit (watchdog)
Tabelle A.8, Überprüfung unter Anwendung von Prüfmustern	99 %	wird von der RAM-Prüfung durchgeführt
Tabelle A.15, Kreuzweise Überwachung verschiedener Aktoren	99 %	zyklische Prüfungen überwachen beide Ausschalt-Stellglieder (Aktoren)

– DC_A für Funktionsblock A: 90 % (siehe Tabelle B.1)

– DC_B für Funktionsblock B: 90 % (siehe Tabelle B.1)

Ausfallraten der Schaltung der Funktionsblöcke A und B (realistische Beispielwerte, die in Ausfälle je Stunde (failures in time, FIT) mit der Einheit 10^{-9}/h angegeben werden):

Block A:	λ_A	(Gesamtausfallrate)		450 FIT
	λ_{AS}	(*Anteil sicherer Ausfälle*)	0,5 · 450 FIT	225 FIT
	λ_{AD}	(*Anteil gefahrbringender Ausfälle*)	0,5 · 450 FIT	225 FIT
	λ_{ADD}	$DC_A \cdot \lambda_{AD}$	0,9 · 225 FIT	202,5 FIT
	λ_{ADU}	$(1 - DC_A) \cdot \lambda_{AD}$	(1 – 0,9) · 225 FIT	22,5 FIT
Block B:	λ_B	(Gesamtausfallrate)		70 FIT
	λ_{BS}	(*Anteil sicherer Ausfälle*)	0,5 · 70 FIT	35 FIT
	λ_{BD}	(*Anteil gefahrbringender Ausfälle*)	0,5 · 70 FIT	35 FIT
	λ_{BDD}	$DC_B \cdot \lambda_{BD}$	0,9 · 35 FIT	31,5 FIT
	λ_{BDU}	$(1 - DC_B) \cdot \lambda_{BD}$	(1 – 0,9) · 35 FIT	3,5 FIT

Der *Anteil sicherer Ausfälle* von *Teilsystem* A/B berechnet nach IEC 61508-2:2000, C.1 g), ist:

$$SFF_{A/B} = [(\lambda_{AS} + \lambda_{BS}) + (DC_A \cdot \lambda_{AD}) + (DC_B \cdot \lambda_{BD})] / [(\lambda_{AS} + \lambda_{BS}) + (\lambda_{AD} + \lambda_{BD})]$$

$$= [(225 + 35) + (0{,}9 \cdot 225) + (0{,}9 \cdot 35)] \text{ FIT} / [(225 + 35) + (225 + 35)] \text{ FIT}$$

$$= 494 \text{ FIT} / 520 \text{ FIT}$$

$$SFF_{A/B} = 95\ \%$$

B.3.1.4 Faktor der *Ausfälle infolge gemeinsamer Ursache* $\beta_{A/B}$

Die Ermittlung des Faktors der *Ausfälle infolge gemeinsamer Ursache* $\beta_{A/B}$ erfolgt unter Anwendung von IEC 61508-6:2000, Anhang D, Tabelle D.4.

$\beta_{A/B}$ = 2 %

B.3.1.5 Zuverlässigkeitsmodell (Markov)

Das Zuverlässigkeitsmodell des *Teilsystems* A/B wird als Markov-Modell realisiert, dessen Zustandsgraph im Bild B.4 dargestellt ist.

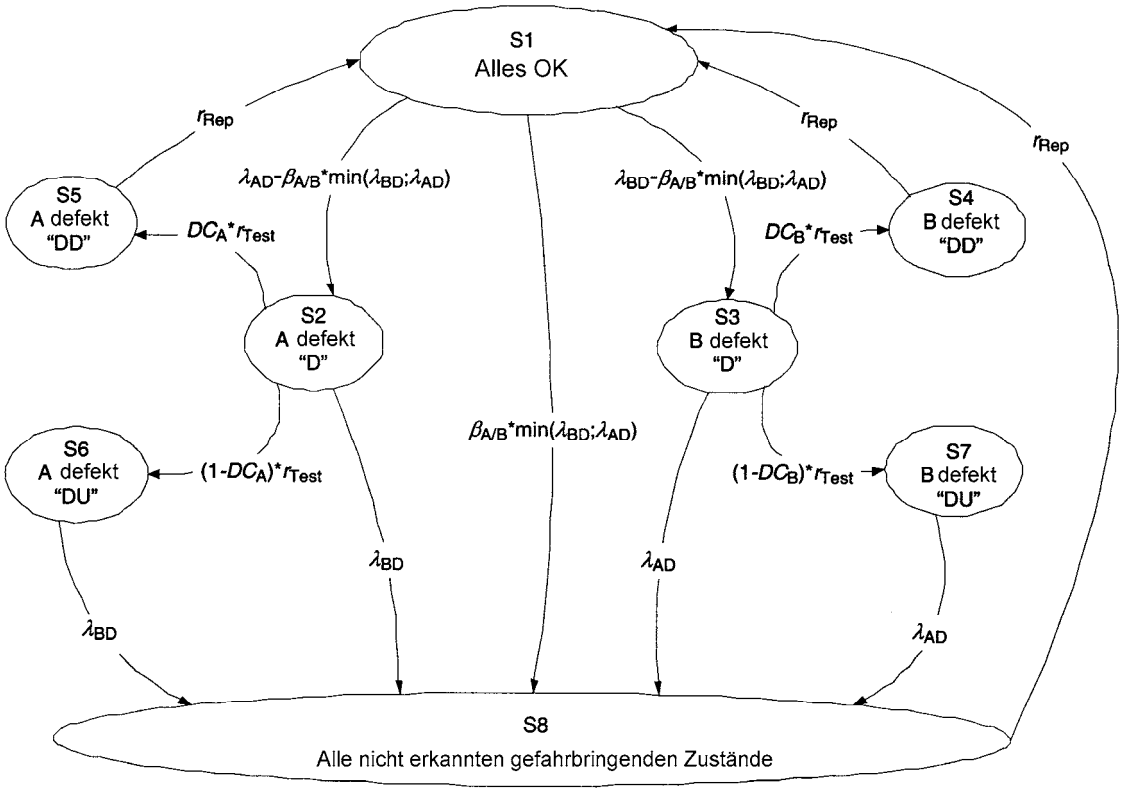


Bild B.4 – Zuverlässigkeitsmodell (Markov) des Teilsystems A/B

ANMERKUNG 1 Aufgrund der Tatsache, dass die Übergangsprozesse, die *Diagnosetests* und durch Ereignisse ausgelösten Reparaturen entsprechen, die notwendigen Bedingungen für die Markov-Technik ihrer Natur nach in einem rein mathematischen Sinn nicht erfüllen, sollte das angegebene Markov-Modell als Näherung betrachtet werden.

ANMERKUNG 2 Das in Bild B.4 dargestellte Modell zeigt detailliert die Einbeziehung von *Diagnosetests*. Aufgrund der üblichen Größe von Ausfallraten und Prüfraten könnte das Modell vereinfacht werden. Im Normalfall ist es nicht von Bedeutung, ob die Prüfrate 1/8 h oder 1/168 h (siehe Tabelle B.2) beträgt.

ANMERKUNG 3 In Bild B.4 bedeutet min(λ_{BD};λ_{AD}) λ_{BD} oder λ_{AD}, je nachdem, welcher Wert kleiner ist.

Das Modell berücksichtigt keine *„sicheren" Ausfälle*, weil diese keinen wichtigen Einfluss auf den *PFH*-Wert besitzen. Für das Modell wird angenommen, dass das *PDS(SR)* nach Erkennung eines Ausfalls vom Prozess abgeschaltet und repariert wird.

Die Rate der *Ausfälle infolge gemeinsamer Ursache* wird durch den Faktor $\beta_{A/B}$ und den kleineren Wert der Raten der *gefahrbringenden Ausfälle* der Funktionsblöcke A und B angegeben (siehe Anmerkung 3).

ANMERKUNG 4 Die Rate gleichzeitiger Ausfälle beider Blöcke kann nie größer sein als die kleinere der beiden Ausfallraten.

Im Zustand S2 ist Funktionsblock A gefahrbringend ausgefallen. Abhängig von der Durchführung des *Diagnosetests* können drei mögliche Zustände folgen:

– S5 folgt, wenn der Ausfall beim *Diagnosetest* erkannt und der Funktionsblock repariert wird;

– S6 folgt, wenn der Ausfall beim *Diagnosetest* nicht erkannt wird;

– S8 folgt, wenn Funktionsblock B ausfällt, bevor der *Diagnosetest* den Ausfall im Funktionsblock A erkennt.

Im Zustand S6 ist Funktionsblock A unerkannt gefahrbringend ausgefallen. S8 folgt, wenn Block B gefahrbringend ausfällt.

Zustand S8 entspricht der gefahrbringenden Situation, in der die *Sicherheitsfunktion* nicht mehr verfügbar und keine Prüfung mehr wirksam ist. Da die Betriebsart mit kontinuierlicher Anforderung des *PDS(SR)* angenommen wird, stellt Zustand S8 auch das „gefahrbringende Ereignis“ dar, das sich durch ein gefahrbringend ausgefallenes *PDS(SR)* ergibt, das mit der Anforderung der *Sicherheitsfunktion* konfrontiert wird.

B.3.1.6 Berechnung des *PFH*-Wertes

In B.3.1.3 und B.3.1.4 sind λ-Werte und *DC*- und β-Faktoren angegeben.

Zusätzliche Voraussetzungen:

– r_{Test} = 1/8 h, 1/24 h, 1/168 h, ... (Rate der *Diagnosetests*);

– r_{Rep} = 1/8 h (Reparaturrate);

– T_{M} = 10 Jahre oder 20 Jahre (*Gebrauchsdauer*).

Zur Ermittlung des *PFH*-Wertes muss der zeitabhängige Verlauf der Wahrscheinlichkeit [$p_{\mathrm{i}}(t)$] jedes Zustandes [Si] des Markov-Modells berechnet werden. Der Anfangs-Wahrscheinlichkeitswert aller Zustände außer von Zustand S1 ist gleich null. Der Anfangs-Wahrscheinlichkeitswert von Zustand S1 ist gleich Eins. Die Berechnung muss bis zur *Gebrauchsdauer* T_{M} erfolgen.

$$PFH_{\mathrm{A/B}} = \frac{1}{T_{\mathrm{M}}} \int_0^{T_{\mathrm{M}}} \left[\beta_{\mathrm{A/B}} \cdot \min(\lambda_{\mathrm{AD}},\lambda_{\mathrm{BD}}) \cdot p_1(t) + \lambda_{\mathrm{BD}} \cdot p_2(t) + \lambda_{\mathrm{AD}} \cdot p_3(t) + \lambda_{\mathrm{BD}} \cdot p_6(t) + \lambda_{\mathrm{AD}} \cdot p_7(t)\right] \mathrm{d}t$$

Die Ergebnisse der Berechnungen für die unterschiedlichen Parameterwerte $\beta_{\mathrm{A/B}}$, r_{Rep}, r_{Test} und T_{M} sind in Tabelle B.2 dargestellt.

Tabelle B.2 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* A/B

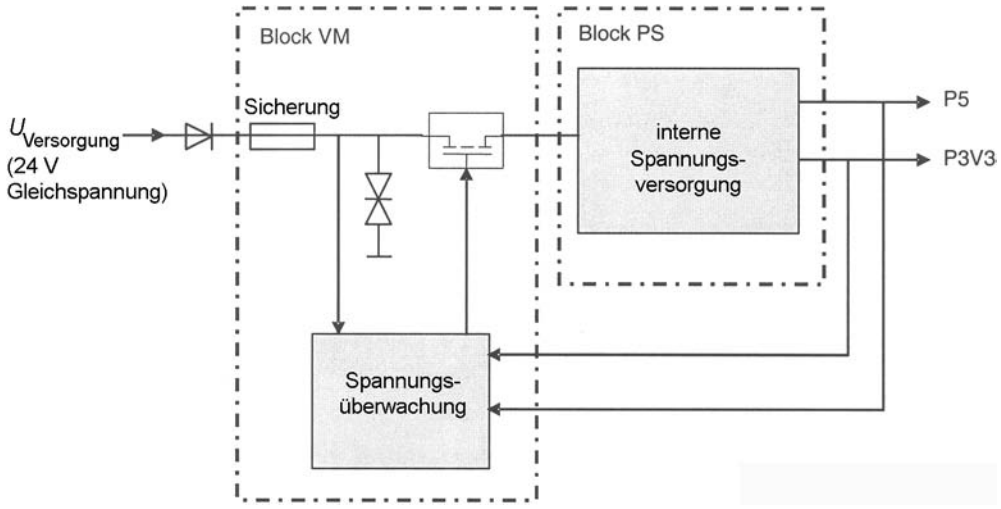
$\beta_{A/B}$	r_{Rep}	r_{Test}	T_M (Jahre)	$PFH_{A/B}$
2 %	1/8 h	1/8 h	10	$6{,}84 \times 10^{-10}$/h
2 %	1/8 h	**1/24 h**	10	$6{,}84 \times 10^{-10}$/h
2 %	1/8 h	**1/168 h**	10	$6{,}86 \times 10^{-10}$/h
2 %	1/8 h	**1/672 h**	10	$6{,}91 \times 10^{-10}$/h
2 %	1/8 h	**1/8760 h**	10	$7{,}72 \times 10^{-10}$/h
2 %	**1/8760 h**	1/8 h	10	$6{,}83 \times 10^{-10}$/h
2 %	1/8 h	1/8 h	**20**	$7{,}38 \times 10^{-10}$/h
2 %	1/8 h	**1/672 h**	20	$7{,}46 \times 10^{-10}$/h
3 %	1/8 h	1/8 h	20	$1{,}05 \times 10^{-9}$/h
5 %	1/8 h	1/8 h	20	$1{,}68 \times 10^{-9}$/h
ANMERKUNG Die fett gedruckten Zahlen geben die gegenüber der vorangegangenen Zeile modifizierten Werte an.				

Die Ergebnisse von Tabelle B.2 zeigen den Einfluss der Prüfrate, der *Gebrauchsdauer* und des Faktors der *Ausfälle infolge gemeinsamer Ursache* auf den *PFH*-Wert. Die Variationen der Parameter sind angegeben, um den Einfluss jedes Parameters auf den *PFH*-Wert zu zeigen.

B.3.2 *Teilsystem* „PS/VM“

B.3.2.1 Zerlegung in Funktionsblöcke

Für die *Sicherheitsfunktion* STO gehört zum *Teilsystem* PS/VM ein Kanal mit zugeordneter Überwachung. Bild B.5 zeigt das *Teilsystem*, das weiter in zwei Funktionsblöcke unterteilt ist, die die interne einzige Spannungsversorgung (PS) und eine Spannungsüberwachungsschaltung (VM) umfassen.



ANMERKUNG P5: Spannungsversorgung 5 V; P3V3: Spannungsversorgung 3,3 V.

Bild B.5 – Funktionsblöcke des *Teilsystems* PS/VM

B.3.2.2 Ausfallraten der Funktionsblöcke

Die Ausfallraten jedes Funktionsblockes werden mit den Verfahren von B.3.2.1 ermittelt.

B.3.2.3 *Anteil sicherer Ausfälle*

Die Ausfallraten der Funktionsblöcke werden nach dem vereinfachten Verfahren in B.3.1.2.3 folgendermaßen ermittelt:

– *Anteil sicherer Ausfälle* an den Ausfällen auf einer Leiterplatte: 50 % (siehe Anmerkung).

ANMERKUNG Der Anteil der *gefahrbringenden Ausfälle* auf einer Leiterplatte beträgt dann auch 50 %.

Der *Diagnosedeckungsgrad (DC)* kann mit den Tabellen in IEC 61508-2:2000, Anhang A, ermittelt werden.

Tabelle B.3 – Bestimmung des *DC*-Faktors des *Teilsystems* PS/VM

Verfahren (IEC 61508-2)	Anspruch an den *DC*	Ausführungsverfahren
Tabelle A.9, Spannungsregelung (sekundär) oder Energieabschaltung mit Sicherheitsabschaltung oder Umschaltung zu einer zweiten Energieversorgung	Hoch	Die Spannungsüberwachung schaltet das *PDS(SR)* ab.

– *DC* für Funktionsblock PS: 99 % (siehe Tabelle B.3)
– *DC* für Funktionsblock VM: 0 % (keine Überwachung der Spannungsüberwachung vorhanden)

Ausfallraten der Schaltungen der Funktionsblöcke PS und VM (realistische Beispielwerte):

Block PS:	λ_{PS}	(Gesamtausfallrate)		250 FIT
	λ_{PSS}	(*Anteil sicherer Ausfälle*)	0,5 · 250 FIT	125 FIT
	λ_{PSD}	(*Anteil gefahrbringender Ausfälle*)	0,5 · 250 FIT	125 FIT
	λ_{PSDD}	$DC_{PS} \cdot \lambda_{PSD}$	0,99 · 125 FIT	123,75 FIT
	λ_{PSDU}	$(1 - DC_{PS}) \cdot \lambda_{PSD}$	0,01 · 125 FIT	1,25 FIT
Block VM:	λ_{VM}	(Gesamtausfallrate)		250 FIT
	λ_{VMS}	(*Anteil sicherer Ausfälle*)	0,5 · 250 FIT	125 FIT
	λ_{VMD}	(*Anteil gefahrbringender Ausfälle*)	0,5 · 250 FIT	125 FIT

Der *Anteil sicherer Ausfälle* von *Teilsystem* PS/VM berechnet nach IEC 61508-2:2000, C.1 g), ist (siehe Anmerkung):

$$SFF_{PS/VM} = [\lambda_{PSS} + (\lambda_{PSD} \cdot DC_{PS})] / \lambda_{PS}$$

$$= [125 + (125 \cdot 0{,}99)] \text{ FIT} / 250 \text{ FIT}$$

$$SFF_{PS/VM} = 99{,}5\ \%$$

ANMERKUNG Der Überwachungsblock trägt nicht zu *SFF* bei.

B.3.2.4 Faktor der *Ausfälle infolge gemeinsamer Ursache* $\beta_{PS/VM}$

Die Ermittlung des Faktors der *Ausfälle infolge gemeinsamer Ursache* $\beta_{PS/VM}$ erfolgt unter Anwendung von IEC 61508-6:2000, Anhang D, Tabelle D.4.

$\beta_{PS/VM} = 2\ \%$

B.3.2.5 Zuverlässigkeitsmodell (Markov)

Das Zuverlässigkeitsmodell des *Teilsystems* PS/VM wird als Markov-Modell realisiert, dessen Zustandsgraph im Bild B.6 dargestellt ist.

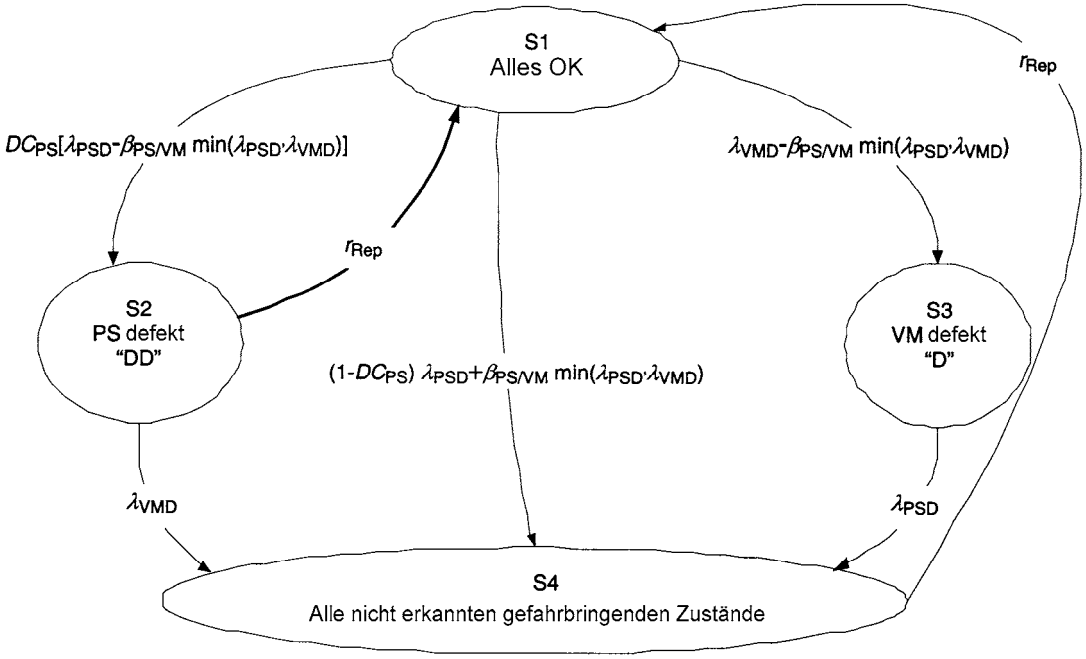


Bild B.6 – Zuverlässigkeitsmodell (Markov) des *Teilsystems* PS/VM

ANMERKUNG 1 Aufgrund der Tatsache, dass die Übergangsprozesse, die *Diagnosetests* und durch Ereignisse ausgelösten Reparaturen entsprechen, die notwendigen Bedingungen für die Markov-Technik ihrer Natur nach in einem rein mathematischen Sinn nicht erfüllen, sollte das angegebene Markov-Modell als Näherung betrachtet werden.

ANMERKUNG 2 Die Spannungsüberwachung liefert eine ununterbrochene Überwachung des Stromversorgungskreises. Aus diesem Grund erscheint im Modell keine Prüfrate. Aufgrund der üblichen Größe der Ausfallraten und der Reparaturraten könnte das Modell vereinfacht werden. Die beschriebene Version dient nur der Veranschaulichung.

Das Modell zeigt die möglichen gefahrbringenden Zustände, aber nicht die sicheren Zustände, die nicht zum *PFH*-Wert beitragen, aber die Komplexität des Modells erhöhen würden. Für das Modell wird angenommen, dass das *PDS(SR)* nach Erkennung eines Ausfalls vom Prozess abgeschaltet und repariert wird.

Die *Ausfälle infolge gemeinsamer Ursache* werden durch den Faktor $\beta_{PS/VM}$ und den kleineren Wert der Raten der *gefahrbringenden Ausfälle* der Funktionsblöcke PS und VM angegeben (siehe Anmerkung).

ANMERKUNG 3 Zur Verdeutlichung: Aufgrund der Tatsache, dass der *Ausfall infolge gemeinsamer Ursache* den Ausfall von Block PS und VM gleichzeitig innerhalb der unterschiedlichen Ausfallraten der Blöcke darstellt, kann die Rate der *Ausfälle infolge gemeinsamer Ursache* nie größer sein als die kleinere der beiden Ausfallraten.

Im Zustand S2 ist Funktionsblock PS erkannt gefahrbringend ausgefallen. Wenn Funktionsblock VM ausfällt, bevor die Reparatur stattfindet, folgt Zustand S4.

Im Zustand S3 ist Funktionsblock VM gefahrbringend ausgefallen, was nicht bemerkt wird, weil keine Überwachung dieses Funktionsblockes erfolgt. Zustand S4 folgt, wenn Funktionsblock PS gefahrbringend ausfällt.

Wenn Funktionsblock PS unerkannt gefahrbringend ausfällt oder beide Funktionsblöcke gleichzeitig ausfallen, folgt Zustand S4 und die *Sicherheitsfunktion* steht nicht mehr zur Verfügung.

Zustand S4 entspricht der gefahrbringenden Situation, in der die *Sicherheitsfunktion* nicht mehr verfügbar und keine Prüfung mehr wirksam ist. Da die Betriebsart mit kontinuierlicher Anforderung des *PDS(SR)* angenommen wird, stellt Zustand S4 auch das „gefahrbringende Ereignis“ dar, das sich durch ein

gefahrbringend ausgefallenes *PDS(SR)* ergibt, das mit der Anforderung der *Sicherheitsfunktion* konfrontiert wird.

B.3.2.6 Berechnung des *PFH*-Wertes

In B.3.2.3 und B.3.2.4 sind λ-Werte und *DC*- und β-Faktoren angegeben.

Zusätzliche Voraussetzungen:

– r_{Rep} = 1/8 h (Reparaturrate);

– T_M = 10 Jahre oder 20 Jahre (*Gebrauchsdauer*).

Zur Ermittlung des *PFH*-Wertes muss der zeitabhängige Verlauf der Wahrscheinlichkeit jedes Zustandes des Markov-Modells berechnet werden. Der Anfangs-Wahrscheinlichkeitswert aller Zustände außer von Zustand S1 ist gleich null. Der Anfangs-Wahrscheinlichkeitswert von Zustand S1 ist gleich Eins. Die Berechnung muss bis zur *Gebrauchsdauer* T_M erfolgen.

$$PFH_{PS/VM} = \frac{1}{T_M}\int_0^{T_M}\left[((1-DC_{PS})\cdot\lambda_{PSD} + \beta_{PS/VM}\cdot\min(\lambda_{PSD},\lambda_{VMD}))\cdot p_1(t) + \lambda_{VMD}\cdot p_2(t) + \lambda_{PSD}\cdot p_3(t)\right]\mathrm{d}t$$

Die Ergebnisse der Berechnungen für die unterschiedlichen Parameterwerte $\beta_{PS/VM}$, r_{Rep} und T_M sind in Tabelle B.4 dargestellt.

Tabelle B.4 – Ergebnisse der Berechnung der *PFH*-Werte für *Teilsystem* PS/VM

$\beta_{PS/VM}$	r_{Rep}	T_M (Jahre)	$PFH_{PS/VM}$
2 %	1/8 h	10	$4{,}39 \times 10^{-9}$/h
2 %	1/8 h	**20**	$5{,}03 \times 10^{-9}$/h
3 %	1/8 h	20	$6{,}25 \times 10^{-9}$/h
5 %	1/8 h	20	$8{,}70 \times 10^{-9}$/h
ANMERKUNG Die fett gedruckten Zahlen geben die gegenüber der vorangegangenen Zeile modifizierten Werte an.			

B.3.3 *PFH*-Wert der Sicherheitsfunktion STO des *PDS(SR)*

Beispiel-*PFH*-Werte mit r_{rep} = 1/8 h und veränderlichem Parameter T_M:

$PFH_{STO/PDS(SR)} = PFH_{A/B} + PFH_{PS/VM}$ (Werte aus den Tabellen B.2 und B.4);

$PFH_{STO/PDS(SR)}$ (T_M = 10 Jahre) = $(6{,}84 \times 10^{-10}$/h + $4{,}39 \times 10^{-9}$/h) = $5{,}074 \times 10^{-9}$/h;

$PFH_{STO/PDS(SR)}$ (T_M = 20 Jahre) = $(7{,}38 \times 10^{-10}$/h + $5{,}03 \times 10^{-9}$/h) = $5{,}768 \times 10^{-9}$/h.

Anhang C
(informativ)

Verfügbare Datenbanken für Ausfallraten

C.1 Datenbanken

Die folgenden Literaturhinweise stellen ein nicht erschöpfendes und in beliebiger Reihenfolge angegebenes Verzeichnis der Datenquellen für Ausfallraten für elektronische und nicht elektronische Bauteile dar. Es sollte beachtet werden, dass diese Quellen nicht immer miteinander übereinstimmen und die Anwendung der Daten deshalb vorsichtig erfolgen sollte.

– IEC/TR 62380; Reliability data handbook – Universalmodell für die Zuverlässigkeitsvorhersage für elektronische Bauelemente, Leiterplatten und Einrichtungen, identisch mit RDF 2000/Reliability Data Handbook, UTE C 80-810, Union Technique de l'Electricité et de la Communication (www.ute-fr.com)

– Siemens-Norm SN 29500, Ausfallraten von Bauelementen (Teile 1 bis 14); kann bezogen werden von: Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739 München

– Reliability Prediction of Electronic Equipment, MIL-HDBK-217E, Department of Defense, Washington DC, 1982

– Reliability Prediction Procedure for Electronic Equipment, Telcordia SR-332, Issue 01, May 2001 (telecom-info.telcordia.com), (Bellcore TR-332, Issue 06)

– EPRD – Electronic Parts Reliability Data (RAC-STD-6100), Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)

– NNPRD-95 – Non-electronic Parts Reliability Data (RAC-STD-6200), Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com)

– British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom (HRD5, last issue)

– Chinese Military Standard GJB/z 299B

– AT&T reliability manual – Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors,l, AT&T Reliability Manual, Van Nostrand Reinhold, 1990, ISBN: 0442318480

– FIDES – (FIDES ist ein neues (Januar 2004) Handbuch für Zuverlässigkeitsdaten, das von einem französischen Industriekonsortium unter der Leitung von French DoD DGA erstellt wurde). FIDES ist auf Anfrage zu beziehen bei fides@innovation.net

– IEEE Gold book – enthält die von IEEE empfohlene Praxis für die Entwicklung von zuverlässigen industriellen und handelsüblichen Energieverteilungssystemen und liefert Daten für die Zuverlässigkeit von Einrichtungen, die in industriellen und handelsüblichen Energieverteilungssystemen angewendet werden; IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Telefon: +1 800 678 IEEE (in den USA und Kanada) +1 732 981 0060 (außerhalb der U.S.A und von Kanada), FAX: +1 732 981 9667 e-mail: customer.service@ieee.org

– IRPH ITALTEL Reliability Prediction Handbook – ist die italienische Version von CNET RDF der italienischen Telekommunikationsunternehmen. Die Normen beruhen auf den gleichen Datensätzen, bei denen nur einige Verfahren und Faktoren geändert sind. Das Italtel IRPH Handbook ist auf Anfrage zu beziehen von: Dr. G. Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italien

– PRISM (RAC/EPRD) – Die PRISM-Software ist von der nachfolgend angegebenen Adresse zu beziehen oder sie ist in verschiedenen handelsüblich verfügbaren Software-Paketen enthalten; The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A

C.2 Hilfreiche Normen für den Bauelementeausfall

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60319, *Presentation and specification of reliability data for electronic components*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60721-1, *Classification of environmental conditions – Part 1: Environmental parameters and their severities*

IEC 61709, *Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion*

Anhang D
(informativ)

Fehlerlisten und Fehlerausschlüsse

D.1 Allgemeines

Die Listen in den Tabellen D.1 bis D.16 beinhalten bestimmte Fehlermodelle und Fehlerausschlüsse mit der zugehörigen Begründung.

Bei der *Validierung* sollten sowohl dauernd auftretende Fehler als auch kurzzeitige Störungen berücksichtigt werden.

Der genaue Zeitpunkt, zu dem der Fehler eintritt, kann kritisch sein. Es sollten eine theoretische Analyse und gegebenenfalls Prüfungen durchgeführt werden, um den ungünstigsten Fall zu ermitteln, z. B. im Stillstand, beim Systemanlauf, während des Betriebs.

D.2 Anmerkungen zu Fehlerausschlüssen

D.2.1 Gültigkeit von Ausschlüssen

Sämtliche Fehlerausschlüsse gelten nur, wenn die Teile innerhalb ihrer festgelegten Bemessungswerte arbeiten.

D.2.2 Zinn-Whisker-Wachstum

Bei der Verwendung von bleifreien Prozessen und Produkten können elektrische Kurzschlüsse aufgrund von Zinn-Whiskern (Nadelkristallen) (siehe Anmerkung 1) auftreten. Wenn der Fehlerausschluss „Kurzschluss …“ beliebiger Bauelemente vorgenommen wird (siehe Anmerkungen 3 und 4), sollte das Risiko von Whiskern betrachtet und bewertet werden (siehe Anmerkung 2).

ANMERKUNG 1 Das Whisker-Wachstum ist eine Erscheinung, die hauptsächlich in Verbindung mit reinen glänzenden Zinn-Oberflächen steht. Die nadelartigen Spitzen können auf mehrere 100 µm Länge anwachsen und elektrische Kurzschlüsse verursachen. Die allgemein geltende Theorie ist, dass Whisker durch Druckspannungen in der Zinnbeschichtung verursacht werden.

ANMERKUNG 2 Bei der Bewertung können folgende Dokumente hilfreich sein:

Test Method for Measuring Whisker Growth on Tin and Tin Alloy Surface Finishes, JESD22A121.01, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, www.jedec.org/download/search/22a121-01.pdf

Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes, JESD201, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, www.jedec.org/DOWNLOAD/search/**JESD201**.pdf

ANMERKUNG 3 Beispiel: Wenn das Risiko von Whisker-Wachstum als hoch angesehen wird, ist der Fehlerausschluss „Kurzschluss eines Widerstandes“ bedeutungslos, weil ein Kurzschluss zwischen den Kontakten dieses Bauelementes in Betracht gezogen werden muss.

ANMERKUNG 4 Whisker auf Leiterplatten wurden bis jetzt noch nicht dokumentiert. Leiterbahnen bestehen üblicherweise aus Kupfer ohne Zinnbeschichtung. Kontaktstellen können mit einer Zinnlegierung beschichtet sein, aber das Herstellungsverfahren scheint die Anfälligkeit für Whisker-Wachstum nicht zu fördern.

D.2.3 Kurzschlüsse von Teilen, die auf Leiterplatten montiert sind

Kurzschlüsse von Teilen, die auf einer Leiterplatte montiert sind, können nur ausgeschlossen werden, wenn der Fehlerausschluss „Kurzschluss zwischen zwei benachbarten Leiterbahnen/Kontaktstellen“ nach Tabelle D.2 vorgenommen wird.

D.3 Fehlermodelle

Tabelle D.1 – Leiter/Kabel

Fehlerannahme	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen Leitern	Kurzschluss zwischen Leitern: – die dauerhaft angeschlossen (fest) und gegen äußere Beschädigung geschützt sind (z. B. durch Kabelkanal, Panzerrohr), oder – in unterschiedlichen Mantelleitungen, oder – innerhalb eines elektrischen Einbauraums (siehe Bemerkung 1)), oder – die einzeln geschirmt sind und eine Erdverbindung besitzen.	1) Sofern sowohl Leiter als auch Einbauraum die zutreffenden Anforderungen erfüllen (siehe IEC 60204-1).
Unterbrechung eines Leiters	Keine	
Kurzschluss zwischen einem beliebigen Leiter und einem ungeschützten leitfähigen Teil oder der Erde oder einer Schutzleiterverbindung	Kurzschluss zwischen Leitern, die sich innerhalb eines elektrischen Einbauraums befinden (siehe Bemerkung 1)).	

Tabelle D.2 – Leiterplatten/Baugruppen

Fehlerannahme	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei benachbarten Leiterbahnen/Kontaktstellen	Kurzschluss zwischen benachbarten Leitern, wenn die Bemerkungen 1) bis 3) zutreffen.	1) Das Leiterplattenmaterial entspricht den Anforderungen von IEC 61800-5-1. 2) Die Kriech- und Luftstrecken sind mindestens nach IEC 60664-1 mit Verschmutzungsgrad 2/Überspannungskategorie III ausgelegt. Wenn beide Leiterbahnen mit einer SELV/PELV-Versorgung gespeist werden, gilt Verschmutzungsgrad 2/Überspannungskategorie II mit einer Mindestluftstrecke von 0,1 mm. 3) Die montierte Leiterplatte wird in ein Gehäuse zum Schutz gegen leitende Verschmutzung eingebaut (z. B ein Gehäuse mit einem Schutzgrad von mindestens IP54) und die bedruckte(n) Seite(n) wird (werden) mit einem alterungsbeständigen Lack oder einer Schutzschicht beschichtet, der/die alle Leiterbahnen abdeckt. ANMERKUNG 1 Erfahrungen haben gezeigt, dass der Lötstopplack als Schutzschicht ausreichend ist. ANMERKUNG 2 Eine weitere Schutzschicht nach IEC 60664-3 kann die Kriech- und Luftstrecken verringern.
Unterbrechung einer Leiterbahn	Keine	–

Tabelle D.3 – Reihenklemme

Fehlerannahme	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei benachbarten Klemmen	Kurzschluss zwischen benachbarten Klemmen, wenn die Bemerkung 1) oder 2) zutrifft.	1) Die verwendeten Anschlüsse und Verbindungen entsprechen den Anforderungen von IEC 61800-5-1. 2) Wird durch konstruktive Maßnahmen gewährleistet, z. B. durch Kunststoff-Schrumpfschlauch über dem Anschlusspunkt.
Unterbrechung einzelner Klemmen	Keine	–

Tabelle D.4 – Mehrpoliger Steckverbinder

Fehlerannahme	Fehlerausschluss	Bemerkungen
Kurzschluss zwischen zwei beliebigen benachbarten Steckerstiften	Kurzschluss zwischen benachbarten Steckerstiften, wenn die Bemerkung 1) zutrifft. Wenn der Steckverbinder auf die Leiterplatte montiert ist, gilt auch Bemerkung 2).	1) Durch Verwendung von Stiften oder anderen geeigneten Mitteln für mehrfach verseilte Leiter. Kriech- und Luftstrecken und alle Luftspalte sollten mindestens nach IEC 60664-1:1992 mit Überspannungskategorie III ausgelegt werden. 2) Die montierte Leiterplatte sollte in ein Gehäuse mit einem Schutzgrad von mindestens IP54 (siehe EN 60529) eingebaut werden und die bedruckte(n) Seite(n) wird (werden) nach IEC 60664-3 mit einem alterungsbeständigen Lack oder einer Schutzschicht beschichtet, der/die alle Leiterpfade abdeckt.
Vertauschter oder falsch eingesteckter Steckverbinder, wenn dies nicht durch mechanische Mittel verhindert wird	Keine	–
Kurzschluss eines Leiters (siehe Bemerkung 3)) mit Erde oder einem leitfähigen Teil oder mit dem Schutzleiter	Keine	3) Die Seele des Kabels wird als Teil des mehrpoligen Steckverbinders betrachtet.
Unterbrechung einzelner Steckverbinderstifte	Keine	–

Tabelle D.5 – Elektromagnetische Bauelemente (z. B. Relais, Schaltrelais)

Fehlerannahme	Fehlerausschluss	Bemerkungen
Alle Kontakte bleiben in Einschaltstellung, wenn die Spule abgeschaltet wird (z. B. durch einen mechanischen Fehler).	Keine	–
Alle Kontakte bleiben in Ausschaltstellung, wenn Energie angelegt wird (z. B. durch einen mechanischen Fehler, Unterbrechung der Spule).	Keine	
Kontakte öffnen nicht.	Keine	
Kontakte schließen nicht.	Keine	
Gleichzeitiger Kurzschluss zwischen den drei Anschlüssen eines Wechselkontaktes	Gleichzeitiger Kurzschluss kann ausgeschlossen werden, wenn die Bemerkungen 1) und 2) zutreffen.	1) Kriech- und Luftstrecken werden mindestens nach IEC 60664-1:1992 mit Verschmutzungsgrad 2/Überspannungskategorie III ausgelegt. 2) Leitfähige Teile, die sich lösen, können die Isolierung zwischen Kontakten und der Spule nicht überbrücken.
Kurzschluss zwischen zwei Kontaktpaaren und/oder zwischen Kontakten und Spulenanschluss	Kurzschluss kann ausgeschlossen werden, wenn die Bemerkungen 1) und 2) zutreffen.	
Gleichzeitiges Schließen von normalerweise offenen (Schließer) und normalerweise geschlossenen (Öffner) Kontakten	Gleichzeitiges Schließen von Kontakten kann ausgeschlossen werden, wenn Bemerkung 3) zutrifft.	3) Es werden zwangsgeführte (oder mechanisch verknüpfte) Kontakte verwendet.

Tabelle D.6 – Transformatoren

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung einer einzelner Wicklung	Keine	–
Kurzschluss zwischen unterschiedlichen Wicklungen	Kurzschluss zwischen unterschiedlichen Wicklungen kann ausgeschlossen werden, wenn die Bemerkungen 1) und 2) zutreffen.	1) Es sollten die Anforderungen der zutreffenden Teile von IEC 61558 erfüllt werden. 2) Zwischen unterschiedlichen Wicklungen muss doppelte oder verstärkte Isolierung oder Schutzschirmung angewendet werden. Es gelten die Prüfungen nach IEC 61558-1, Abschnitt 18. Entsprechende Prüfspannungen sind in IEC 61558-1, Tabelle 8a, angegeben. Kurzschlüsse in Spulen und Wicklungen müssen durch geeignete Schritte vermieden werden, z. B. durch: – Tränken der Spulen, so dass alle Hohlräume zwischen einzelnen Spulen und dem Spulenkörper und dem Kern ausgefüllt werden, und – Verwendung des Wicklungsleiters innerhalb seiner Bemessungswerte für Isolation und hohe Temperatur. 3) Bei einem sekundärseitigen Kurzschluss sollte keine Erwärmung über eine festgelegte Betriebstemperatur auftreten.
Kurzschluss in einer Wicklung	Kurzschluss in einer Wicklung kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft.	
Veränderung des wirksamen Windungsverhältnisses	Der Wechsel des wirksamen Windungszahlenverhältnisses kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft. Als Richtlinie siehe auch Bemerkung 3).	

Tabelle D.7 – Induktivitäten

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung	Keine	–
Kurzschluss	Kurzschluss kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft.	1) Die Spule ist einlagig gewickelt, glasiert oder vergossen, hat axiale Drahtanschlüsse und wird axial montiert.
Zufällige Änderung des Wertes $0{,}5L_N < L < L_N$ + Toleranz wobei L_N der Nennwert der Induktivität ist (siehe Bemerkung 2))	Keine	2) Abhängig von der Bauart können andere Bereiche in Betracht gezogen werden.

Tabelle D.8 – Widerstände

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung	Keine	–
Kurzschluss	Kurzschluss kann ausgeschlossen werden, wenn Bemerkung 1) oder Bemerkung 2) zutrifft.	1) Der Widerstand ist ein Schichtwiderstand oder Drahtwiderstand mit Schutz gegen Abwickeln des Drahtes bei einem Bruch, mit axialen Drahtanschlüssen, axial montiert und lackiert. 2) Ein oberflächenmontierbarer Widerstand muss ein Dünnschicht-Metallwiderstand sein. Das Gehäuse muss vom Typ MELF, miniMELF oder µMELF sein.
Zufällige Änderung des Wertes $0{,}5R_N < R < 2R_N$ wobei R_N der Nennwert des Widerstandes ist (siehe Bemerkung 3))	Keine	3) Abhängig von der Bauart können andere Bereiche in Betracht gezogen werden.

Tabelle D.9 – Widerstandsnetzwerke

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung	Keine	–
Kurzschluss zwischen zwei beliebigen Anschlüssen	Keine	
Kurzschluss zwischen beliebigen Anschlüssen	Keine	
Zufällige Änderung des Wertes $0{,}5R_N < R < 2R_N$ wobei R_N der Nennwert des Widerstandes ist (siehe Bemerkung 1))	Keine	1) Abhängig von der Bauart können andere Bereiche in Betracht gezogen werden.

Tabelle D.10 – Potentiometer

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Keine	–
Kurzschluss zwischen allen Anschlüssen	Keine	
Kurzschluss zwischen zwei Anschlüssen	Keine	
Zufällige Änderung des Wertes $0{,}5R_P < R < 2R_P$ wobei R_P der Nennwert des Widerstandes ist (siehe Bemerkung 1))	Keine	1) Abhängig von der Bauart können andere Bereiche in Betracht gezogen werden.

Tabelle D.11 – Kondensatoren

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung	Keine	–
Kurzschluss	Keine	
Zufällige Änderung des Wertes $0{,}5C_N < C < C_N$ + Toleranz wobei C_N der Nennwert der Kapazität ist (siehe Bemerkung 1))	Keine	1) Abhängig von der Bauart können andere Bereiche in Betracht gezogen werden.
Änderung des Wertes tan δ	Keine	–

Tabelle D.12 – Diskrete Halbleiter (z. B. Dioden, Zener-Dioden, Transistoren, Triacs, GTO-Thyristoren, IGBTs, Spannungsregler, Schwingquarze, Fototransistoren, Leuchtdioden (LEDs))

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung eines Anschlusses	Keine	–
Kurzschluss zwischen zwei Anschlüssen	Keine	
Kurzschluss zwischen allen Anschlüssen	Keine	
Änderung von Kenndaten	Keine	
Explosion des Bauelementengehäuses	Kann ausgeschlossen werden, wenn Bemerkung 1) zutrifft.	1) Die Kurzschlussleistung der Versorgung wird auf die Fähigkeit des Bauelementen-gehäuses begrenzt.

Tabelle D.13 – Optokoppler

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung eines einzelnen Anschlusses	Keine	–
Kurzschluss zwischen zwei beliebigen Eingangsanschlüssen	Keine	
Kurzschluss zwischen zwei beliebigen Ausgangsanschlüssen	Keine	
Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	Kurzschluss zwischen Ein- und Ausgang kann ausgeschlossen werden, wenn die Bemerkungen 1) und 2) zutreffen	1) Der Optokoppler ist nach Überspannungskategorie III von IEC 61800-5-1 und IEC 60664:1992, Tabelle 1, gebaut. Bei Verwendung einer SELV/PELV-Versorgung gilt Verschmutzungsgrad 2 / Überspannungskategorie II. 2) Es werden Maßnahmen ergriffen, die sicherstellen, dass ein interner Ausfall des Optokopplers nicht zu einer überhöhten Temperatur seines Isolierstoffs führen kann.

Tabelle D.14 – Nicht programmierbare integrierte Schaltkreise

Fehlerannahme	Fehlerausschluss	Bemerkungen
Unterbrechung jedes einzelnen Anschlusses	Keine	–
Kurzschluss zwischen zwei beliebigen Anschlüssen	Keine	
Stuck-at-Fehler (d. h. Kurzschluss zu 1 und 0 bei isoliertem Eingang oder unterbrochenem Ausgang). Statisches „0“- und „1“-Signal an allen Ein- und Ausgängen, entweder einzeln oder gleichzeitig	Keine	
Störschwingung der Ausgänge	Keine	
Veränderung von Kennwerten (z. B. Eingangs-/Ausgangsspannung analoger Geräte)	Keine	
ANMERKUNG In dieser Norm werden ICs mit weniger als 1 000 Gattern und/oder weniger als 24 Anschlüssen, Operationsverstärker, Schieberegister und Hybridmodule als nicht komplex betrachtet. Diese Definition ist willkürlich.		

Tabelle D.15 – Programmierbare und/oder komplexe integrierte Schaltkreise

Fehlerannahme	Fehlerausschluss	Bemerkungen
Fehler der gesamten Funktion oder eines Teils der Funktion	Keine	–
Unterbrechung jedes einzelnen Anschlusses	Keine	
Kurzschluss zwischen zwei Anschlüssen	Keine	
Stuck-at-Fehler (d. h. Kurzschluss zu 1 und 0 bei isoliertem Eingang oder unterbrochenem Ausgang). Statisches „0“- und „1“-Signal an allen Ein- und Ausgängen, entweder einzeln oder gleichzeitig	Keine	
Störschwingung der Ausgänge	Keine	
Veränderung von Kennwerten (z. B. Eingangs-/Ausgangsspannung analoger Geräte)	Keine	
unerkannte Fehler in der Hardware, die wegen der Komplexität des integrierten Schaltkreises nicht entdeckt werden	Keine	
ANMERKUNG In dieser Norm werden ICs als komplex betrachtet, wenn sie mehr als 1 000 Gatter und/oder mehr als 24 Anschlüsse besitzen. Diese Definition ist willkürlich. Die Analyse sollte zusätzliche Fehler aufzeigen, die berücksichtigt werden sollten, wenn sie den Betrieb der *Sicherheitsfunktion* beeinflussen.		

Tabelle D.16 – Bewegungs- und Lagesensoren

Fehlerannahme	Fehlerausschluss	Bemerkungen
Allgemeines		
Kurzschluss zwischen zwei beliebigen Leitern der Anschlussleitung	Es gilt Tabelle D.1.	
Unterbrechung eines beliebigen Leiters der Anschlussleitung	Keine	
Statisches „0“- oder „1“-Signal an Ein- und Ausgängen, einzeln oder an mehreren Ein-/Ausgängen gleichzeitig	Keine	
Unterbrechung oder hochohmiger Zustand an einem einzelnen oder an mehreren Ein-/Ausgängen gleichzeitig	Keine	
Verringerung oder Erhöhung der Ausgangsamplitude	Keine	
Störschwingungen an einem oder an mehreren Ausgängen[a]	Keine	Schwingungen an mehreren Ausgängen werden als phasengleich betrachtet.
Änderung der Phasenverschiebung zwischen Ausgangssignalen[a]	Keine	z. B. durch eine verschmutzte Codescheibe

Tabelle D.16 – Bewegungs- und Lagesensoren *(fortgesetzt)*

Fehlerannahme	Fehlerausschluss	Bemerkungen
Befestigung löst sich im Stillstand: – Sensorgehäuse löst sich vom Motorgehäuse – Sensorwelle löst sich von der Motorwelle	Durchführung einer FMEA und Nachweis der Dauerfestigkeit der mechanischen Befestigungen	Ausgangssignal entspricht Drehzahl Null Wenn der Fehlerausschluss angewendet wird, hält die Konstruktion der Befestigung des Sensorgehäuses am Motorgehäuse und der Sensorwelle an der Motorwelle gewöhnlich einem Faktor einer etwa 20fachen Überbeanspruchung stand und es sollten besondere Instandhaltungs-informationen angegeben werden.
Befestigung löst sich während der Bewegung: – Sensorgehäuse löst sich vom Motorgehäuse – Sensorwelle löst sich von der Motorwelle	Durchführung einer FMEA und Nachweis der Dauerfestigkeit der mechanischen Befestigungen	Mögliche Auswirkungen: – statischer Versatz der Sensorwelle; – dynamischer Schlupf der Sensorwelle; – Ausgangssignal ist falsch / entspricht einer Drehzahl von Null Wenn der Fehlerausschluss angewendet wird, hält die Konstruktion der Befestigung des Sensorgehäuses am Motorgehäuse und der Sensorwelle an der Motorwelle gewöhnlich einem Faktor einer etwa 20fachen Überbeanspruchung stand und es sollten besondere Instandhaltungs-informationen angegeben werden.
Maßverkörperung löst sich[a] (z. B. optische Codierscheibe)	Keine	Ausgang liefert falsche Positionsinformation
Kein Licht von der Sendediode	Keine	
Zusätzliche Anforderungen für Drehgeber mit sin/cos-Ausgangssignalen, analoge Signalerzeugung		
Statisches Signal an Ein- und Ausgängen, einzeln oder an mehreren Signalen, Amplitude im Bereich der Spannungsversorgung	Keine	
Änderung der Signalform	Keine	z. B. kein sin/cos-Signal, Signaloffset
Vertauschen des sin- und cos-Ausgangssignals	Fehlerausschluss zulässig, wenn keine elektronischen Bauelemente verwendet werden, um ein Ausgangssignal von mehreren Quellen auszuwählen.	
Zusätzliche Anforderungen für Inkremental-Drehgeber mit Rechteck-Ausgangssignalen		
Störschwingung am Ausgang	Keine	
Ausgangssignal bricht ab	Keine	z. B. aufgrund einer zerkratzten Codescheibe
Nullimpuls fällt aus, ist zu kurz, zu lang oder mehrfach	Keine	z. B. aufgrund einer mechanischen Beschädigung
Zusätzliche Anforderungen für Drehgeber mit inkrementellen und absoluten Signalen		
Gleichzeitig falsche Positionsänderung vom inkrementellen und vom absoluten Signal	Fehlerausschluss, wenn die inkrementellen und die absoluten Daten unabhängig voneinander erzeugt werden.	Zutreffend z. B. für sin/cos-Geber mit zusätzlichen Ausgängen für Absolutwert und/oder Kommutierung

Tabelle D.16 – Bewegungs- und Lagesensoren *(fortgesetzt)*

Fehlerannahme	Fehlerausschluss	Bemerkungen
Zusätzliche Anforderungen für Drehgeber mit Rechnerschnittstelle		
Übertragungssfehler: – Wiederholung; – Verlust; – Einfügung; – falsche Abfolge; – Nachrichtenverfälschung; – Verzögerung	Keine	Entspricht dem Fehlermodell für Bussysteme
Zusätzliche Anforderungen für Multiturn-Drehgeber		
Falsche Anzahl der Umdrehungen	Keine	Kann ohne Auswirkung auf Singleturn-Signale sein
Zusätzliche Anforderungen für Drehgeber mit synthetisch generierten Ausgangssignalen		
Beliebige Verfälschung des Ausgangs-signals	Keine	
Zusätzliche Anforderungen für Drehgeber mit Positionsermittlung durch Zähler		
Falscher Positionswert aufgrund fehlerhafter Zählung	Keine	
Zusätzliche Anforderungen für Lineargeber		
Befestigung des Lesekopfes gebrochen	Durchführung einer FMEA und Nachweis der Dauerfestigkeit der mechanischen Befestigungen	Wenn der Fehlerausschluss gefordert wird, hält die Sensorbefestigung üblicherweise den Überbeanspruchungen stand und es sollten besondere Instandhaltungs-informationen gegeben werden.
Statischer Versatz der Maßverkörperung[a] (z. B. optischer Codestreifen)	Keine	
Beschädigte Maßverkörperung[a] (z. B. optischer Codestreifen)	Keine	Impulsform ist verändert, Impulse bleiben aus bei Inkrementalgebern
Zusätzliche Anforderungen für Resolver mit Signalverarbeitung/Referenzgenerator		
Übersprechen der Referenzfrequenz	Keine	
– zentraler Timer fällt aus – kein Conversion Start für A/D-Wandler – Sample & Hold erfolgt zum falschen Zeitpunkt	Keine	
A/D-Wandler erzeugt falsche Werte	Keine	z. B. durch Übermodulation infolge einer zu hohen Referenzspannung oder elektro-magnetischer Beeinflussung
A/D-Wandler erzeugt keine Werte	Keine	
Referenzgenerator liefert keine Frequenz	Keine	
Referenzgenerator liefert falsche Frequenz	Keine	
Referenzgenerator liefert kein periodisches Referenzsignal	Keine	
Verstärkungsfehler bei der Signal-verarbeitung (Referenz-, sin-, cos-Signal), Oszillieren	Keine	
Magnetische Beeinflussung am Einbauort	Ausreichende Abschirmung für den Einbauort	z. B. durch Magnetfeld einer elektromagnetischen Bremse
[a] Gilt nicht für Resolver.		
ANMERKUNG Diese Tabelle wurde unter Annahme des Einsatzes von optischen Sensoren geschrieben. Wenn andere Sensoren (z. B. induktive Sensoren) verwendet werden, gelten entsprechende Fehler.		

Literaturhinweise

IEC 60050-191:1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60300-3-1, *Application guide – Analysis techniques for dependability: Guide on methodology*

ANMERKUNG Harmonisiert als EN 60300-3-1:2004 (nicht modifiziert).

IEC 60664-1:1992, *Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests*

ANMERKUNG Harmonisiert als EN 60664-1:2003 (nicht modifiziert).

IEC 60664-3, *Insulation coordination for equipment within low-voltage systems – Part 3: Use of coating, potting or moulding for protection against pollution*

ANMERKUNG Harmonisiert als EN 60664-3:2003 (nicht modifiziert).

IEC 61025, *Fault tree analysis (FTA)*

ANMERKUNG Harmonisiert als EN 61025:2007 (nicht modifiziert).

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and boolean methods*

ANMERKUNG Harmonisiert als EN 61078:2006 (nicht modifiziert).

IEC 61165, *Application of Markov techniques*

ANMERKUNG Harmonisiert als EN 61165:2006 (nicht modifiziert).

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

ANMERKUNG Harmonisiert als EN 61508-4:2001 (nicht modifiziert).

IEC 61511 (alle Teile), *Functional safety – Safety instrumented systems for the process industry sector*

ANMERKUNG Harmonisiert in der Reihe EN 61511 (nicht modifiziert).

IEC 61511-1, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

ANMERKUNG Harmonisiert als EN 61511-1:2004 (nicht modifiziert).

IEC 61513, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*

IEC 61558 (alle Teile), *Safety of power transformers, power supplies, reactors and similar products*

ANMERKUNG Harmonisiert in der Reihe EN 61558 (teilweise modifiziert).

IEC 61558-1:2005, *Safety of power transformers, power supplies, reactors and similar products – Part 1: General requirements and tests*

ANMERKUNG Harmonisiert als EN 61558-1:2005 (nicht modifiziert).

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

ANMERKUNG Harmonisiert als EN 62061:2005 (nicht modifiziert).

IEC 62280-1, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

IEC 62280-2, *Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems*

ISO 13849-1, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ANMERKUNG Harmonisiert als EN ISO 13849-1:2006 (nicht modifiziert).

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

ANMERKUNG Harmonisiert als EN ISO 13849-2:2003 (nicht modifiziert).

ENV 50129, *Railway applications – Safety-related electronic systems for signalling*

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

Anhang ZA
(normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

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).

ANMERKUNG Wenn internationale Publikationen durch gemeinsame Abänderungen geändert wurden, durch (mod) angegeben, gelten die entsprechenden EN/HD.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 60204-1 (mod)	– [1)]	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	EN 60204-1	2006 [2)]
IEC 61508	Reihe	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	Reihe
IEC 61508-1 + Corr. Mai	1998 1999	Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 1: General requirements	EN 61508-1	2001
IEC 61508-2	2000	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001
IEC 61508-3 + Corr. April	1998 1999	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements	EN 61508-3	2001
IEC 61508-5	– [1)]	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels	EN 61508-5	2001 [2)]
IEC 61508-6	2000	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3	EN 61508-6	2001
IEC 61508-7	2000	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures	EN 61508-7	2001

[1)] Undatierte Verweisung.

[2)] Zum Zeitpunkt der Veröffentlichung dieser Norm gültige Ausgabe.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 61800-1	– [1)]	Adjustable speed electrical power drive systems – Part 1: General requirements – Rating specifications for low voltage adjustable speed d.c. power drive systems	EN 61800-1	1998 [2)]
IEC 61800-2	– [1)]	Adjustable speed electrical power drive systems – Part 2: General requirements – Rating specifications for low voltage adjustable frequency a.c. power drive systems	EN 61800-2	1998 [2)]
IEC 61800-3	– [1)]	Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods	EN 61800-3	2004 [2)]
IEC 61800-4	– [1)]	Adjustable speed electrical power drive systems – Part 4: General requirements – Rating specifications for a.c. power drive systems above 1 000 V a.c. and not exceeding 35 kV	EN 61800-4	2003 [2)]
IEC 61800-5-1	2003	Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy	EN 61800-5-1 [3)]	2003
IEC 62280	Reihe	Railway applications – Communication, signalling and processing systems	–	–

[3)] EN 61800-5-1 wurde ersetzt durch EN 61800-5-1:2007, die auf IEC 61800-5-1:2007 basiert.

Anhang ZZ
(informativ)

Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien

Anhang ZZA
(informativ)

Zusammenhang mit grundlegenden Anforderungen von Richtlinie 98/37/EG

Diese Europäische Norm wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde. Diese Europäische Norm deckt innerhalb ihres Anwendungsbereiches die folgenden grundlegenden Anforderungen ab, die in Anhang I der EG-Richtlinie 98/37/EG enthalten sind:

– 1.2.1;

– 1.2.7.

Die Übereinstimmung mit dieser Norm ist eine Möglichkeit, die Konformität mit den festgelegten grundlegenden Anforderungen der betreffenden Richtlinie zu erklären.

WARNHINWEIS: Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Anforderungen und weitere EG-Richtlinien anwendbar sein.

Anhang ZZB
(informativ)

Zusammenhang mit grundlegenden Anforderungen von Richtlinie 2006/42/EG

Diese Europäische Norm wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde. Diese Europäische Norm deckt innerhalb ihres Anwendungsbereiches die folgenden grundlegenden Anforderungen ab, die in Anhang I der EG-Richtlinie 2006/42/EG enthalten sind:

– 1.2.1.

Die Übereinstimmung mit dieser Norm ist eine Möglichkeit, die Konformität mit den festgelegten grundlegenden Anforderungen der betreffenden Richtlinie zu erklären.

WARNHINWEIS: Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Anforderungen und weitere EG-Richtlinien anwendbar sein.