

	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
ICS 29.160.30 Ersatz für DIN EN 61800-5-2 (VDE 0160-105-2):2008-04 Siehe Anwendungsbeginn Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-2: Anforderungen an die Sicherheit – Funktionale Sicherheit (IEC 61800-5-2:2016); Deutsche Fassung EN 61800-5-2:2017 Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (IEC 61800-5-2:2016); German version EN 61800-5-2:2017 Entraînements électriques de puissance à vitesse variable – Partie 5-2: Exigences de sécurité – Fonctionnelle (IEC 61800-5-2:2016); Version allemande EN 61800-5-2:2017 Gesamtumfang 102 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-05-23 angenommene Europäische Norm als DIN-Norm ist 2017-11-01.

Für **DIN EN 61800-5-2 (VDE 0160-105-2):2008-04** besteht eine Übergangsfrist bis 2020-04-28.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61800-5-2 (VDE 0160-105-2):2014-06.

Für dieses Dokument ist das nationale Arbeitsgremium K 226 „Ausrüstung von Starkstromgeräten und -anlagen mit elektronischen Betriebsmitteln“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in 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 (stability 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.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber **DIN EN 61800-5-2 (VDE 0160-105-2):2008-04** wurden folgende Änderungen vorgenommen:

- a) Ergänzung einer Begründung im **Abschnitt 1** „Anwendungsbereich“ dafür, warum die Betriebsart mit niedriger Anforderungsrate nicht in der vorliegenden Norm behandelt wird;
- b) die Normativen Verweisungen wurden aktualisiert und angepasst;
- c) umfangreiche Überarbeitung des Abschnitts 3 "Begriffe" und Ergänzungen von Definitionen für: „Kategorie“ und "Sicherheitsfunktion";
- d) Anpassungen im **Abschnitt 4** unter Sicherheitsteilfunktionen (Stopp-Funktionen, Überwachungsfunktionen und Ausgangsfunktionen);
- e) komplette Überarbeitung des Abschnitts 5 „Management der funktionalen Sicherheit“, neu aufgenommen wurde Unterabschnitt „Architekturspezifikationen des Sicherheitssystems des PDS(SR)“;
- f) Ersatz des Begriffs „Sicherheitsfunktion“ durch „Sicherheits-Teilfunktion“ im gesamten Dokument;
- g) Aktualisierung der Verweisungen auf die Normenreihe IEC 61508, Ausgabe 2010;
- h) Ergänzung der grundsätzlichen Regeln nach ISO 13849-1 und einer Verweisung auf die Tabellen von ISO 13849-2;
- i) **6.1.6**, Ersatz des Textes durch **Tabelle 2**;
- j) **6.1.7**, Anpassung von „Integrierte Schaltkreise mit On-Chip-Redundanz“ an die geänderte Anforderung in **IEC 61508-2:2010, Anhang E**;
- k) Ergänzung der Anforderungen an die systematische Sicherheitsintegrität eines sicherheitsbezogenen Leistungsantriebssystems und -teilsysteme, sowie Anforderungen an deren elektromagnetische Störfestigkeit, Wärmeunempfindlichkeit und mechanische Unempfindlichkeit;
- l) Anpassung der Anwenderdokumentation in **Abschnitt 7**;

- m) komplette Überarbeitung des Abschnitts „Verifikation und Validierung“ ([Abschnitt 8](#));
- n) Prüfanforderungen hinsichtlich der elektromagnetischen Wärme und mechanischen Unempfindlichkeit wurden neu aufgenommen;
- o) das Entwurfs- und Entwicklungsverfahren für PDS (SR) im [Anhang A](#) wurde nach den Angaben aus diesem Dokument angepasst;
- p) umfangreiche Überarbeitung des Anhangs D „Fehlerlisten und Fehlerausschlüsse“; insbesondere die Anforderungen zu Bewegung und Lagerrückführungssensoren;
- q) neu aufgenommen wurde [Anhang E](#) "Anforderungen an die elektromagnetische Störfestigkeit eines PDS(SR)" und [Anhang F](#) „Abschätzung des PFD_{avg} -Werts für Anwendungen mit niedriger Anforderungsrate aus einem vorgegebenen PFH-Wert“.

Frühere Ausgaben

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

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Dokumenten

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

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

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden Deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1 (1 von 3)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 50495:2010	–	DIN EN 50495 (VDE 0170-18):2010-10	VDE 0170-18
	IEC 60050-191:1990	a	
	IEC 60050-351:2013	a	
EN 60079	IEC 60079 (alle Teile)	DIN EN 60079 (VDE 0170)	VDE0170
–	IEC 60204-1	–	–
EN 60300-3-1:2004	IEC 60300-3-1:2003	DIN EN 60300-3-1:2005-5	–
–	IEC 60500:1998	–	–
EN 60664-1:2007	IEC 60664-1:2007	DIN EN 60664-1 (VDE 0110-1):2008-01	VDE 0110-1
–	IEC 60664-3	–	–

Tabelle NA.1 (2 von 3)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61000-2-4:2002	IEC 61000-2-4:2002	DIN EN 61000-2-4 (VDE 0839-2-4):2003-05	VDE 0839-2-4
–	IEC 61000 2-8	–	–
EN 61000-4-2:2009	IEC 61000-4-2:2008	DIN EN 61000-4-2 (VDE 0847-4-2):2009-12	VDE 0847-4-2
EN 61000-4-3:2006 + A1:2008 + A2:2010	IEC 61000-4-3:2006 + AMD1:2007 + AMD2:2010	DIN EN 61000-4-3 (VDE 0847-4-3):2011-04	VDE 0847-4-3
EN 61000-4-4:2012	IEC 61000-4-4:2012	DIN EN 61000-4-4 (VDE 0847-4-4):2013-04	VDE 0847-4-4
EN 61000-4-5:2014	IEC 61000-4-5:2014	DIN EN 61000-4-5 (VDE 0847-4-5):2015-03	VDE 0847-4-5
EN 61000-4-6:2014	IEC 61000-4-6:2013	DIN EN 61000-4-6 (VDE 0847-4-6):2014-08	VDE 0847-4-6
EN 61000-4-11	IEC 61000 4-11	DIN EN 61000-4-11 (VDE 0847-4-11)	VDE 0847-4-11
EN 61000-4-29:2000	IEC 61000-4-29:2000	DIN EN 61000-4-29 (VDE 0847-4-29):2001-10	VDE 0847-4-29
EN 61000-4-34 + A1:2009	IEC 61000-4-34:2005 + A1:2009 + Cor.:2009	DIN EN 61000-4-34 (VDE 0847-4-34):2010-04	VDE 0847-4-34
EN 61000-6-7:2015	IEC 61000-6-7:2014	DIN EN 61000-6-7 (VDE 0839-6-7):2015-12	VDE 0839-6-7
EN 61025	IEC 61025	DIN EN 61025	–
–	IEC 61078	–	–
EN 61165	IEC 61165	DIN EN 61165	–
EN 61400-21:2008	IEC 61400-21:2008	DIN EN 61400-21 (VDE 0127-21):2009-06	VDE 0127-21
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7
EN 61511 (alle Teile)	IEC 61511 (alle Teile)	–	–
EN 61511-1	IEC 61511-1	–	–
EN 61513	IEC 61513	DIN EN 61513 (VDE 0491-2)	VDE 0491-2

Tabelle NA.1 (3 von 3)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61558-1 (alle Teile)	IEC 61558 (alle Teile)	DIN EN 61558 (VDE 0570)	VDE 0570
EN 61558-1:2005	IEC 61558-1:2005 + AMD1:2009	DIN EN 61558-1 (VDE 0570-1):2006-07	VDE 0570-1
–	IEC 61709:2011 <i>ersetzt durch:</i> IEC 61709:2017	–	–
EN 61784-3	IEC 61784-3	–	–
EN 61800-1	IEC 61800-1	DIN EN 61800-1 (VDE 0160-101)	VDE 0160-101
EN 61800-2:2015	IEC 61800-2:2015	DIN EN 61800-2 (VDE 0160-102):2016-08	VDE 0160-102
–	IEC 61800-3:2004 + AMD1:2011 <i>ersetzt durch:</i> IEC 61800-3:2017	–	–
EN 61800-4	IEC 61800-4	DIN EN 61800-4 (VDE 0160-104)	VDE 0160-104
EN 61800-5-1:2007	IEC 61800-5-1:2007	DIN EN 61800-5-1 (VDE 0160-105-1):2008-04	VDE 0160-105-1
EN 62061	IEC 62061	DIN EN 62061 (VDE 0113-50)	VDE 0113-50
–	IEC 62280-1	–	–
–	IEC 62280-2	–	–
–	IEC 62425	–	–
EN ISO 12100	ISO 12100	DIN EN ISO 12100	–
<i>ersetzt durch:</i> EN ISO 13849-1:2015	ISO 13849-1:2006 <i>ersetzt durch:</i> ISO 13849 1:2015	DIN EN ISO 13849-1 <i>ersetzt durch:</i> DIN EN ISO 13849-1:2016-06	–
EN ISO 13849-2:2012	ISO 13849-2:2012	DIN EN ISO 13849-2:2013-02	–
EN ISO 13850	ISO 13850	DIN EN ISO 13850	–
EN 1037	ISO 14118	DIN EN 1037	–
–	ISO/IEC Guide 51:1999 <i>ersetzt durch:</i> ISO/IEC Guide 51:2014	DIN 820-120:2001-10 <i>ersetzt durch:</i> DIN 820-120:2014-06	–
–	IEC Guide 107	–	–
^a „Internationales Elektrotechnisches Wörterbuch – Deutsche Ausgabe“, Online-Zugang: http://www.dke.de/dke-iev .			

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN 820-12:2014-06, *Normungsarbeit – Teil 12: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen (ISO/IEC Guide 51:2014)*

DIN EN 1037, *Sicherheit von Maschinen – Vermeidung von unerwartetem Anlauf*

DIN EN 50495 (VDE 0170-18):2010-10, *Sicherheitseinrichtungen für den sicheren Betrieb von Geräten im Hinblick auf Explosionsgefahren; Deutsche Fassung EN 50495:2010*

DIN EN 60079-5 (VDE 0170) (alle Teile), *Explosionsgefährdete Bereiche*

DIN EN 60300-3-1:2005-5, *Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik (IEC 60300-3-1:2003); Deutsche Fassung EN 60300-3-1:2004*

DIN EN 60664-1 (VDE 0110-1):2008-01, *Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen – Teil 1: Grundsätze, Anforderungen und Prüfungen (IEC 60664-1:2007); Deutsche Fassung EN 60664-1:2007*

DIN EN 61000-2-4 (VDE 0839-2-4):2003-05, *Elektromagnetische Verträglichkeit (EMV) – Teil 2-4: Umgebungsbedingungen – Verträglichkeitspegel für niederfrequente leitungsgeführte Störgrößen in Industrieanlagen (IEC 61000-2-4:2002); Deutsche Fassung EN 61000-2-4:2002*

DIN EN 61000-4-2 (VDE 0847-4-2):2009-12, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-2: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität (IEC 61000-4-2:2008); Deutsche Fassung EN 61000-4-2:2009*

DIN EN 61000-4-3 (VDE 0847-4-3):2011-04, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-3: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen hochfrequente elektromagnetische Felder (IEC 61000-4-3:2006 + A1:2007 + A2:2010); Deutsche Fassung EN 61000-4-3:2006 + A1:2008 + A2:2010*

DIN EN 61000-4-4 (VDE 0847-4-4):2013-04, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-4: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst (IEC 61000-4-4:2012); Deutsche Fassung EN 61000-4-4:2012*

DIN EN 61000-4-5 (VDE 0847-4-5):2015-03, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-5: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen Stoßspannungen (IEC 61000-4-5:2014); Deutsche Fassung EN 61000-4-5:2014*

DIN EN 61000-4-6 (VDE 0847-4-6):2014-08, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-6: Prüf- und Messverfahren – Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder (IEC 61000-4-6:2013); Deutsche Fassung EN 61000-4-6:2014*

DIN EN 61000-4-11 (VDE 0847-4-11), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-11: Prüf- und Messverfahren – Prüfungen der Störfestigkeit gegen Spannungseinbrüche, Kurzzeitunterbrechungen und Spannungsschwankungen*

DIN EN 61000-4-29 (VDE 0847-4-29):2001-10, *Elektromagnetische Verträglichkeit (EMV) – Teil 4-29: Prüf- und Messverfahren; Prüfungen der Störfestigkeit gegen Spannungseinbrüche, Kurzzeitunterbrechungen und Spannungsschwankungen an Gleichstrom-Netzeingängen (IEC 61000-4-29:2000); Deutsche Fassung EN 61000-4-29:2000*

DIN EN 61000-4-34 (VDE 0847-4-34):2010-04, Elektromagnetische Verträglichkeit (EMV) – Teil 4-34: Prüf- und Messverfahren – Prüfungen der Störfestigkeit von Geräten und Einrichtungen mit einem Netzstrom > 16 A je Leiter gegen Spannungseinbrüche, Kurzzeitunterbrechungen und Spannungsschwankungen (IEC 61000-4-34:2005 + A1:2009 + Cor.:2009); Deutsche Fassung EN 61000-4-34:2007 + A1:2009

DIN EN 61000-6-7 (VDE 0839-6-7):2015-12, Elektromagnetische Verträglichkeit (EMV) – Teil 6-7: Fachgrundnormen – Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind (IEC 61000-6-7:2014); Deutsche Fassung EN 61000-6-7:2015

DIN EN 61025, Fehlzustandsbaumanalyse

DIN EN 61165, Anwendung des Markoff-Verfahrens

DIN EN 61400-21 (VDE 0127-21):2009-06, Windenergieanlagen – Teil 21: Messung und Bewertung der Netzverträglichkeit von netzgekoppelten Windenergieanlagen (IEC 61400-21:2008); Deutsche Fassung EN 61400-21:2008

DIN EN 61508-1 (VDE 0803-1):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010

DIN EN 61508-2 (VDE 0803-2):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010

DIN EN 61508-3 (VDE 0803-3):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010

DIN EN 61508-4 (VDE 0803-4):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010

DIN EN 61508-5 (VDE 0803-5):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010

DIN EN 61508-6 (VDE 0803-6):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010

DIN EN 61508-7 (VDE 0803-7):2011-02, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010

DIN EN 61513 (VDE 0491-2), Kernkraftwerke – Leittechnik für Systeme mit sicherheitstechnischer Bedeutung – Allgemeine Systemanforderungen

DIN EN 61558 (VDE 0570) (alle Teile), Sicherheit von Transformatoren, Netzgeräten, Drosseln und dergleichen

DIN EN 61558-1 (VDE 0570-1):2006-07, Sicherheit von Transformatoren, Netzgeräten, Drosseln und dergleichen – Teil 1: Allgemeine Anforderungen und Prüfungen (IEC 61558-1:2005); Deutsche Fassung EN 61558-1:2005

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

DIN EN 61800-5-2 (VDE 0160-105-2):2017-11

DIN EN 61800-2 (VDE 0160-102):2016-08, *Drehzahlveränderbare elektrische Antriebe – Teil 2: Allgemeine Anforderungen – Festlegungen für die Bemessung von Niederspannungs-Wechselstrom-Antriebssystemen mit einstellbarer Frequenz (IEC 61800-2:2015); Deutsche Fassung EN 61800-2:2015*

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 0160-105-1):2008-04, *Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-1: Anforderungen an die Sicherheit – Elektrische, thermische und energetische Anforderungen (IEC 61800-5-1:2007); Deutsche Fassung EN 61800-5-1:2007*

DIN EN 62061 (VDE 0113-50), *Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*

DIN EN ISO 12100, *Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung*

DIN EN ISO 13849-1:2016-06, *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015); Deutsche Fassung EN ISO 13849-1:2015*

DIN EN ISO 13849-2:2013-02, *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO 13849-2:2012); Deutsche Fassung EN ISO 13849-2:2012*

DIN EN ISO 13850, *Sicherheit von Maschinen – Not-Halt-Funktion – Gestaltungsleitsätze*

**Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl –
Teil 5-2: Anforderungen an die Sicherheit –
Funktionale Sicherheit
(IEC 61800-5-2:2016)**

Adjustable speed electrical power drive systems –
Part 5-2: Safety requirements –
Functional
(IEC 61800-5-2:2016)

Entraînements électriques de puissance à
vitesse variable –
Partie 5-2: Exigences de sécurité –
Fonctionnelle
(IEC 61800-5-2:2016)

Diese Europäische Norm wurde von CENELEC am 2016-05-23 angenommen. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CENELEC-Mitglieder sind die nationalen elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

CEN-CENELEC Management Centre : Avenue Marnix 17, B-1000 Brüssel

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61800-5-2:2017 D

Europäisches Vorwort

Der Text des Dokuments 22G/332/FDIS, zukünftige 2. Ausgabe der IEC 61800-5-2, erarbeitet vom SC 22G „Adjustable speed electric drive systems incorporating semiconductor power converters“ des IEC/TC 22 „Power electronic systems and equipment“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 61800-5-2:2017 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2017-10-28
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-04-28

Dieses Dokument ersetzt **EN 61800-5-2:2007**.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument wurde unter einem Mandat erstellt, das von der Europäischen Kommission und der Europäischen Freihandelszone an CENELEC gegeben wurde.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61800-5-2:2016 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 60300-3-1:2003	ANMERKUNG	Harmonisiert als EN 60300-3-1:2003.
IEC 60664-1:2007	ANMERKUNG	Harmonisiert als EN 60664-1:2007 .
IEC 606643	ANMERKUNG	Harmonisiert als EN 60664-3 .
IEC 61025	ANMERKUNG	Harmonisiert als EN 61025.
IEC 61078	ANMERKUNG	Harmonisiert als EN 61078.
IEC 61165	ANMERKUNG	Harmonisiert als EN 61165.
IEC 61508-4:2010	ANMERKUNG	Harmonisiert als EN 61508-4:2010 .
IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 .
IEC 61511 (alle Teile)	ANMERKUNG	Harmonisiert als EN 61511 (alle Teile).
IEC 61511-1	ANMERKUNG	Harmonisiert als EN 61511-1 .
IEC 61513	ANMERKUNG	Harmonisiert als EN 61513 .
IEC 61558 (alle Teile)	ANMERKUNG	Harmonisiert als EN 61558 (alle Teile).

IEC 61558-1:2005	ANMERKUNG	Harmonisiert als EN 61558-1:2005.
IEC 61558-1:2005/AMD1:2009	ANMERKUNG	Harmonisiert als EN 61558-1:2005/A1:2009.
IEC 61784-3	ANMERKUNG	Harmonisiert als EN 61784-3.
IEC 62061	ANMERKUNG	Harmonisiert als EN 62061.
ISO 13849-2	ANMERKUNG	Harmonisiert als EN ISO 13849-2.

Inhalt

Seite

Europäisches Vorwort.....	2
Einleitung	9
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe	13
4 Festgelegte <i>Sicherheits-Teilfunktionen</i>	20
4.1 Allgemeines	20
4.2 <i>Sicherheits-Teilfunktionen</i>	21
4.2.1 Allgemeines	21
4.2.2 Grenzwerte	22
4.2.3 Stopp-Funktionen	22
4.2.4 Überwachungsfunktionen	24
4.2.5 Ausgangsfunktionen – Sichere Bremsenansteuerung (en: safe brake control, SBC)	25
5 Management der <i>funktionalen Sicherheit</i>	25
5.1 Zweck	25
5.2 Anforderungen für das Management der <i>funktionalen Sicherheit</i>	26
5.3 Entwicklungslebenszyklus eines <i>PDS(SR)</i>	26
5.4 Planung des Managements der <i>funktionalen Sicherheit</i> des <i>PDS(SR)</i>	27
5.5 <i>Spezifikation der Anforderungen an die Sicherheit (SRS) für ein PDS(SR)</i>	29
5.5.1 Allgemeines	29
5.5.2 <i>Spezifikation der Anforderungen an die Sicherheits-Teilfunktionen</i>	29
5.5.3 <i>Spezifikation der Anforderungen an die Sicherheitsintegrität</i>	30
5.6 Architekturspezifikation des Sicherheitssystems des <i>PDS(SR)</i>	31
5.6.1 Allgemeines	31
5.6.2 Anforderungen an die Architekturspezifikation des Sicherheitssystems.....	31
6 Anforderungen an Entwurf und Entwicklung eines <i>PDS(SR)</i>	32
6.1 Allgemeine Anforderungen	32
6.1.1 Wechsel des Betriebszustands	32
6.1.2 Entwurfsnormen	32
6.1.3 Realisierung.....	32
6.1.4 <i>Sicherheitsintegrität</i> und Fehlererkennung	32
6.1.5 <i>Sicherheits-Teilfunktionen</i> und nicht sicherheitsbezogene Teilfunktionen.....	33
6.1.6 <i>SIL</i> für mehrere <i>Sicherheits-Teilfunktionen</i> innerhalb eines <i>PDS(SR)</i>	33
6.1.7 Integrierte Schaltkreise mit On-Chip-Redundanz.....	34
6.1.8 Anforderungen an die Software.....	34
6.1.9 Dokumentation des Entwurfs	34
6.2 Anforderungen an den Entwurf des <i>PDS(SR)</i>	34
6.2.1 Wesentliche und bewährte Sicherheitsgrundsätze	34
6.2.2 Anforderungen für die Abschätzung der Wahrscheinlichkeit von gefährbringenden zufälligen Hardwareausfällen je Stunde (<i>PFH</i>)	34
6.2.3 Strukturelle Einschränkungen	37
6.2.4 Abschätzung des <i>Anteils ungefährlicher Ausfälle (SFF)</i>	39

6.2.5	Anforderungen an die <i>systematische Sicherheitsintegrität</i> eines PDS(SR) und von PDS(SR)-Teilsystemen	39
6.2.6	Entwurfsanforderungen an die elektromagnetische Störfestigkeit eines PDS(SR)	42
6.2.7	Entwurfsanforderungen für die Wärmeunempfindlichkeit eines PDS(SR)	43
6.2.8	Entwurfsanforderungen für die mechanische Unempfindlichkeit eines PDS(SR)	43
6.3	Verhalten bei der Erkennung von Fehlern	43
6.3.1	Fehlererkennung	43
6.3.2	Fehlertoleranz größer null	43
6.3.3	Fehlertoleranz von null	43
6.4	Zusätzliche Anforderungen für die Datenkommunikation	43
6.5	Anforderungen an Integration und Prüfung des PDS(SR)	44
6.5.1	Integration der Hardware	44
6.5.2	Integration der Software	44
6.5.3	Modifikationen während der Integration	44
6.5.4	Durchzuführende Integrationsprüfungen	44
6.5.5	Prüfprotokoll	44
7	Anwenderdokumentation	44
7.1	Allgemeines	44
7.2	Informationen und Anweisungen für eine sichere Anwendung eines PDS(SR)	45
8	Verifikation und Validierung	46
8.1	Allgemeines	46
8.2	Verifikation	47
8.3	Validierung	47
8.4	Dokumentation	47
9	Prüfanforderungen	47
9.1	Prüfplanung	47
9.2	Funktionsprüfungen	47
9.3	Prüfung der elektromagnetischen Störfestigkeit	48
9.3.1	Allgemeines	48
9.3.2	Vorgesehene elektromagnetische Umgebung	48
9.3.3	Leistungskriterium (<i>Fail-safe-Zustand – FS</i>)	48
9.4	Prüfung der Wärmeunempfindlichkeit	49
9.4.1	Allgemeines	49
9.4.2	Thermische Funktionsprüfung	49
9.4.3	Thermische Bauteilprüfung	49
9.5	Prüfung der mechanischen Unempfindlichkeit	49
9.5.1	Allgemeines	49
9.5.2	Schwingprüfung	49
9.5.3	Schockprüfung	49
9.5.4	Leistungskriterium für Prüfungen der mechanischen Unempfindlichkeit (<i>Fail-safe-Zustand – FS</i>)	49
9.6	Prüfdokumentation	50
10	Modifikation	50
10.1	Ziel	50

10.2	Anforderungen	50
10.2.1	Allgemeines	50
10.2.2	Anforderung einer Modifikation	50
10.2.3	Einflussanalyse	50
10.2.4	Berechtigung	50
10.2.5	Dokumentation	51
Anhang A (informativ)	Aufgabenablaufplan	52
Anhang B (informativ)	Beispiel für die Abschätzung der <i>PFH</i>	57
B.1	Allgemeines	57
B.2	Aufbau des Beispiel- <i>PDS(SR)</i>	57
B.2.1	Allgemeines	57
B.2.2	<i>Teilsystem A/B</i>	58
B.2.3	<i>Teilsystem PS/VM</i>	59
B.3	Bestimmung des <i>PFH</i> -Werts für das Beispiel- <i>PDS(SR)</i>	59
B.3.1	<i>Teilsystem „A/B“ (Haupt-Teilsystem)</i>	59
B.3.1.1	Zerlegung in Funktionsblöcke	59
B.3.1.2	Bestimmung der Ausfallraten der Funktionsblöcke	60
B.3.1.3	<i>Anteil ungefährlicher Ausfälle</i>	61
B.3.1.4	Faktor der <i>Ausfälle infolge gemeinsamer Ursache</i> $\beta_{A/B}$	62
B.3.1.5	Zuverlässigkeitsmodell (Markov)	62
B.3.1.6	Berechnung des <i>PFH</i> -Werts	64
B.3.2	<i>Teilsystem „PS/VM“</i>	65
B.3.2.1	Zerlegung in Funktionsblöcke	65
B.3.2.2	Ausfallraten der Funktionsblöcke	66
B.3.2.3	<i>Anteil ungefährlicher Ausfälle</i>	66
B.3.2.4	Faktor der <i>Ausfälle infolge gemeinsamer Ursache</i> $\beta_{PS/VM}$	67
B.3.2.5	Zuverlässigkeitsmodell (Markov)	67
B.3.2.6	Berechnung des <i>PFH</i> -Werts	69
B.3.3	<i>PFH</i> -Wert der <i>Sicherheits-Teilfunktion STO</i> des <i>PDS(SR)</i>	69
B.4	Verringerung von <i>DC</i> und <i>SFF</i> in Abhängigkeit vom Prüfintervall	70
Anhang C (informativ)	Verfügbare Datenbanken für Ausfallraten	71
C.1	Datenbanken	71
C.2	Hilfreiche Normen für den Bauelementeausfall	71
Anhang D (informativ)	Fehlerlisten und Fehlerausschlüsse	73
D.1	Allgemeines	73
D.2	Anmerkungen zu Fehlerausschlüssen	73
D.2.1	Gültigkeit von Ausschlüssen	73
D.2.2	Zinn-Whisker-Wachstum	73
D.2.3	Kurzschlüsse von Teilen, die auf Leiterplatten montiert sind	74
D.3	Fehlermodelle	74
D.3.1	Leiter/Kabel	74
D.3.2	Leiterplatten/Baugruppen	74
D.3.3	Reihenklemmen	75

D.3.4	Mehrpolarer Steckverbinder	75
D.3.5	Elektromechanische Bauelemente.....	76
D.3.6	Transformatoren.....	76
D.3.7	Induktivitäten	76
D.3.8	Widerstände	76
D.3.9	Widerstandsnetzwerke	76
D.3.10	Potentiometer	77
D.3.11	Kondensatoren	77
D.3.12	Diskrete Halbleiter	77
D.3.13	Signalisierbauteile	77
D.3.14	Nicht programmierbare integrierte Schaltkreise.....	78
D.3.15	Programmierbare und/oder komplexe integrierte Schaltkreise.....	78
D.3.16	Bewegungs- und Lagerückführungssensoren	79
Anhang E (normativ)	Anforderungen an die elektromagnetische Störfestigkeit eines <i>PDS(SR)</i>	83
E.1	Allgemeines.....	83
E.2	Anforderungen an die Störfestigkeit – niederfrequente Störungen.....	83
E.3	Anforderungen an die Störfestigkeit – hochfrequente Störungen.....	86
Anhang F (informativ)	Abschätzung des PFD_{avg} -Werts für Anwendungen mit niedriger Anforderungsrate aus einem vorgegebenen <i>PFH</i> -Wert	90
F.1	Allgemeines.....	90
F.2	Abschätzung des PFD_{avg} -Werts für Anwendungen mit niedriger Anforderungsrate aus einem vorgegebenen <i>PFH</i> -Wert	90
Literaturhinweise		91
Anhang ZA (normativ)	Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	93
Bilder		
Bild 1	– Anlagen- und Funktionsteile eines <i>PDS(SR)</i>	11
Bild 2	– Aus <i>Sicherheits-Teilfunktionen</i> bestehende <i>Sicherheitsfunktion</i>	22
Bild 3	– Entwicklungslebenszyklus eines <i>PDS(SR)</i>	26
Bild B.1	– Beispiel- <i>PDS(SR)</i>	57
Bild B.2	– <i>Teilsysteme</i> des <i>PDS(SR)</i>	58
Bild B.3	– Funktionsblöcke des <i>Teilsystems</i> A/B	60
Bild B.4	– Zuverlässigkeitsmodell (Markov) des <i>Teilsystems</i> A/B.....	63
Bild B.5	– Funktionsblöcke des <i>Teilsystems</i> PS/VM.....	66
Bild B.6	– Zuverlässigkeitsmodell (Markov) des <i>Teilsystems</i> PS/VM	68
Tabellen		
Tabelle 1	– Verzeichnis der Begriffe	13
Tabelle 2	– Beispiel für die Bestimmung des <i>SIL</i> aus der Hardware- und Software-Unabhängigkeit.....	33
Tabelle 3	– <i>Sicherheits-Integritätslevel</i> : Ausfallgrenzwerte für eine <i>Sicherheits-Teilfunktion</i> eines <i>PDS(SR)</i>	35
Tabelle 4	– Höchster zulässiger <i>Sicherheits-Integritätslevel</i> für eine <i>Sicherheits-Teilfunktion</i> , die von einem sicherheitsbezogenen <i>Teilsystem</i> des Typs A ausgeführt wird	38
Tabelle 5	– Höchster zulässiger <i>Sicherheits-Integritätslevel</i> für eine <i>Sicherheits-Teilfunktion</i> , die von einem sicherheitsbezogenen <i>Teilsystem</i> des Typs B ausgeführt wird	39
Tabelle A.1	– Entwurfs- und Entwicklungsverfahren für <i>PDS(SR)</i>	52

Tabelle B.1 – Bestimmung des <i>DC</i> -Faktors des <i>Teilsystems</i> A/B	61
Tabelle B.2 – Ergebnisse der Berechnung der <i>PFH</i> -Werte für <i>Teilsystem</i> A/B	65
Tabelle B.3 – Bestimmung des <i>DC</i> -Faktors des <i>Teilsystems</i> A/B	66
Tabelle B.4 – Ergebnisse der Berechnung der <i>PFH</i> -Werte für <i>Teilsystem</i> PS/VM.....	69
Tabelle D.1 – Leiterplatten/Baugruppen	74
Tabelle D.2 – Reihenklemme	75
Tabelle D.3 – Mehrpoliger Steckverbinder	75
Tabelle D.4 – Elektromechanische Bauelemente (z. B. Relais, Schaltrelais)	76
Tabelle D.5 – Signalisierbauteile	77
Tabelle D.6 – Nicht programmierbare integrierte Schaltkreise.....	78
Tabelle D.7 – Programmierbare und/oder komplexe integrierte Schaltkreise.....	78
Tabelle D.8 – Bewegungs- und Lagerückführungssensoren	79
Tabelle E.1 – Mindestanforderungen an die Störfestigkeit für Spannungsabweichungen, Spannungseinbrüche und kurzzeitige Unterbrechungen	84
Tabelle E.2 – Mindestanforderungen an die Störfestigkeit von <i>PDS(SR)</i> für Spannungsabweichungen, Spannungseinbrüche und kurzzeitige Unterbrechungen an Netzspannungsanschlüssen mit einer Bemessungsspannung über 1 000 V	85
Tabelle E.3 – Anforderungen an die Störfestigkeit – hochfrequente Störungen	86
Tabelle E.4 – Allgemeine Frequenzbereiche für ortsveränderliche Sender und ISM für die Prüfung abgestrahlter Störgrößen.....	88
Tabelle E.5 – Allgemeine Frequenzbereiche für ortsveränderliche Sender und ISM für die Prüfung leitungsgeführter Störgrößen.....	89

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, Extrudiermaschinen;
- 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 *Performance Level (PL)*), um die Integration eines *PDS(SR)* in sicherheitsbezogene Steuerungssysteme solcher Maschinen zu erleichtern.

ANMERKUNG „Normen des Typs C“ sind in ISO 12100 als Normen für die Sicherheit von Maschinen definiert, die detaillierte Anforderungen an die Sicherheit für bestimmte Maschinen oder Gruppen von Maschinen behandeln.

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 *Gefährdungen*, bei der ein Zugang zur Gefahrenzone nur möglich ist, wenn rotierende Teile zum Stillstand gekommen sind. Dieser Teil von IEC 61800 legt eine Methode fest, mit der der Beitrag eines *PDS(SR)* zu bestimmten *Sicherheits-Teilfunktionen* ermittelt werden kann und die einen geeigneten Entwurf des *PDS(SR)* ermöglicht und den Nachweis, dass dieser 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 und systematischen Fehler des *PDS(SR)* angegeben.

1 Anwendungsbereich

Dieser Teil von IEC 61800, der eine Produktnorm darstellt, legt Anforderungen fest und gibt Empfehlungen für den Entwurf und die Entwicklung, die Integration und die *Validierung* von sicherheitsbezogenen Leistungsantriebssystemen (*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, wie in **IEC 61800-2** angegeben.

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

ANMERKUNG 2 Weitere Teile von IEC 61800 behandeln Festlegungen für die Bemessung, EMV, elektrische Sicherheit usw.

Diese Internationale Norm gilt, wenn *funktionale Sicherheit* eines *PDS(SR)* beansprucht wird und das *PDS(SR)* überwiegend in der *Betriebsart* mit hoher Anforderungsrate oder kontinuierlicher Anforderung (siehe 3.15) betrieben wird.

Obwohl für ein *PDS(SR)* die *Betriebsart* mit niedriger Anforderungsrate möglich ist, ist der Schwerpunkt dieser Norm die *Betriebsart* mit hoher Anforderungsrate und kontinuierlicher Anforderung. *Sicherheits-Teilfunktionen*, die für die *Betriebsart* mit hoher Anforderungsrate oder kontinuierlicher Anforderung ausgeführt werden, können auch in der *Betriebsart* mit niedriger Anforderungsrate verwendet werden. Anforderungen für die *Betriebsart* mit niedriger Anforderungsrate sind in der Normenreihe IEC 61508 angegeben. **Anhang F** enthält einen Leitfaden für die Abschätzung des Werts der mittleren Wahrscheinlichkeit *gefährdender Ausfälle* auf Anforderung (PFD_{avg}).

Dieser Teil von IEC 61800 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) Teile eines *PDS(SR)* unter Berücksichtigung der sicherheitsbezogenen Leistungsfähigkeit der *Sicherheits-Teilfunktion(en)* eines PDS ermöglicht.

Hersteller und Lieferanten von *PDS(SR)* können Anwendern (Systemintegrator, Erstausrüster) durch die Umsetzung der normativen Festlegungen dieses Teils von IEC 61800 die Leistungsfähigkeit zur Funktionalen Sicherheit ihrer Betriebsmittel nachweisen. Dies ermöglicht die Einbindung eines *PDS(SR)* in ein sicherheitsbezogenes Steuerungssystem unter Anwendung der Grundsätze von IEC 61508 und möglicherweise seine Implementierung in spezifischen Bereichen (z. B. IEC 61511, **IEC 61513**, **IEC 62061** oder ISO 13849).

Durch Anwendung der Anforderungen aus diesem Teil der Normenreihe IEC 61800 werden alle entsprechenden Anforderungen von IEC 61508 erfüllt, die für ein *PDS(SR)* gefordert werden.

Dieser Teil der IEC 61800 legt keine Anforderungen fest für:

- die *Gefährdungs-* und Risikoanalyse für eine bestimmte Anwendung;
- die Festlegung von *Sicherheits-Teilfunktionen* für diese Anwendung;
- die Erstzuordnung von *SIL* zu diesen *Sicherheits-Teilfunktionen*;
- die angetriebene Einrichtung mit Ausnahme der Schnittstellenanordnung;
- *Sekundärgefährdungen* (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)*;
- Sicherheitsaspekte (Security) (z. B. IT-Sicherheit oder Zugangssicherheit für das *PDS(SR)*).

ANMERKUNG 3 Die Anforderungen an die *funktionale Sicherheit* eines PDS(SR) hängen von der Anwendung ab und können 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).

Dieser Teil von IEC 61800 gilt nur für PDS(SR), die *Sicherheits-Teilfunktionen* nicht größer als SIL 3 ausführen.

Bild 1 zeigt die *Anlagen-* und *Funktionsteile* eines PDS(SR), die in diesem Teil von IEC 61800 behandelt werden, und gibt eine eher logische Darstellung eines PDS(SR) als dessen physikalische Beschreibung an.

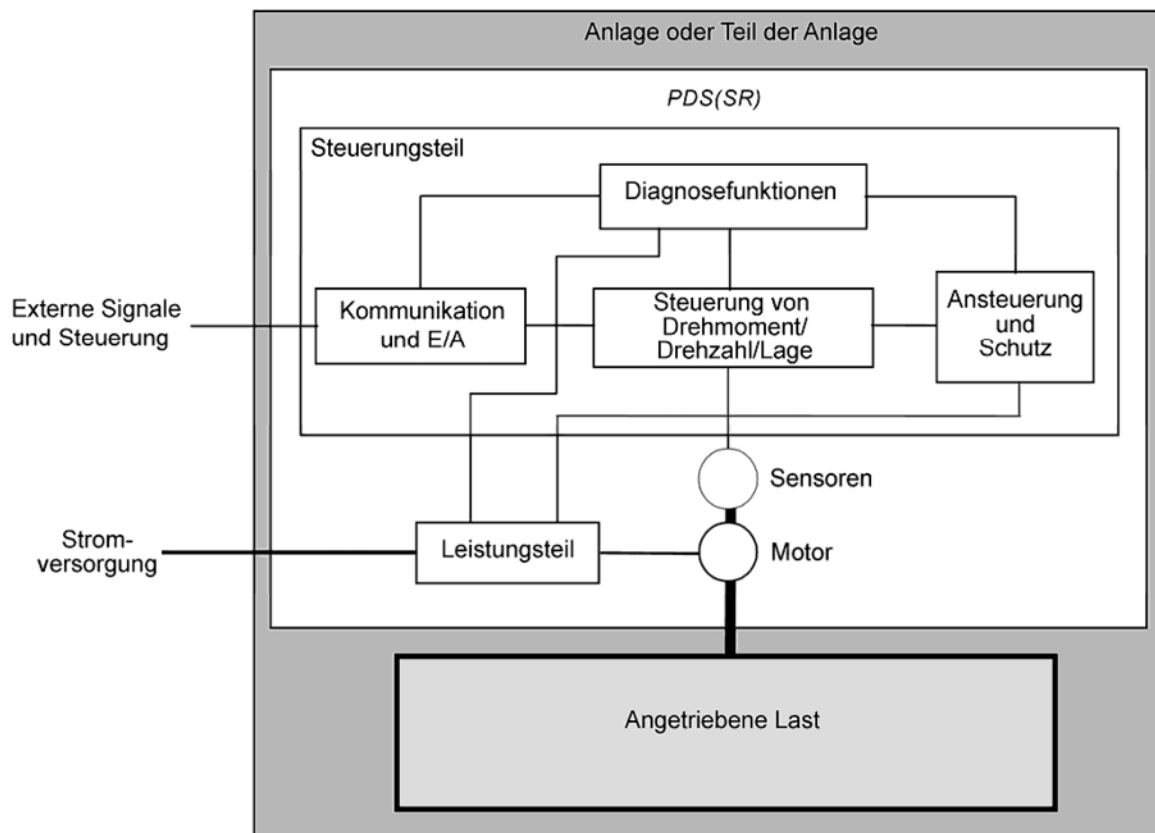


Bild 1 – Anlagen- und Funktionsteile eines PDS(SR)

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, 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).

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

IEC 61000-2-4:2002, *Electromagnetic compatibility (EMC) – Part 2-4: Environment – Compatibility levels in industrial plants for low-frequency conducted disturbances*

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-3:2006/AMD1:2007
IEC 61000-4-3:2006/AMD2:2010

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2014, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2013, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-29:2000, *Electromagnetic compatibility (EMC) – Part 4-29: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests*

IEC 61000-4-34:2005, *Electromagnetic compatibility (EMC) – Part 4-34: Testing and measurement techniques – Voltage dips, short interruptions and voltage variations immunity tests for equipment with input current more than 16 A per phase*

IEC 61000-6-7:2014, *Electromagnetic compatibility (EMC) – Part 6-7: Generic standards – Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61400-21:2008, *Wind turbines – Part 21: Measurement and assessment of power quality characteristics of grid connected wind turbines*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 3: Software requirements*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safetyrelated systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safetyrelated 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 61800-2:2015, *Adjustable speed electrical power drive systems – Part 2: General requirements – Rating specifications for low voltage adjustable speed a.c. power drive systems*

IEC 61800-3:2004, *Adjustable speed electrical power drive systems – Part 3: EMC requirements and specific test methods*
IEC 61800-3:2004/AMD1:2011

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 61800-5-1:2007, *Adjustable speed electrical power drive systems – Part 5-1: Safety requirements – Electrical, thermal and energy*

ISO 13849-1:2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

3 Begriffe

Für die Anwendung dieses Dokumentes gelten die folgenden Begriffe.

Tabelle 1 enthält ein (in der englischen Originalfassung alphabetisches) Verzeichnis der Begriffe.

Tabelle 1 – Verzeichnis der Begriffe

3.1	Antriebsgrundmodul <i>BDM</i>	3.12	Gefährdung	3.23	Sicherheits-Teilfunktion (eines <i>PDS(SR)</i>)
3.2	Kategorie	3.13	Anlage	3.24	Sicherheitsintegrität
3.3	vollständiges Antriebsmodul <i>CDM</i>	3.14	Gebrauchsdauer T_M	3.25	Sicherheits-Integritätslevel <i>SIL</i>
3.4	Ausfall infolge gemeinsamer Ursache	3.15	Betriebsart	3.26	sicherheitsbezogenes System
3.5	gefahrbringender Ausfall	3.16	<i>PDS(SR)</i>	3.27	Spezifikation der Anforderungen an die Funktionale Sicherheit <i>SRS</i>
3.6	Diagnosedeckungsgrad <i>DC</i>	3.17	mittlere Häufigkeit eines gefahr- bringenden Ausfalls <i>PFH</i>	3.28	<i>SIL</i> -Fähigkeit
3.7	Diagnoseprüfung	3.18	Performance Level <i>PL</i>	3.29	Teilsystem
3.8	sicher bei Ausfall <i>fail-safe</i>	3.19	ungefährlicher Ausfall	3.30	systematischer Ausfall
3.9	Fail-safe-Zustand <i>FS</i>	3.20	Anteil ungefährlicher Ausfälle <i>SFF</i>	3.31	systematische Sicherheitsinteg- rität
3.10	Fehlerreaktionsfunktion	3.21	sicherer Zustand	3.32	Validierung
3.11	funktionale Sicherheit	3.22	Sicherheitsfunktion	3.33	Verifikation

ANMERKUNG In der gesamten vorliegenden Internationalen Norm sind die definierten Begriffe *kursiv* geschrieben.

3.1

Antriebsgrundmodul BDM

(en: basic drive module)

elektronischer Leistungsstromrichter mit zugehöriger Regelung, der zwischen der elektrischen Versorgung und einem Motor angeschlossen ist

Anmerkung 1 zum Begriff: Das *BDM* kann die Leistung von der elektrischen Versorgung zum Motor und eventuell auch die Leistung vom Motor zur elektrischen Versorgung übertragen.

Anmerkung 2 zum Begriff: Das *BDM* regelt einige oder alle Größen der zum Motor und Motorausgang übertragenen Leistung: Strom, Frequenz, Spannung, Drehzahl, Drehmoment, Kraft.

Anmerkung 3 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

[QUELLE: IEC 61800-3:2004/AMD1:2011, 3.1.1]

3.2

Kategorie

(en: category)

Einstufung der sicherheitsbezogenen Teile eines *PDS(SR)* bezüglich ihres Widerstandes gegen Fehler und ihres nachfolgenden Verhaltens bei einem Fehler, die erreicht wird durch die Struktur der Anordnung der Teile, die Fehlererkennung und/oder ihre Zuverlässigkeit

[QUELLE: ISO 13849-1, Begriff 3.1.2, modifiziert – „Steuerung“ wurde durch „*PDS(SR)*“ ersetzt.]

3.3

vollständiges Antriebsmodul

CDM

(en: complete drive module)

Antriebsmodul, welches aus dem *BDM* und den Erweiterungen wie Schutzeinrichtungen, Transformatoren und Hilfseinrichtungen besteht, jedoch nicht darauf begrenzt ist. Dazu zählen jedoch nicht der Motor und die Messfühler, die mechanisch an die Motorwelle gekoppelt sind

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

[QUELLE: IEC 61800-3:2004/AMD1:2011, 3.1.2]

3.4

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 *Sicherheits-Teilfunktion* führen

[QUELLE: IEC 61508-4:2010, 3.6.10, modifiziert – „zu einem Systemausfall führen“ wurde durch „zu einem Ausfall der *Sicherheits-Teilfunktion* führen“ ersetzt.]

3.5

gefährbringender Ausfall

(en: dangerous failure)

Ausfall eines Bauteils und/oder *Teilsystems* und/oder Systems, die/das Anteil an der Ausführung der *Sicherheits-Teilfunktion* haben/hat, der

- verhindert, dass eine *Sicherheits-Teilfunktion* eines *PDS(SR)* ausgeführt wird, sodass das Betriebsmittel oder die Maschine, das bzw. die durch das *PDS(SR)* angetrieben wird, in einen gefährlichen oder möglicherweise gefährlichen Zustand gebracht wird; oder
- die Wahrscheinlichkeit vermindert, die *Sicherheits-Teilfunktion* ordnungsgemäß auszuführen

[QUELLE: IEC 61508-4:2010, 3.6.7, modifiziert – „EUC“ wird durch „*PDS(SR)*“ ersetzt und „bei Anforderung“ wurde gestrichen.]

3.6

Diagnosedeckungsgrad

DC

(en: diagnostic coverage)

Anteil der *gefährbringenden Ausfälle*, die durch automatische *Diagnoseprüfungen* erkannt werden

Anmerkung 1 zum Begriff: Der *Diagnosedeckungsgrad* kann auch angegeben werden als das Verhältnis der Summe der Rate erkannter *gefährbringender Ausfälle* λ_{DD} zur Summe der Rate aller *gefährbringenden Ausfälle* λ_D :

$$DC = \lambda_{DD} / \lambda_D$$

Anmerkung 2 zum Begriff: Der *Diagnosedeckungsgrad* kann für das gesamte *sicherheitsbezogene System* oder Teile davon gelten. Er kann z. B. für Sensoren und/oder logische *Teilsysteme* und/oder *Ausgangsteilsysteme* vorliegen.

Anmerkung 3 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

[QUELLE: IEC 61508-4:2010, 3.8.6, modifiziert – Aus „diagnostischen Online-Prüfungen“ wurde „Online“ gestrichen.]

3.7

Diagnoseprüfung

(en: diagnostic test)

Prüfung zur Erkennung von Fehlern oder Ausfällen, die zu einem festgelegten Ergebnis führt, wenn ein Fehler oder Ausfall erkannt wird

3.8

sicher bei Ausfall

fail-safe

(en: fail safe)

Konstruktionseigenschaft einer Einheit, die verhindern soll, dass deren Ausfälle zu gefahrbringenden Fehlzuständen führen

[QUELLE: IEC 60500:1998, 821-01-10, modifiziert – „kritischen“ wurde durch „gefahrbringenden“ ersetzt.]

3.9

Fail-safe-Zustand

FS

(en: fail safe state)

definierter *sicherer Zustand*, der sich in der Regel durch einen Ausfall ergibt

Anmerkung 1 zum Begriff: *Fail-safe-Zustand (FS)* wird in dieser Norm anstelle des definierten Zustands (DS) nach IEC 61000-6-7 benutzt.

Anmerkung 2 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

3.10

Fehlerreaktionsfunktion

(en: fault reaction function)

Funktion, die ausgelöst wird, wenn ein Fehler oder Ausfall im *PDS(SR)* erkannt wird, der einen Verlust der *Sicherheits-Teilfunktion* 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

3.11

funktionale Sicherheit

(en: functional safety)

Teil der Gesamtsicherheit, bezogen auf das *PDS(SR)*, der von der korrekten Funktion des sicherheitsbezogenen Teils des *PDS(SR)* und äußerer risikomindernder Maßnahmen abhängt

Anmerkung 1 zum Begriff: Diese Norm betrachtet nur diejenigen Aspekte in der Definition der *funktionalen Sicherheit*, die von der korrekten Funktion des *PDS(SR)* abhängen.

[QUELLE: IEC 61508-4:2010, 3.1.12, modifiziert – „EUC und das EUC-Leit- oder Steuerungssystem“ wurde durch „*PDS(SR)*“ ersetzt und „des sicherheitsbezogenen E/E/PE-Systems und anderer“ wurde durch „des sicherheitsbezogenen Teils des *PDS(SR)* und äußerer“ ersetzt.]

3.12

Gefährdung

(en: hazard)

potentielle Schadensquelle

Anmerkung 1 zum Begriff: Der Begriff umfasst eine Gefahr für Personen, die innerhalb eines kurzen Zeitraumes entsteht (z. B. Brand und Explosion), und auch solche Gefahren, die eine langzeitige Auswirkung auf die Gesundheit von Personen haben (z. B. Freisetzung von Giftstoffen).

[QUELLE: IEC 60050-351:2013, 351-57-01, modifizierte Anmerkung 1 zum Begriff]

3.13

Anlage

(en: installation)

PDS(SR), durch das *PDS(SR)* angetriebene Betriebsmittel und mögliche weitere Betriebsmittel (siehe Bild 1)

Anmerkung 1 zum Begriff: Der Begriff „Anlage (en: installation)“ wird in der englischsprachigen Internationalen Norm auch zur Bezeichnung der Errichtung eines *PDS(SR)* benutzt. In diesen Fällen wird in dieser Norm der Wortlaut „Errichtung der Anlage (en: act of installing)“ angewendet.

3.14

Gebrauchsdauer

T_M

(en: mission time)

festgelegte kumulierte Betriebsdauer der sicherheitsbezogenen Teile des *PDS(SR)* während ihrer Gesamtlebensdauer

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

3.15

Betriebsart

(en: mode of operation)

Art der vorgesehenen Verwendung einer *Sicherheits-Teilfunktion* in Bezug auf die Anforderungsrate, die an sie gestellt wird und die entweder eine *Betriebsart* mit niedriger Anforderungsrate oder eine *Betriebsart* mit hoher Anforderungsrate oder kontinuierlicher Anforderung sein kann

Anmerkung 1 zum Begriff: *Betriebsart* mit niedriger Anforderungsrate (en: low demand mode): mit einer Anforderungsrate für die *Sicherheits-Teilfunktion* von höchstens einmal im Jahr.

Anmerkung 2 zum Begriff: *Betriebsart* mit hoher Anforderungsrate und kontinuierlicher Anforderung (en: high demand and continuous mode): mit einer Anforderungsrate für die *Sicherheits-Teilfunktion* von mehr als einmal im Jahr.

Anmerkung 3 zum Begriff: Die *Betriebsart* mit niedriger Anforderungsrate wird für *PDS(SR)*-Anwendungen im Allgemeinen als nicht erheblich angesehen. Deshalb wird in der vorliegenden Norm davon ausgegangen, dass *PDS(SR)* hauptsächlich in der *Betriebsart* mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrieben werden.

[QUELLE: IEC 61508-4:2010, 3.5.16, modifiziert – Die „*Betriebsart* mit hoher Anforderungsrate“ und die „*Betriebsart* mit kontinuierlicher Anforderung“ wurden zusammengefasst und die Definition wurde auf Zeitangaben reduziert.]

3.16

PDS

(SR)

elektrisches Leistungsantriebssystem mit einstellbarer Drehzahl, die *Sicherheits-Teilfunktionen* zur Verfügung stellt

3.17

mittlere Häufigkeit eines gefahrbringenden Ausfalls

PFH

(en: average frequency of a dangerous failure)

mittlere Häufigkeit eines gefahrbringenden Ausfalls eines *PDS(SR)*, die festgelegte *Sicherheits-Teilfunktion* über einen gegebenen Zeitraum auszuführen

Anmerkung 1 zum Begriff: In IEC 62061 wird die Abkürzung PFH_D verwendet.

Anmerkung 2 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

[QUELLE: IEC 61508-4:2010, 3.6.19, modifiziert – „sicherheitsbezogenes E/E/PE-System“ wurde durch „*PDS(SR)*“ ersetzt.]

3.18

Performance Level

PL

diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine *Sicherheits-Teilfunktion* unter vorhersehbaren Bedingungen auszuführen

[QUELLE: ISO 13849-1:2006, 3.1.23, modifiziert – „*Sicherheitsfunktion*“ wurde durch „*Sicherheits-Teilfunktion*“ ersetzt.]

3.19

ungefährlicher Ausfall

(en: safe failure)

Ausfall eines Bauteils und/oder *Teilsystems* und/oder Systems, die/das Anteil an der Ausführung der *Sicherheits-Teilfunktion* haben/hat, der

- a) zur Fehlauslösung der *Sicherheits-Teilfunktion* führt, das *PDS(SR)* (oder Teile davon) in einen *sicheren Zustand* zu bringen oder den *sicheren Zustand* aufrechtzuerhalten; oder
- b) die Wahrscheinlichkeit der Fehlauslösung der *Sicherheits-Teilfunktion* erhöht, das *PDS(SR)* (oder Teile davon) in einen *sicheren Zustand* zu bringen oder den *sicheren Zustand* aufrechtzuerhalten

[QUELLE: IEC 61508-4:2010, 3.6.8, modifiziert – „Element“ wurde durch „Bauteil“ ersetzt, „EUC“ wurde durch „*PDS(SR)*“ ersetzt.]

3.20

Anteil ungefährlicher Ausfälle

SFF

(en: safe failure fraction)

Eigenschaft eines sicherheitsbezogenen Bauteils und *Teilsystems*, die durch das Verhältnis der Summe der mittleren Ausfallraten *ungefährlicher* und *gefahrbringender* erkannter *Ausfälle* zur Summe *ungefährlicher* und aller *gefahrbringenden Ausfälle* definiert wird

Anmerkung 1 zum Begriff: Dieses Verhältnis wird durch die folgende Gleichung dargestellt:

$$SFF = (\sum \lambda_s + \sum \lambda_{DD}) / (\sum \lambda_s + \sum \lambda_D)$$

Anmerkung 2 zum Begriff: Siehe IEC 61508-2:2010, Anhang C.

Anmerkung 3 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

[QUELLE: IEC 61508-4:2010, 3.6.15, modifiziert – „Element“ wurde durch „Bauteils und *Teilsystems*“ ersetzt.]

3.21

sicherer Zustand

(en: safe state)

Zustand des *PDS(SR)*, in dem die Sicherheit erreicht ist

Anmerkung 1 zum Begriff: Beim Übergang von einem potentiell gefährlichen Zustand zum endgültigen *sicheren Zustand* kann das *PDS(SR)* eine Anzahl von Sicherheits-Zwischenzuständen durchlaufen.

[QUELLE: IEC 61508-4:2010, 3.1.13, modifiziert – „EUC“ wurde durch „*PDS(SR)*“ ersetzt.]

3.22

Sicherheitsfunktion

(en: safety function)

Funktion, die von einem *sicherheitsbezogenen System* oder anderen risikomindernden Maßnahmen ausgeführt wird und dazu vorgesehen ist, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen *sicheren Zustand* für das Betriebsmittel oder die Maschine, das bzw. die vom *PDS(SR)* angetrieben wird, zu erreichen oder aufrechtzuerhalten

[QUELLE: IEC 61508-4:2010, 3.5.1, modifiziert – „E/E/PE“ wurde gestrichen, „EUC“ wurde durch „das Betriebsmittel oder die Maschine, das bzw. die vom *PDS(SR)* angetrieben wird“ ersetzt.]

3.23

Sicherheits-Teilfunktion (eines *PDS(SR)*)

(en: safety sub-funktion (of a *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

Anmerkung 1 zum Begriff: Es gibt nur wenige Fälle, in denen die *Sicherheitsfunktion* der vollständigen Anwendung ausschließlich innerhalb des *PDS(SR)* ausgeführt wird. In diesen Fällen wird die *Sicherheitsfunktion* in dieser Norm trotzdem als *Sicherheits-Teilfunktion* bezeichnet (z. B. immer aktive SLS ohne äußere Auslösung).

3.24

Sicherheitsintegrität

(en: safety integrity)

Wahrscheinlichkeit, dass ein *PDS(SR)* eine geforderte *Sicherheits-Teilfunktion* unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes anforderungsgemäß ausführt

Anmerkung 1 zum Begriff: Je höher der *Sicherheits-Integritätslevel* des *PDS(SR)*, umso geringer ist die Wahrscheinlichkeit, dass das sicherheitsbezogene *PDS(SR)* die geforderte *Sicherheits-Teilfunktion* nicht ausführt.

Anmerkung 2 zum Begriff: Die *Sicherheitsintegrität* kann für jede vom *PDS(SR)* ausgeführte *Sicherheits-Teilfunktion* anders sein.

[QUELLE: IEC 61508-4:2010, 3.5.4, modifiziert – „sicherheitsbezogenes E/E/PE-System“ wurde durch „*PDS(SR)*“ ersetzt.]

3.25

Sicherheits-Integritätslevel

SIL

(en: safety integrity level)

diskrete Stufen (eine von drei möglichen) zur Festlegung der Anforderungen an die *Sicherheitsintegrität* einer *Sicherheits-Teilfunktion*, die einem *PDS(SR)* (insgesamt oder teilweise) zugeordnet werden

Anmerkung 1 zum Begriff: *SIL* 3 ist die höchste Stufe der *Sicherheitsintegrität* und *SIL* 1 die niedrigste Stufe.

Anmerkung 2 zum Begriff: *SIL* 4 wird in dieser Norm nicht betrachtet, da es für die Anforderungen an die Risikominde- rung im Zusammenhang mit *PDS(SR)* in der Regel nicht relevant ist. Für *SIL* 4 geltende Anforderungen können IEC 61508 entnommen werden.

Anmerkung 3 zum Begriff: Für *SILx* werden mehrere Schreibweisen verwendet. Im vorliegenden Dokument wird *SIL* x benutzt.

Anmerkung 4 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

[QUELLE: IEC 61508-4:2010, 3.5.8, modifiziert – „die einem Wertebereich der *Sicherheitsintegrität* entsprechen, wobei der *Sicherheits-Integritätslevel* 4 die höchste Stufe der *Sicherheitsintegrität* und der *Sicherheits-Integritätslevel* 1 die niedrigste darstellt“ wurde durch „zur Festlegung der Anforderungen an die *Sicherheits- integrität* einer *Sicherheits-Teilfunktion*, die einem *PDS(SR)* (insgesamt oder teilweise) zugeordnet werden“ ersetzt.]

3.26

sicherheitsbezogenes System

(en: safety-related system)

System, das sowohl

- die erforderlichen *Sicherheitsfunktionen* ausführt, die notwendig sind, um einen *sicheren Zustand* für das Betriebsmittel oder die Maschine, das bzw. die durch das *PDS(SR)* angetrieben wird, zu erreichen oder aufrechtzuerhalten, als auch
- dazu vorgesehen ist, selbst oder mit anderen risikomindernden Maßnahmen die notwendige *Sicherheitsintegrität* für die geforderten *Sicherheitsfunktionen* zu erreichen

[QUELLE: IEC 61508-4:2010, 3.4.1, modifiziert – „EUC“ wurde durch „das Betriebsmittel oder die Maschine, das bzw. die durch das *PDS(SR)* angetrieben wird“ ersetzt und „E/E/PE“ wurde gestrichen.]

3.27

Spezifikation der Anforderungen an die Sicherheit

SRS

(en: safety requirements specification)

Spezifikation, die alle Anforderungen der *Sicherheits-Teilfunktionen* enthält, die vom *PDS(SR)* auszuführen sind

Anmerkung 1 zum Begriff: Diese Anmerkung gilt nur für die französische Sprachfassung.

3.28

SIL-Fähigkeit

(en: SIL capability)

höchster *SIL*, der durch die Auslegung eines *PDS(SR)* hinsichtlich der *systematischen Sicherheitsintegrität* und der strukturellen Einschränkungen für die *Sicherheitsintegrität* der Hardware als erreicht betrachtet werden kann

Anmerkung 1 zum Begriff: Jeder der bezeichneten *Sicherheits-Teilfunktionen*, die ein *PDS(SR)* ausführen soll, kann eine andere *SIL-Fähigkeit* zugeordnet werden.

Anmerkung 2 zum Begriff: Die *SIL-Fähigkeit* umfasst die systematische Fähigkeit, die strukturellen Einschränkungen und die Ausfallrate der Hardware oder den *PFH*-Wert zu erfüllen.

3.29

Teilsystem

(en: subsystem)

Teil des strukturellen Entwurfs eines *sicherheitsbezogenen Systems* auf oberster Ebene, dessen Ausfall zu einem Ausfall einer sicherheitsbezogenen Funktion führt

Anmerkung 1 zum Begriff: Ein *PDS(SR)* kann selbst ein *Teilsystem* sein oder aus einer Anzahl von einzelnen *Teilsystemen* aufgebaut sein, die nach dem Zusammenfügen die betreffende *Sicherheits-Teilfunktion* ausführen. Ein *Teilsystem* kann mehr als einen Kanal besitzen.

Anmerkung 2 zum Begriff: Beispiele für *Teilsysteme* eines *PDS(SR)* sind Geber, Leistungsteil, Steuerungsteil (siehe Bild 1).

3.30

Versagen

systematischer Ausfall

(en: systematic failure)

systematisches Versagen/Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann

Anmerkung 1 zum Begriff: Beispiele von Ursachen für *systematische Ausfälle* schließen menschliches Versagen ein in

- der Spezifikation der Anforderungen an die Sicherheit;

- dem Entwurf, der Herstellung, dem Einbau, dem Betrieb der Hardware;
- dem Entwurf und der Implementierung usw. der Software.

Anmerkung 2 zum Begriff: In dieser Norm werden Ausfälle in einem *sicherheitsbezogenen System* in zufällige Hardwareausfälle oder *systematische Ausfälle* eingeteilt.

[QUELLE: IEC 61508-4:2010, 3.6.6]

3.31

systematische Sicherheitsintegrität

(en: systematic safety integrity)

Teil der *Sicherheitsintegrität* eines *sicherheitsbezogenen Systems*, der sich auf *systematische Ausfälle* mit gefahrbringender Ausfallart bezieht

Anmerkung 1 zum Begriff: Die *systematische Sicherheitsintegrität* kann üblicherweise nicht quantifiziert werden (zum Unterschied zur *Sicherheitsintegrität* der Hardware, bei der dies üblicherweise möglich ist).

[QUELLE : IEC 61508-4:2010, 3.5.6]

3.32

Validierung

(en: validation)

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

Anmerkung 1 zum Begriff: Die *Validierung* ist die Tätigkeit, die darlegt, dass das *PDS(SR)* vor und nach der Errichtung der *Anlage* in jeder Hinsicht der *Spezifikation der Anforderungen an die Sicherheit* entspricht.

[QUELLE: IEC 61508-4:2010, 3.8.2 – Anmerkung 1 zum Begriff wurde modifiziert.]

3.33

Verifikation

(en: verification)

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

[QUELLE: IEC 61508-4:2010, 3.8.1, modifiziert – Anmerkung 1 zum Begriff wurde gestrichen.]

4 Festgelegte Sicherheits-Teilfunktionen

4.1 Allgemeines

In diesem Abschnitt werden Funktionen eines *PDS(SR)* beschrieben, die vom *PDS(SR)*-Lieferanten als sicherheitsbezogen festgelegt werden dürfen. Die Auflistung der angegebenen *Sicherheits-Teilfunktionen* wird nicht als vollständig betrachtet. Wegen der umfangreichen Möglichkeiten wurden Einzelheiten der Implementierung grundlegender *Sicherheits-Teilfunktionen* und komplexer *Sicherheits-Teilfunktionen*, die sich aus mehreren grundlegenden *Sicherheits-Teilfunktionen* zusammensetzen, nicht angegeben. In einigen Fällen können zum *PDS(SR)* weitere externe *sicherheitsbezogene Systeme* (z. B. eine mechanische Bremse) erforderlich sein, um die Sicherheit aufrechtzuerhalten, wenn die elektrische Energie abgeschaltet ist.

Die technischen Maßnahmen, die zur Umsetzung dieser Funktionen erforderlich sind, hängen von der geforderten *SIL-Fähigkeit* und der geforderten Wahrscheinlichkeit gefahrbringender Hardwareausfälle ab, die in der *Spezifikation der Anforderungen an die Sicherheit* angegeben sind. Die technischen Maßnahmen sind im [Abschnitt 6](#) beschrieben.

Jede *Sicherheits-Teilfunktion* darf sichere Eingänge und/oder Ausgänge beinhalten, damit die notwendige Kommunikation mit (oder die Aktivierung von) anderen Funktionen, *Teilsystemen* oder Systemen (die sicherheitsbezogen sein können oder nicht) erfolgen kann.

Einige der *Sicherheits-Teilfunktionen* führen nur Überwachungsaufgaben aus, andere eine sicherheitsbezogene Steuerung oder sonstige 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 *Sicherheits-Teilfunktion* erkannt wird; und
- einer *Fehlerreaktionsfunktion* (gilt für alle *Sicherheits-Teilfunktionen*):
die Reaktionsfunktion, wenn durch Diagnose ein Fehler innerhalb der *Sicherheits-Teilfunktion* 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 Anforderungen an die Sicherheit* angegeben (siehe 5.5).

Die Bezeichnungen für die *Sicherheits-Teilfunktionen* beinhalten das Wort „sicher“, um anzuzeigen, dass diese Funktionen in einer sicherheitsbezogenen Anwendung eingesetzt werden können aufgrund einer Einschätzung (d. h. einer Risikoanalyse) dieser bestimmten Anwendung, die vom *PDS(SR)* auszuführende sicherheitsbezogene Funktionen und deren Integrität erfordert.

ANMERKUNG Ausführliche Beispiele für die *PDS(SR)*-Teilfunktionen, die in diesem Abschnitt festgelegt sind, können den Literaturhinweisen (IFA Report 7/2013) entnommen werden.

4.2 *Sicherheits-Teilfunktionen*

4.2.1 Allgemeines

In den meisten Fällen sind die *Sicherheitsfunktionen* des *PDS(SR)* Bestandteil der *Sicherheitsfunktionen* einer Anwendung und deshalb werden die *Sicherheitsfunktionen* des *PDS(SR)* in diesem Dokument als *Sicherheits-Teilfunktionen* bezeichnet. Bild 2 zeigt ein Beispiel für eine *Sicherheitsfunktion*, die aus *Sicherheits-Teilfunktionen* besteht.

System (Maschine, Prozess) mit einer *Sicherheitsfunktion*, z. B. „Sicherer Maschinen-Stopp“

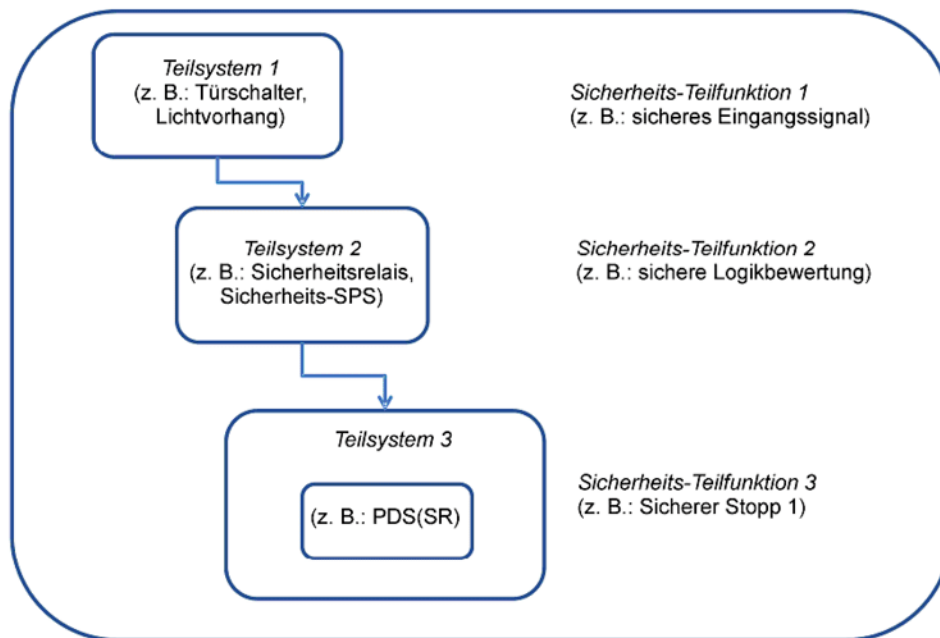


Bild 2 – Aus Sicherheits-Teilfunktionen bestehende Sicherheitsfunktion

ANMERKUNG Weitere Informationen über *Sicherheits-Teilfunktionen* können dem IFA Report 7/2013 „Sichere Antriebssteuerungen mit Frequenzumrichtern“ (Literaturhinweise) entnommen werden.

4.2.2 Grenzwerte

Wenn eine *Sicherheits-Teilfunktion* auf einem Grenzwert (auf 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 kann eine mögliche Überschreitung der Grenzwerte bei einer Übertretung berücksichtigt werden. Zum Beispiel kann (können) bei der Festlegung des (der) Lagegrenzwerte(s) in 4.2.4.9 der (die) größte(n) zulässige(n) Nachlaufweg(e) berücksichtigt werden.

Eine bestimmte *Sicherheits-Teilfunktion* darf einen oder mehrere festgelegte(n) Grenzwert(e) besitzen, (der)die während des Betriebs ausgewählt werden (kann)können.

4.2.3 Stopp-Funktionen

4.2.3.1 Allgemeines

Für jeden Typ des PDS(SR) steht 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 Stopp-Funktionen zu realisieren, können einzelne Betätigungen von Hand und Verbindungen mit den Steuerkreisen erforderlich sein.

ANMERKUNG Wenn Sicherheits-Stopp-Funktionen für Funktionen wie die Vermeidung eines unerwarteten Anlaufs oder Not-Halt angewendet werden, können die entsprechenden Normen wie IEC 60204-1, ISO 13850, ISO 12100 oder ISO 14118 herangezogen werden.

Von den Kunden des PDS(SR)-Herstellers können besondere Anforderung an das Verhalten einer Stopp-Funktion festgelegt werden. In der Praxis werden häufig folgende Beispiele für Stopp-Funktionen eingesetzt.

4.2.3.2 Sicher abgeschaltetes Drehmoment (en: safe torque off, STO)

Diese Funktion verhindert, dass dem Motor eine krafterzeugende Energie zugeführt wird.

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

ANMERKUNG 1 Diese *Sicherheits-Teilfunktion* kann verwendet werden, wenn die Abschaltung der Energie zur Verhinderung eines unerwarteten Anlaufs nach ISO 14118 erforderlich ist.

ANMERKUNG 2 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 3 Elektronische Einrichtungen und bestimmte Schütze bilden keinen ausreichenden Schutz gegen elektrischen Schlag.

ANMERKUNG 4 Wenn diese Funktion aktiviert ist, ist bei einem Ausfall im Leistungsteil des PDS(SR) immer noch eine begrenzte Bewegung möglich.

4.2.3.3 Sicherer Stopp 1 (en: safe stop 1, SS1)

Diese Funktion ist entweder festgelegt als

- a) Sicherer Stopp 1 mit gesteuerter Verzögerung
SS1-d (en: safe stop 1 deceleration controlled)

Auslösen und Steuern der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der STO-Funktion (siehe 4.2.3.2), wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt; oder

- b) Sicherer Stopp 1 mit Überwachung der Verzögerungsrampe
SS1-r (en: safe stop 1 ramp monitored)

Auslösen und Überwachen der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der STO-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt; oder

- c) Sicherer Stopp 1 mit Zeitsteuerung
SS1-t (en: safe stop 1 time controlled)

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

Diese *Sicherheits-Teilfunktion* entspricht einem gesteuerten Stillsetzen nach IEC 60204-1, Stopp-Kategorie 1.

ANMERKUNG Das gesteuerte Stillsetzen von SS1-t kann unerkannt versagen, daher kann SS1-t nicht angewendet werden, wenn dieses Versagen eine gefahrbringende Situation in der Endanwendung verursachen kann.

4.2.3.4 Sicherer Stopp 2 (en: safe stop 2, SS2)

Diese Funktion ist entweder festgelegt als

- a) Sicherer Stopp 2 mit gesteuerter Verzögerung
SS2-d (en: safe stop 2 deceleration controlled)

Auslösen und Steuern der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der SOS-Funktion (siehe 4.2.4.1), wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt; oder

- b) Sicherer Stopp 2 mit Überwachung der Verzögerungsrampe
SS2-r (en: safe stop 2 ramp monitored)

Auslösen und Überwachen der Größe der Motorverzögerung innerhalb ausgewählter Grenzen zum Stillsetzen des Motors und Ausführen der SOS-Funktion, wenn die Motordrehzahl unter einen festgelegten Grenzwert fällt; oder