

	DIN EN 61800-5-2 (VDE 0160-105-2)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
<p>ICS 29.200</p> <p>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</p> <p>Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (IEC 61800-5-2:2007); German version EN 61800-5-2:2007</p> <p>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</p> <p>Gesamtumfang 73 Seiten</p> <p>DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE</p>		

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 61800-5-2 (VDE 0160-105-2):2008-04

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

**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

© 2007 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

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 <i>Sicherheitsfunktionen</i>	14
4.1 Allgemeines	14
4.2 <i>Sicherheitsfunktionen</i>	14
4.2.1 Grenzwerte	14
4.2.2 Stoppfunktionen.....	15
4.2.3 Andere <i>Sicherheitsfunktionen</i>	16
5 Management der <i>funktionalen Sicherheit</i>	17
5.1 Ziel	17
5.2 Sicherheitslebenszyklus eines <i>PDS(SR)</i>	17
5.3 Planung der <i>funktionalen Sicherheit</i>	18
5.4 <i>Spezifikation der Sicherheitsanforderungen</i> (SRS) für ein <i>PDS(SR)</i>	20
5.4.1 Allgemeines	20
5.4.2 Spezifikation der Anforderungen an die <i>Sicherheitsfunktionen</i>	20
5.4.3 Spezifikation der Anforderungen zur <i>Sicherheitsintegrität</i>	21
6 Anforderungen an Entwurf und Entwicklung eines <i>PDS(SR)</i>	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 <i>Sicherheitsintegrität</i> und Fehlererkennung.....	22
6.1.5 <i>Sicherheitsfunktionen</i> und nicht sicherheitsbezogene Funktionen	22
6.1.6 Anzuwendender <i>SIL</i>	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 <i>PDS(SR)</i> -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 <i>Anteils sicherer Ausfälle (SFF)</i>	27
6.2.4 Anforderungen an die systematische <i>Sicherheitsintegrität</i> eines <i>PDS(SR)</i> und von <i>PDS(SR)-Teilsystemen</i>	28
6.2.5 Anforderungen an die elektromagnetische Störfestigkeit eines <i>PDS(SR)</i>	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 <i>PDS(SR)</i>	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 <i>PDS(SR)</i>	33
8 <i>Verifikation</i> und <i>Validierung</i>	35
8.1 Allgemeines	35
8.2 <i>Verifikation</i>	35
8.3 <i>Validierung</i>	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 <i>PFH</i>	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

Bild 1 – Funktionselemente eines <i>PDS(SR)</i>	8
Bild 2 – Entwicklungslebenszyklus eines <i>PDS(SR)</i>	18
Bild 3 – Architekturen der Datenkommunikation: a) Weißer Kanal, b) Schwarzer Kanal	32
Bild B.1 – Beispiel- <i>PDS(SR)</i>	42
Bild B.2 – <i>Teilsysteme</i> des <i>PDS(SR)</i>	43
Bild B.3 – Funktionsblöcke des <i>Teilsystems</i> A/B	44
Bild B.4 – Zuverlässigkeitsmodell (Markov) des <i>Teilsystems</i> A/B	47
Bild B.5 – Funktionsblöcke des <i>Teilsystems</i> PS/VM	49
Bild B.6 – Zuverlässigkeitsmodell (Markov) des <i>Teilsystems</i> PS/VM	51
 Tabelle 1 – Alphabetisches Verzeichnis der Begriffe	 9
Tabelle 2 – <i>Sicherheits-Integritätslevel</i> : Ausfallgrenzwerte für eine <i>Sicherheitsfunktion</i> eines <i>PDS(SR)</i>	23
Tabelle 3 – Hardware- <i>Sicherheitsintegrität</i> : Strukturelle Einschränkungen der Architektur für sicherheitsbezogene <i>Teilsysteme</i> des Typs A	27
Tabelle 4 – Hardware- <i>Sicherheitsintegrität</i> : Strukturelle Einschränkungen der Architektur für sicherheitsbezogene <i>Teilsysteme</i> des Typs B	27
Tabelle B.1 – Bestimmung des <i>DC</i> -Faktors des <i>Teilsystems</i> A/B	46
Tabelle B.2 – Ergebnisse der Berechnung der <i>PFH</i> -Werte für <i>Teilsystem</i> A/B	49
Tabelle B.3 – Bestimmung des <i>DC</i> -Faktors des <i>Teilsystems</i> PS/VM	50
Tabelle B.4 – Ergebnisse der Berechnung der <i>PFH</i> -Werte für <i>Teilsystem</i> 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 *Sicherheitsfunktionen* 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.

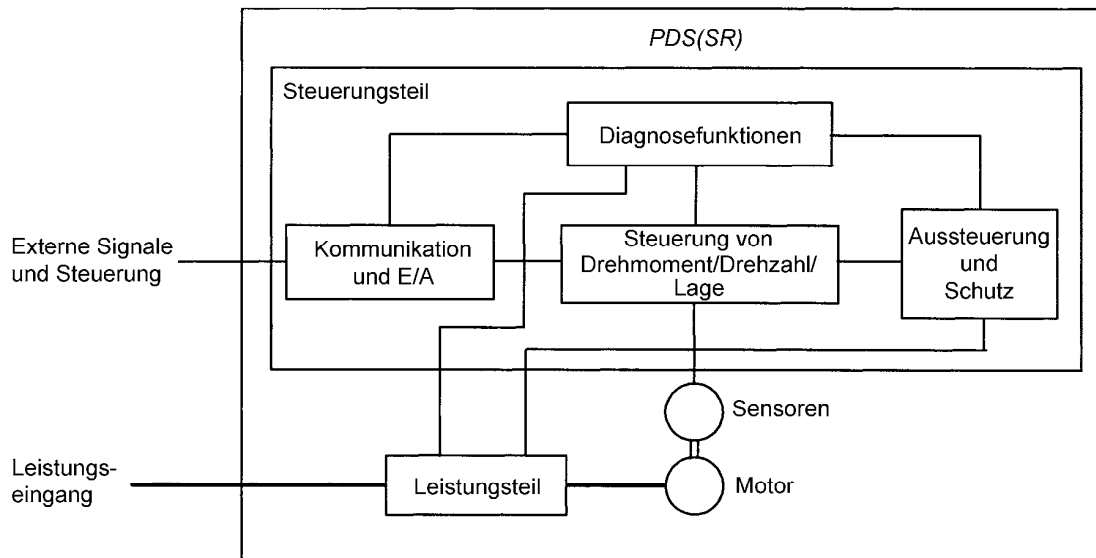


Bild 1 – Funktionselemente eines PDS(SR)

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

gefährbringender 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 gefährbringenden 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 *gefährbringenden Ausfällen* λ_{DD} zur Summe aller *gefährbringenden 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 gefährbringender 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 *Gefährdungen* 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 *Betriebsarten* 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-Tests* 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 *gefährbringender Ausfälle* eines *PDS(SR)*-*Teilsystems* 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 gefährbringender 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 Betriebes, 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 -abbremung 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.

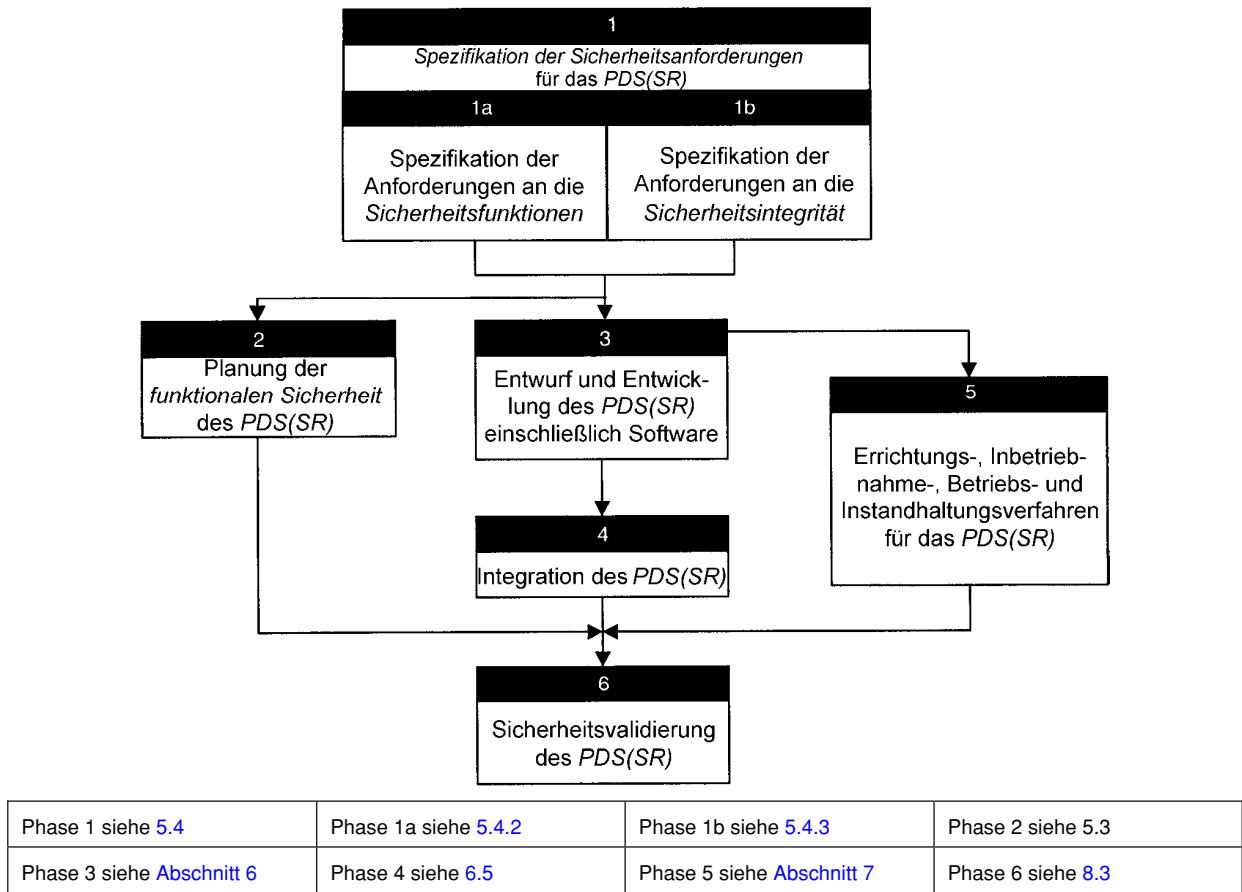


Bild 2 – Entwicklungslebenszyklus eines PDS(SR)

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: