

	DIN EN 62061 (VDE 0113-50)	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 13.110; 25.040.99; 29.020 Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005); Deutsche Fassung EN 62061:2005 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (IEC 62061:2005); German version EN 62061:2005 Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité (CEI 62061:2005); Version allemande EN 62061:2005 Gesamtumfang 115 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE Normenausschuss Sicherheitstechnische Grundsätze (NASG)		

Beginn der Gültigkeit

Die von CENELEC am 2004-12-01 angenommene EN 62061 gilt als DIN-Norm ab 2005-10-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 62061 (VDE 0113-50):2003-06.

Für die vorliegende Norm ist das nationale Arbeitsgremium K 225 „Elektrotechnische Ausrüstung und Sicherheit von Maschinen und maschinellen Anlagen“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig.

Die enthaltene IEC-Publikation wurde vom TC 44 „Safety of machinery – Electrotechnical aspects“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem auf der IEC-Website unter „<http://webstore.iec.ch>“ mit den Daten zu dieser Publikation angegebenen Datum (maintenance result date) unverändert bleiben soll. 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 nachstehend wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 954-1:1996	ISO 13849-1:1999	DIN EN 954-1:1997-03	–
EN 1050:1996	ISO 14121:1999	DIN EN 1050:1997-01	–
EN 50159-1:2001	–	DIN EN 50159-1 (VDE 0831-159-1):2001-11	VDE 0831-159-1
EN 50159-2:2001	–	DIN EN 50159-2 (VDE 0831-159-2):2001-12	VDE 0831-159-2
EN 60204-1:1997	IEC 60204-1:1997 + Corr. 1998	DIN EN 60204-1 (VDE 0113-1):1998-11	VDE 0113-1
EN 61000-4-2:1995 + A1:1998 + A2:2001	IEC 61000-4-2:1995 + A1:1998 + A2 :2000	DIN EN 61000-4-2 (VDE 0847-4-2):2001-12	VDE 0847-4-2
EN 61000-4-3:2002 +A1:2002	IEC 61000-4-3:2002 + A1:2002	DIN EN 61000-4-3 (VDE 0847-4-3):2003-11	VDE 0847-4-3
EN 61000-4-4:2004	IEC 61000-4-4:2004	DIN EN 61000-4-4 (VDE 0847-4-4):2005-07	VDE 0847-4-4
EN 61000-4-5:1995 + A1:2001	IEC 61000-4-5:1995 + A1:2000	DIN EN 61000-4-5 (VDE 0847-4-5):2001-12	VDE 0847-4-5
EN 61000-4-6:1996 + A1:2001	IEC 61000-4-6:1996 + A1:2000	DIN EN 61000-4-6 (VDE 0847-4-6):2001-12	VDE 0847-4-6
EN 61000-4-8:1993 + A1:2001	IEC 61000-4-8:1993 + A1:2000	DIN EN 61000-4-8 (VDE 0847-4-8):2001-12	VDE 0847-4-8
EN 61000-4-11:2004	IEC 61000-4-11:2004	DIN EN 61000-4-11 (VDE 0847-4-11):2005-02	VDE 0847-4-11
EN 61000-6-2:2001	IEC 61000-6-2:1999, mod.	DIN EN 61000-6-2 (VDE 0839-6-2):2002-08	VDE 0839-6-2
Normen der Reihe EN 61310	Normen der Reihe IEC 61310	Normen der Reihe DIN EN 61310 (VDE 0113)	Normen der Reihe VDE 0113
EN 61496-1:2004	IEC 61496-1:2004, mod.	DIN EN 61496-1 (VDE 0113-201):2005-01	VDE 0113-201
EN 61508-1:2001	IEC 61508-1:1998 + Corrigendum 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 + Corrigendum 1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-4:2001	IEC 61508-4:1998 + Corrigendum 1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4
EN 61508-5:2001	IEC 61508-5:1998 + Corrigendum 1999	DIN EN 61508-5 (VDE 0803-5):2002-11	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	DN EN 61508-7 (VDE 0803-7):2003-06	VDE 0803-7

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61511-1:2004	IEC 61511-1:2003 + Corrigendum 2004	DIN EN 61511-1 (VDE 0810-1):2005-05	VDE 0810-1
EN ISO 12100-1:2003	ISO 12100-1:2003	DIN EN ISO 12100-1:2004-04	–
EN ISO 12100-2:2003	ISO 12100-2:2003	DIN EN ISO 12100-2:2004-04	–
EN ISO 13849-2:2003	ISO 13849-2:2003	DIN EN ISO 13849-2:2003-12	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 954-1, *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze*; Deutsche Fassung EN 954-1:1996.

DIN EN 1050, *Sicherheit von Maschinen – Leitsätze zur Risikobeurteilung*; Deutsche Fassung EN 1050:1996.

DIN EN 50159-1 (VDE 0831-159-1), *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen*; Deutsche Fassung EN 50159-1:2001.

DIN EN 50159-2 (VDE 0831-159-2), *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen*; Deutsche Fassung EN 50159-2:2001.

DIN EN 60204-1 (VDE 0113-1), *Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 60204-1:1997 + Corrigendum 1998)*; Deutsche Fassung EN 60204-1:1997.

DIN EN 61000-4-2 (VDE 0847-4-2), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-2: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität (IEC 61000-4-2:1995 + A1:1998 + A2:2000)*; Deutsche Fassung EN 61000-4-2:1995 + A1:1998 + A2:2001.

DIN EN 61000-4-3 (VDE 0847-4-3), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-3: Prüf- und Messverfahren; Prüfung der Störfestigkeit gegen hochfrequente elektromagnetische Felder (IEC 61000-4-3:2002 + A1:2002)*; Deutsche Fassung EN 61000-4-3:2002 + A1:2002.

DIN EN 61000-4-4 (VDE 0847-4-4), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-4: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst (IEC 61000-4-4:2004)*; Deutsche Fassung EN 61000-4-4:2004.

DIN EN 61000-4-5 (VDE 0847-4-5), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-5: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen Stoßspannungen (IEC 61000-4-5:1995 + A1:2000)*; Deutsche Fassung EN 61000-4-5:1995 + A1:2001.

DIN EN 61000-4-6 (VDE 0847-4-6), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-6: Prüf- und Messverfahren – Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder (IEC 61000-4-6:1996 + A1:2000)*; Deutsche Fassung EN 61000-4-6:1996 + A1:2001.

DIN EN 61000-4-8 (VDE 0847-4-8), *Elektromagnetische Verträglichkeit (EMV) – Teil 4-8: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen Magnetfelder mit energietechnischen Frequenzen (IEC 61000-4-8:1993 + A1:2000)*; Deutsche Fassung EN 61000-4-8:1993 + A1:2001.

DIN EN 61000-4-11 (VDE 0847-4-11), Elektromagnetische Verträglichkeit (EMV) – Teil 4-11: Prüf- und Messverfahren – Prüfung der Störfestigkeit gegen Spannungseinbrüche, Kurzzeitunterbrechungen und Spannungsschwankungen (IEC 61000-4-11:2004); Deutsche Fassung EN 61000-4-11:2004.

DIN EN 61000-6-2 (VDE 0839-6-2), Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen – Störfestigkeit für Industriebereich (IEC 61000-6-2:1999, modifiziert); Deutsche Fassung EN 61000-6-2:2001.

Normen der Reihe DIN EN 61310 (VDE 0113), Sicherheit von Maschinen – Anzeigen, Kennzeichen und Bedienen.

DIN EN 61496-1 (VDE 0113-201), Sicherheit von Maschinen – Berührungslos wirkende Schutzeinrichtungen – Teil 1: Allgemeine Anforderungen und Prüfungen (IEC 61496-1:2004, modifiziert); Deutsche Fassung EN 61496-1:2004.

DIN EN 61508-1 (VDE 0803-1), 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 61508-2 (VDE 0803-2), 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), 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 61508-4 (VDE 0803-4), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-4:2001.

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) (IEC 61508-5:1998 + Corrigendum 1999); Deutsche Fassung EN 61508-5:2001.

DIN EN 61508-6 (VDE 0803-6), 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), 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 61511-1 (VDE 0810-1), Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003 + Corrigendum 2004); Deutsche Fassung EN 61511-1:2004.

DIN EN ISO 12100-1, Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze – Teil 1: Grundsätzliche Terminologie, Methodologie (ISO 12100-1:2003); Deutsche Fassung EN ISO 12100-1:2003.

DIN EN ISO 12100-2, Sicherheit von Maschinen – Grundbegriffe, allgemeine Gestaltungsleitsätze – Teil 2: Technische Leitsätze (ISO 12100-2:2003); Deutsche Fassung EN ISO 12100-2:2003.

DIN EN ISO 13849-2, Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung (ISO 13849-2:2003); Deutsche Fassung EN ISO 13849-2:2003.

– Leerseite –

Sicherheit von Maschinen
Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und
programmierbarer elektronischer Steuerungssysteme
(IEC 62061:2005)

Safety of machinery
Functional safety of safety-related electrical,
electronic and programmable electronic control
systems
(IEC 62061:2005)

Sécurité des machines
Sécurité fonctionnelle des systèmes de
commande électriques, électroniques et
électroniques programmables relatifs à la
sécurité
(CEI 62061:2005)

Diese Europäische Norm wurde von CENELEC am 2004-12-01 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, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, 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

Vorwort

Der Text des Schriftstücks 44/460/FDIS, zukünftige Ausgabe 1 der IEC 62061, ausgearbeitet von dem IEC/TC 44 „Safety of machinery – Electrotechnical aspects“, wurde der IEC-CENELEC Parallelen Abstimmung unterworfen und von CENELEC am 2004-12-01 als EN 62061 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): 2005-11-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2007-12-01

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 der EG-Richtlinie 98/37/EG ab. Siehe Anhang ZZ.

INTERVALL FÜR DEN PROOF-TEST UND DIE GEBRAUCHSDAUER

Die folgenden wichtigen Informationen in Bezug auf die Anforderungen dieser Norm sollten zur Kenntnis genommen werden:

Wo die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_D) in hohem Maße von Proof-Tests abhängt (d. h. Tests, die dazu vorgesehen sind Fehler aufzudecken, die nicht durch Diagnosefunktionen erkannt werden), ist es notwendig zu zeigen, dass das Intervall für den Proof-Test im Zusammenhang mit der erwarteten Verwendung des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) realistisch und praktikabel ist (z. B. können Intervalle für den Proof-Test^{*)}, die kürzer als 10 Jahre sind, für viele Maschinenanwendungen unvernünftig kurz sein).

CEN/TC114/WG6 hat im Rahmen der Abschätzung der mittleren Zeit bis zum gefahrbringenden Ausfall ($MTTF_D$) für die Realisierung der vorgesehenen Architekturen in Anhang B von prEN ISO 13849-1 ein Intervall für den Proof-Test (Gebrauchsdauer) von 20 Jahren verwendet. Daher wird empfohlen, dass Konstrukteure von SRECS ein Intervall für den Proof-Test von 20 Jahren anstreben.

Es ist bekannt, dass einige Teilsysteme und/oder Teilsystem-Elemente (z. B. elektromechanische Bauteile mit hohem Nutzungsfaktor) innerhalb des Intervalls für den Proof-Test des SRECS einen Austausch erfordern.

Proof-Tests bedingen ausführliche und umfassende Überprüfungen, die in der Praxis nur durchgeführt werden können, wenn das SRECS und/oder seine Teilsysteme entworfen worden sind, um Proof-Tests zu erleichtern (z. B. vorgesehene Test-Ports) und mit den notwendigen Informationen versehen sind (z. B. Anweisungen für den Proof-Test).

^{*)} In **DIN EN 61508-4:2002** ist der englische Begriff „proof test“ mit „Wiederholungsprüfung“ übersetzt. Da dieser Begriff im Maschinenbereich jedoch nicht üblich ist, wurde in dieser Übersetzung der EN 62061 der englische Begriff beibehalten.

Um die Gültigkeit des vom Konstrukteur festgelegten Intervalls sicherzustellen, ist es wichtig, dass alle anderen notwendigen vorgesehenen Tests (z. B. Funktionsprüfungen) ebenfalls erfolgreich am SRECS durchgeführt werden.

Die [Anhänge ZA](#) und [ZZ](#) sind durch CENELEC hinzugefügt worden.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 62061:2005 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Vorwort.....	2
Einleitung.....	7
1 Anwendungsbereich	10
2 Normative Verweisungen.....	11
3 Begriffe, Definitionen und Abkürzungen	12
3.1 Alphabetische Liste der Definitionen	12
3.2 Begriffe und Definitionen	13
3.3 Abkürzungen.....	24
4 Management der funktionalen Sicherheit	24
4.1 Ziel	24
4.2 Anforderungen	24
5 Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen (SRCFs).....	26
5.1 Ziel	26
5.2 Spezifikation der Anforderungen für SRCFs	26
6 Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	28
6.1 Ziel	28
6.2 Allgemeine Anforderungen	28
6.3 Anforderungen zum Verhalten (des SRECS) bei Erkennung eines Fehlers im SRECS.....	29
6.4 Anforderungen zur systematischen Sicherheitsintegrität des SRECS	30
6.5 Auswahl eines sicherheitsbezogenen elektrischen Steuerungssystems	32
6.6 Entwurf und Entwicklung eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	32
6.7 Realisierung von Teilsystemen.....	38
6.8 Realisierung von Diagnosefunktionen	55
6.9 Hardware-Implementierung des SRECS	56
6.10 Spezifikation der Software-Sicherheitsanforderungen	56
6.11 Software-Entwurf und Entwicklung	57
6.12 Integration und Test des sicherheitsbezogenen elektrischen Steuerungssystems.....	64
6.13 Installation des SRECS	66
7 Benutzerinformationen des SRECS	66
7.1 Ziel	66
7.2 Dokumentation für Installation, Gebrauch und Instandhaltung	66
8 Validierung des sicherheitsbezogenen elektrischen Steuerungssystems.....	67
8.1 Ziel	68
8.2 Allgemeine Anforderungen	68
8.3 Validierung der systematischen Sicherheitsintegrität des SRECS.....	68
9 Modifikation.....	69

	Seite
9.1 Ziel	69
9.2 Modifikationsverfahren	70
9.3 Konfigurationsmanagementverfahren	70
10 Dokumentation	72
Anhang A (informativ) Festsetzung des SIL	74
Anhang B (informativ) Beispiel eines Entwurfs eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) unter Anwendung der Konzepte und Anforderungen aus den Abschnitten 5 und 6	82
Anhang C (informativ) Hinweise zu Entwurf und Entwicklung von Embedded-Software	89
Anhang D (informativ) Ausfallarten elektrischer/elektronischer Bauteile	98
Anhang E (informativ) Elektromagnetische (EM) Phänomene und erhöhte Störfestigkeitsgrade für SRECS, die für den Gebrauch im Industriebereich nach IEC 61000-6-2 vorgesehen sind	103
Anhang F (informativ) Methodologie zur Abschätzung der Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache (CCF)	105
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	108
Anhang ZZ (informativ) Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien	109
 Bild 1 – Verhältnis der IEC 62061 zu anderen relevanten Normen	8
Bild 2 – Ablauf des SRECS-Entwurfs- und Entwicklungsprozesses	35
Bild 3 – Zuordnung von Sicherheitsanforderungen der Funktionsblöcke zu Teilsystemen (siehe 6.6.2.1.1)	36
Bild 4 – Ablauf für Entwurf und Entwicklung eines Teilsystems (siehe Kästchen 6B von Bild 2)	41
Bild 5 – Aufteilung eines Funktionsblocks in redundante Funktionsblock-Elemente und ihre zugehörigen Teilsystem-Elemente	42
Bild 6 – Logische Darstellung Teilsystem A	49
Bild 7 – Logische Darstellung Teilsystem B	50
Bild 8 – Logische Darstellung Teilsystem C	50
Bild 9 – Logische Darstellung Teilsystem D	52
Bild A.1 – Ablauf des Prozesses der Festsetzung des SIL	75
Bild A.2 – Parameter der Risikoabschätzung	76
Bild B.1 – Terminologie im Zusammenhang funktionaler Aufteilung	82
Bild B.2 – Beispiel einer Maschine	83
Bild B.3 – Spezifikation der Anforderungen für eine SRCF	83
Bild B.4 – Aufteilung in eine Struktur von Funktionsblöcken	84
Bild B.5 – Erstes Konzept für eine Architektur eines SRECS	85
Bild B.6 – SRECS-Architektur mit innerhalb jedes Teilsystems eingebetteten Diagnosefunktionen (TS1 bis TS4)	86
Bild B.7 – SRECS-Architektur mit innerhalb des Teilsystems TS3 eingebetteten Diagnosefunktionen	87
Bild B.8 – Abschätzung der PFH_D für ein SRECS	88
 Tabelle 1 – Empfohlene Anwendung von IEC 62061 und ISO 13849-1 (in Revision)	9
Tabelle 2 – Übersicht und Ziele der IEC 62061	11

	Seite
Tabelle 3 – Sicherheits-Integritätslevels: Ausfallgrenzwerte für SRCFs.....	28
Tabelle 4 – Merkmale der in diesem Beispiel verwendeten Teilsysteme 1 und 2 (siehe vorstehende Anmerkung)	38
Tabelle 5 – Strukturelle Einschränkungen von Teilsystemen: maximal in Anspruch nehmbarer SIL für eine SRCF, die dieses Teilsystem verwendet	44
Tabelle 6 – Strukturelle Einschränkungen: SILCL in Bezug auf Kategorien	45
Tabelle 7 – Wahrscheinlichkeit eines gefahrbringenden Ausfalls.....	48
Tabelle 8 – Informationen und Dokumentation eines SRECS.....	73
Tabelle A.1 – Klassifikation der Schwere (S).....	76
Tabelle A.2 – Klassifikation der Häufigkeit und der Dauer der Exposition (F).....	77
Tabelle A.3 – Klassifikation der Wahrscheinlichkeit (W).....	78
Tabelle A.4 – Klassifikation der Möglichkeit ³⁾ der Vermeidung oder Begrenzung des Schadens (P)	79
Tabelle A.5 – Parameter zur Festlegung der Klasse der Wahrscheinlichkeit des Schadens (K).....	79
Tabelle A.6 – Matrix der Festlegung des SIL.....	79
Tabelle D.1 – Beispiele für Anteile von Ausfallarten für elektrische/elektronische Bauteile.....	98
Tabelle E.1 – EM-Phänomene und erhöhte Störfestigkeitsgrade für SRECS.....	103
Tabelle E.2 – Ausgewählte Frequenzen für HF-Feld-Prüfungen.....	104
Tabelle E.3 – Ausgewählte Frequenzen für Prüfungen leitungsgeführter HF	105
Tabelle F.1 – Kriterien zur Bestimmung von CCF	106
Tabelle F.2 – Abschätzung des CCF-Faktors (β)	107

Einleitung

Als ein Ergebnis der Automatisierung, der Forderung nach gesteigerter Produktion und reduziertem körperlichen Aufwand des Benutzers spielen sicherheitsbezogene elektrische Steuerungssysteme (nachfolgend SRECS genannt) von Maschinen eine zunehmende Rolle in der Verwirklichung der Maschinengesamtsicherheit. Weiterhin verwenden die SRECS selbst zunehmend komplexe elektronische Technologie.

In der Vergangenheit gab es ohne das Vorhandensein von Normen wegen der Ungewissheit in Bezug auf die Leistungsfähigkeit einer solchen Technologie eine Abneigung, SRECS in sicherheitsbezogenen Funktionen für signifikante Maschinengefährdungen zu akzeptieren.

Diese Internationale Norm ist für Maschinenkonstrukteure, Hersteller von Steuerungssystemen und Integratoren und andere, die an der Spezifikation, dem Entwurf und der Validierung von SRECS beteiligt sind, vorgesehen. Sie beschreibt einen Lösungsweg und beschreibt Anforderungen zum Erreichen der notwendigen Leistungsfähigkeit.

Diese Norm ist maschinensektorspezifisch innerhalb des Rahmens der IEC 61508. Sie ist dazu vorgesehen, das Spezifizieren der Leistungsfähigkeit von sicherheitsbezogenen elektrischen Steuerungssystemen in Bezug auf die signifikanten Gefährdungen (siehe 3.8 der ISO 12100-1) von Maschinen zu erleichtern.

Diese Norm stellt einen maschinensektorspezifischen Rahmen für funktionale Sicherheit eines SRECS von Maschinen bereit. Sie behandelt nur diejenigen Aspekte des Sicherheitslebenszyklus, die in Bezug zur Zuweisung der Sicherheitsanforderungen bis hin zur Validierung der Sicherheit stehen. Es werden Anforderungen beschrieben für Informationen für den sicheren Gebrauch von SRECS von Maschinen, die auch für spätere Lebensphasen des SRECS relevant sein können.

Es gibt viele Situationen an Maschinen, wo SRECS als Teil der vorgesehenen Sicherheitsmaßnahmen benutzt werden, um eine Minderung des Risikos zu erreichen. Ein typischer Fall ist die Verwendung einer verriegelten trennenden Schutzeinrichtung, die, wenn geöffnet, um Zugang zum Gefährdungsbereich zu ermöglichen, dem elektrischen Steuerungssystem signalisiert, die gefährliche Maschinenbewegung zu stoppen. Ebenso trägt in der Automatisierung das elektrische Steuerungssystem, das verwendet wird, um den korrekten Betrieb des Maschinenprozesses zu erreichen, oft zur Sicherheit bei, indem es die mit den Gefährdungen, die direkt von Ausfällen des Steuerungssystems herrühren, verbundenen Risiken verringert. Diese Norm stellt eine Methodologie und Anforderungen bereit, um:

- den erforderlichen Sicherheits-Integritätslevel für jede sicherheitsbezogene Steuerungsfunktion, die vom SRECS auszuführen ist, zu bestimmen;
- den Entwurf des SRECS in Angemessenheit zu der (den) bestimmten sicherheitsbezogenen Steuerungsfunktion(en) zu ermöglichen;
- in Übereinstimmung mit ISO 13849 entworfene sicherheitsbezogene Teilsysteme zu integrieren;
- das SRECS zu validieren.

Diese Norm ist zur Verwendung innerhalb des Gesamtrahmens der in ISO 12100-1 beschriebenen systematischen Risikominderung und in Verbindung mit einer Risikobeurteilung gemäß den in ISO 14121 (EN 1050) beschriebenen Prinzipien vorgesehen. Eine zur Festlegung des Sicherheits-Integritätslevel (SIL) vorgeschlagene Methodologie ist im informativen [Anhang A](#) enthalten.

Es werden Maßnahmen angegeben, um die Leistungsfähigkeit des SRECS mit der vorgesehenen Risikominderung unter Berücksichtigung der Wahrscheinlichkeiten und der Auswirkungen von zufälligen und systematischen Fehlern innerhalb des elektrischen Steuerungssystems zu koordinieren.

[Bild 1](#) zeigt die Beziehung dieser Norm zu anderen relevanten Normen.

[Tabelle 1](#) gibt Empfehlungen für die empfohlene Anwendung dieser Norm und der Revision der ISO 13849-1.

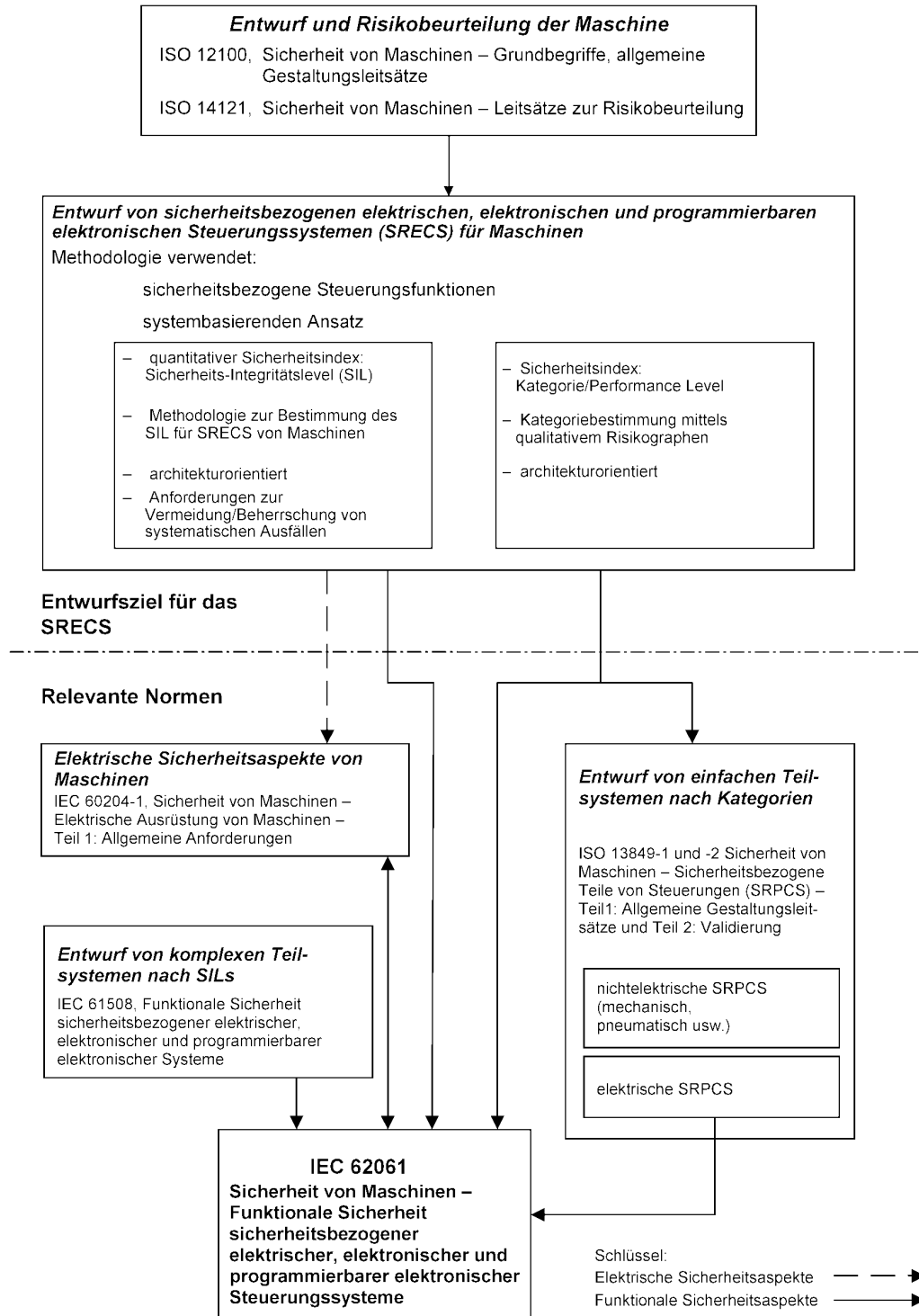


Bild 1 – Verhältnis der IEC 62061 zu anderen relevanten Normen

Informationen zur empfohlenen Anwendung von IEC 62061 und ISO 13849-1 (in Revision)

IEC 62061 und ISO 13849-1 (in Revision) legen Anforderungen für den Entwurf und die Implementierung von sicherheitsbezogenen Steuerungssystemen von Maschinen fest. Die Anwendung jeder dieser Normen in Übereinstimmung mit ihren Anwendungsbereichen kann die Erfüllung der relevanten grundsätzlichen Sicherheitsanforderungen vermuten lassen. Tabelle 1 fasst die Anwendungsbereiche von IEC 62061 und ISO 13849-1 (in Revision) zusammen.

ANMERKUNG ISO 13849-1 ist augenblicklich in Bearbeitung durch ISO TC 199 und CEN TC 114.

Tabelle 1 – Empfohlene Anwendung von IEC 62061 und ISO 13849-1 (in Revision)

	Technologie, in der die sicherheits- bezogene(n) Steuerungsfunktion(en) ausgeführt wird (werden)	ISO 13849-1 (in Revision)	IEC 62061
A	Nichtelektrik, z. B. Hydraulik	X	nicht betrachtet
B	Elektromechanik, z. B. Relais oder einfache Elektronik	beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und bis zu PL=e	alle Architekturen und bis zu SIL 3
C	komplexe Elektronik, z. B. programmierbar	beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und bis zu PL=d	alle Architekturen und bis zu SIL 3
D	A kombiniert mit B	beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und bis zu PL=e	X siehe Anmerkung 3
E	C kombiniert mit B	beschränkt auf vorgesehene Architekturen (siehe Anmerkung 1) und bis zu PL=d	alle Architekturen und bis zu SIL 3
F	C kombiniert mit A oder C kombiniert mit A und B	X siehe Anmerkung 2	X siehe Anmerkung 3
„X“ bedeutet, dass dieser Punkt in der Norm, die in der Spaltenüberschrift angegeben ist, behandelt wird. ANMERKUNG 1 Vorgesehene Architekturen sind in Anhang B der EN ISO 13849-1 (Rev.) definiert, um einen vereinfachten Ansatz zur Quantifizierung der Performance Level bereitzustellen. ANMERKUNG 2 Für komplexe Elektronik: Verwendung der vorgesehenen Architekturen in Übereinstimmung mit EN ISO 13849-1 (Rev.) bis zu PL=d oder jede Architektur nach IEC 62061. ANMERKUNG 3 Für nichtelektrische Technologie: Verwendung von Teilen nach EN ISO 13849-1 (Rev.) als Teilsysteme.			

1 Anwendungsbereich

Diese Internationale Norm legt Anforderungen fest und gibt Empfehlungen für den Entwurf, die Integration und die Validierung von sicherheitsbezogenen elektrischen, elektronischen und programmierbaren elektronischen Steuerungssystemen (SRECS) für Maschinen (siehe Anmerkungen 1 und 2). Sie ist auf Steuerungssysteme anwendbar, die entweder einzeln oder in Kombination verwendet werden, um sicherheitsbezogene Steuerungsfunktionen an Maschinen auszuführen, die während der Arbeit nicht von Hand tragbar sind, einschließlich einer Gruppe von Maschinen, die koordiniert zusammenarbeiten.

ANMERKUNG 1 In dieser Norm wird der Begriff „elektrische Steuerungssysteme“ für „Elektrische, Elektronische und Programmierbare Elektronische (E/E/PE) Steuerungssysteme“ und der Begriff „SRECS“ für „sicherheitsbezogene elektrische, elektronische und programmierbare elektronische Steuerungssysteme“ verwendet.

ANMERKUNG 2 In dieser Norm wird angenommen, dass die Ausführung von komplexen programmierbaren elektronischen Teilsystemen oder Teilsystem-Elementen mit den relevanten Anforderungen von IEC 61508 übereinstimmt. Diese Norm stellt eher eine Methodologie für die Verwendung solcher Teilsysteme und Teilsystem-Elemente als Teil eines SRECS zur Verfügung, als für deren Entwicklung.

Diese Norm ist eine Anwendungsnorm und ist nicht dazu gedacht, den technologischen Fortschritt zu begrenzen oder zu behindern. Sie umfasst nicht alle Anforderungen (z. B. Verwendung von Schutzeinrichtungen, nicht-elektrische Verriegelung oder nicht-elektrische Steuerung), die notwendig sind oder durch andere Normen oder Vorschriften gefordert werden, um Personen vor Gefährdungen zu schützen. Jede Art von Maschine besitzt eigene Anforderungen, die erfüllt werden müssen, um für ausreichende Sicherheit zu sorgen.

Diese Norm:

- bezieht sich nur auf Anforderungen zur funktionalen Sicherheit, die vorgesehen sind zur Minderung des Risikos von Verletzungen oder des Verlusts der Gesundheit von Personen in unmittelbarer Umgebung der Maschine und denjenigen Personen, die direkt mit dem Gebrauch der Maschine befasst sind;
- ist beschränkt auf Risiken, die direkt aus den Gefährdungen der Maschine selbst herrühren oder einer Gruppe von Maschinen, die koordiniert zusammenarbeiten;

ANMERKUNG 3 Anforderungen zur Verminderung von Risiken, die von anderen Gefährdungen herrühren, ergeben sich aus relevanten Sektornormen. Wo eine (mehrere) Maschine(n) zum Beispiel Teil einer Prozessaktivität ist (sind), sollten die Anforderungen zur funktionalen Sicherheit des elektrischen Steuerungssystems der Maschine zusätzlich andere Anforderungen (z. B. IEC 61511) erfüllen, insofern die Sicherheit des Prozesses betroffen ist.

- legt keine Anforderungen für die Leistungsfähigkeit von nicht-elektrischen (z. B. hydraulischen, pneumatischen) Steuerungselementen für Maschinen fest;

ANMERKUNG 4 Obwohl die Anforderungen in dieser Norm spezifisch für elektrische Steuerungssysteme sind, kann der festgelegte Rahmen und die Methodologie für sicherheitsbezogene Teile von Steuerungssystemen anwendbar sein, die andere Technologien verwenden.

- schließt keine elektrischen Gefährdungen ein, die von der elektrischen Steuereinrichtung selbst herrühren (z. B. elektrischer Schlag – siehe [IEC 60204-1](#)).

Die Ziele der einzelnen Abschnitte in der IEC 62061 sind in [Tabelle 2](#) angegeben.

Tabelle 2 – Übersicht und Ziele der IEC 62061

Abschnitt	Ziel
4: Management der funktionalen Sicherheit	Spezifikation der Managementaktivitäten und technischer Aktivitäten, die für das Erreichen der erforderlichen funktionalen Sicherheit des SRECS notwendig sind.
5: Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen	Festlegung der Verfahren zur Spezifikation der Anforderungen für sicherheitsbezogene Steuerungsfunktionen. Diese Anforderungen werden ausgedrückt in Form der Spezifikation der funktionalen Anforderungen und der Spezifikation der Anforderungen zur Sicherheitsintegrität.
6: Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems	Spezifikation der Auswahlkriterien und/oder der Verfahren für Entwurf und Implementierung des SRECS, um die Anforderungen zur funktionalen Sicherheit zu erfüllen. Dies schließt ein: Auswahl der Systemarchitektur, Auswahl der sicherheitsbezogenen Hardware und Software, Entwurf der Hardware und Software, Verifikation, dass die entworfene Hardware und Software die Anforderungen zur funktionalen Sicherheit erfüllen.
7: Benutzerinformationen für die Maschine	Spezifikation der Anforderungen für die Benutzerinformationen des SRECS, die mit der Maschine geliefert werden müssen. Dies schließt ein: Bereitstellung der Benutzeranleitung und der Verfahren, Bereitstellung der Instandhaltungsanleitung und der Verfahren.
8: Validierung des sicherheitsbezogenen elektrischen Steuerungssystems	Spezifikation der Anforderungen für den auf das SRECS anzuwendenden Validierungsprozess. Dies schließt Inspektion und Test des SRECS ein, um sicherzustellen, dass es die in der Spezifikation der Sicherheitsanforderungen festgelegten Anforderungen erreicht.
9: Modifikation des sicherheitsbezogenen elektrischen Steuerungssystems	Spezifikation der Anforderungen für das Modifikationsverfahren, das bei Modifikation des SRECS angewendet werden muss. Dies schließt ein: Modifikationen an irgendeinem SRECS werden geeignet geplant und vor der Ausführung überprüft, die Spezifikation der SRECS-Sicherheitsanforderungen wird eingehalten, nachdem irgendwelche Modifikationen ausgeführt worden sind.

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).

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

IEC 61000-6-2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments*.

IEC 61310 (alle Teile), *Safety of machinery – Indication, marking und actuation*.

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

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

ISO 12100-1:2003, *Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology.*

ISO 12100-2:2003, *Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles.*

ISO 13849-1:1999, *Safety of machinery – Safety related parts of control systems – Part 1: General principles for design.*

ISO 13849-2:2003, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation.*

ISO 14121, *Safety of machinery – Principles of risk assessment.*

3 Begriffe, Definitionen und Abkürzungen

3.1 Alphabetische Liste der Definitionen

Begriff	Nummer der Definition
Anforderung	3.2.25
Anteil sicherer Ausfälle	3.2.42
Anwendungssoftware	3.2.46
Architektur	3.2.35
Ausfall	3.2.39
Ausfall in Folge gemeinsamer Ursache	3.2.43
Ausfallgrenzwert	3.2.29
Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung	3.2.27
Betriebsart mit niedriger Anforderungsrate	3.2.26
Diagnosedeckungsgrad	3.2.38
einfache(s) Bauteil/Baugruppe	3.2.7
elektrisches Steuerungssystem	3.2.3
Embedded-Software	3.2.47
Fehler	3.2.30
Fehlertoleranz	3.2.31
funktionale Sicherheit	3.2.9
Funktionsblock	3.2.32
Funktionsblock-Element	3.2.33
gefahrbringender Ausfall	3.2.40
Gefährdung (durch Maschinen)	3.2.10
Gefährdungssituation	3.2.11
komplexes Bauteil	3.2.8
Maschine	3.2.1
Maschinen-Steuerungssystem	3.2.2

Begriff	Nummer der Definition
mittlere Zeit bis zum Ausfall (MTTF)	3.2.34
Programmiersprache mit eingeschränktem Sprachumfang (LVL)	3.2.49
Programmiersprache mit uneingeschränktem Sprachumfang (FVL)	3.2.48
Proof-Test	3.2.37
Risiko	3.2.13
Schutzmaßnahme	3.2.12
sicherheitsbezogene Software	3.2.50
sicherheitsbezogene Steuerungsfunktion (SRCF)	3.2.16
sicherheitsbezogenes elektrisches Steuerungssystem (SRECS)	3.2.4
Sicherheitsfunktion	3.2.15
Sicherheitsintegrität	3.2.19
Sicherheitsintegrität der Hardware	3.2.20
Sicherheitsintegrität der Software	3.2.21
Sicherheits-Integritätslevel (SIL)	3.2.23
SIL-Anspruchsgrenze	3.2.24
SRECS-Diagnosefunktion	3.2.17
SRECS-Fehlerreaktionsfunktion	3.2.18
Steuerungsfunktion	3.2.14
strukturelle Einschränkung	3.2.36
systematische Sicherheitsintegrität	3.2.22
systematischer Ausfall	3.2.45
Teilsystem	3.2.5
Teilsystem-Element	3.2.6
Validierung	3.2.52
Verifikation	3.2.51
Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH _D)	3.2.28
zufälliger Hardwarefehler	3.2.44

3.2 Begriffe und Definitionen

Für die Anwendung dieser Norm gelten die folgenden Begriffe und Definitionen.

3.2.1

Maschine

(en: **machinery**)

Gesamtheit von miteinander verbundenen Teilen oder Baugruppen, von denen mindestens eine(s) beweglich ist, mit entsprechenden Maschinen-Antriebselementen, Steuer- und Energiekreisen, die für eine bestimmte Anwendung zusammengefügt sind, insbesondere für die Verarbeitung, Behandlung, Fortbewegung oder Verpackung eines Materials

Der Begriff „Maschine“ gilt auch für Maschinenanlagen, die so angeordnet und gesteuert werden, dass sie als einheitliches Ganzes funktionieren, um das gleiche Ziel zu erreichen.

[ISO 12100-1:2003, 3.1]

3.2.2

Maschinen-Steuerungssystem

(en: **machine control system**)

System, das auf eine Eingabe reagiert, zum Beispiel vom Prozess, von anderen Maschinenelementen, von einem Benutzer, von externen Steuereinrichtungen, und eine (mehrere) Ausgabe(n) erzeugt (erzeugen), die dazu führt (führen), dass die Maschine sich in der beabsichtigten Weise verhält

3.2.3

elektrisches Steuerungssystem

(en: **electrical control system**)

alle elektrischen, elektronischen und programmierbaren elektronischen Teile des Maschinensteuerungssystems, die zum Beispiel für die betriebliche Steuerung, Überwachung, Verriegelung, Kommunikation, den Schutz und die sicherheitsbezogene Steuerungsfunktionen verwendet werden

ANMERKUNG Sicherheitsbezogene Steuerungsfunktionen können durch ein elektrisches Steuerungssystem ausgeführt werden, das entweder integraler Bestandteil oder unabhängig von den Teilen des Maschinensteuerungssystems ist, das nicht sicherheitsbezogene Funktionen ausführt.

3.2.4

sicherheitsbezogenes elektrisches Steuerungssystem

SRECS

(en: **Safety-Related Electrical Control System (SRECS)**)

elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung des Risikos (der Risiken) führt

ANMERKUNG Ein SRECS schließt alle Teile eines elektrischen Steuerungssystems ein, deren Ausfall zu einer Reduzierung oder einem Verlust der funktionalen Sicherheit führen kann. Dies kann sowohl Schaltungsteile zur elektrischen Stromversorgung als auch Steuerkreise einschließen.

3.2.5

Teilsystem

(en: **subsystem**)

Einheit des Architekturentwurfs des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Teilsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt

ANMERKUNG 1 Ein vollständiges Teilsystem kann aus einer Anzahl von identifizierbaren und getrennten Teilsystem-Elementen bestehen, die, wenn sie zusammengefügt werden, die zu dem Teilsystem zugeordneten Funktionsblöcke implementieren.

ANMERKUNG 2 Diese Definition ist eine Einschränkung der allgemeinen Definition in IEC 61508-4: „Anzahl von Elementen, die entsprechend einem Entwurf in gegenseitiger Beziehung stehen, wobei ein Element eines Systems ein anderes System, genannt Teilsystem, sein kann, das Hardware, Software und menschliche Eingriffe einschließen kann“.

ANMERKUNG 3 Diese Definition unterscheidet sich vom allgemeinen Sprachgebrauch, in dem „Teilsystem“ irgendeinen Teil einer unterteilten Einheit bedeuten kann. Der Begriff „Teilsystem“ wird in dieser Norm in einer streng definierten Hierarchie der Terminologie verwendet: „Teilsystem“ bedeutet die Unterteilung eines Systems auf oberster Ebene. Die Teile, die aus einer weiteren Unterteilung eines Teilsystems hervorgehen, werden „Teilsystem-Elemente“ genannt.

3.2.6

Teilsystem-Element

(en: **subsystem element**)

Teil eines Teilsystems, das ein einzelnes Bauteil oder irgendeine Gruppe von Bauteilen umfasst

3.2.7**einfache(s) Bauteil/Baugruppe**(en: **low complexity component**)

Bauteil/Baugruppe für das (die):

- die Ausfallarten bekannt sind und
- das Verhalten unter Fehlerbedingungen vollständig bestimmt werden kann

[IEC 61508-4, 3.4.4 modifiziert]

ANMERKUNG 1 Das Verhalten des (der) einfachen Bauteils/Baugruppe unter Fehlerbedingungen kann durch analytische und/oder Prüfverfahren bestimmt werden.

ANMERKUNG 2 Ein Teilsystem oder Teilsystem-Element, das ein oder mehrere Grenzscharter enthält, der (die) möglicherweise über zwischengeschaltete elektromechanische Relais ein oder mehrere Schütze ansteuert (ansteuern), um einen elektrischen Motor abzuschalten, ist ein Beispiel für eine einfache Baugruppe.

3.2.8**komplexe(s) Bauteil/Baugruppe**(en: **complex component**)

Bauteil/Baugruppe für das (die):

- die Ausfallarten nicht ausreichend definiert sind oder
- das Verhalten unter Fehlerbedingungen nicht vollständig bestimmt werden kann

3.2.9**funktionale Sicherheit**(en: **functional safety**)

Teil der Sicherheit der Maschine und des Maschinen-Steuerungssystems, der von der korrekten Funktion des SRECS, sicherheitsbezogener Systeme anderer Technologie und externer Einrichtungen zur Risikominderung abhängt

[IEC 61508-4, 3.1.9 modifiziert]

ANMERKUNG 1 Diese Norm betrachtet nur den Teil der funktionalen Sicherheit, der von der korrekten Funktion des SRECS in Maschinenanwendungen abhängt.

ANMERKUNG 2 ISO/IEC Guide 51 definiert Sicherheit als Freiheit von unvermeidbaren Risiken.

3.2.10**Gefährdung (durch Maschinen)**(en: **hazard (from machinery)**)

potenzielle Quelle einer Verletzung oder eines gesundheitlichen Schadens

[ISO 12100-1: 2003, 3.6 modifiziert]

ANMERKUNG Der Begriff Gefährdung kann präzisiert werden, um die Herkunft oder die Art des zu erwartenden Schadens anzugeben (z. B. Gefährdung durch elektrischen Schlag, Gefährdung durch Quetschen, Gefährdung durch Scheren, Gefährdung durch Vergiftung, Gefährdung durch Feuer).

3.2.11**Gefährdungssituation**(en: **hazardous situation**)

Sachlage, bei der eine Person einer (mehrerer) Gefährdung(en) ausgesetzt ist

[ISO 12100-1:2003, 3.9 modifiziert]

3.2.12**Schutzmaßnahme**(en: **protective measure**)

Maßnahme, die zum Erreichen einer Risikominderung vorgesehen ist

[ISO 12100-1:2003, 3.18 modifiziert]

3.2.13

Risiko

(en: **risk**)

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes

[ISO 12100-1:2003, 3.11]

3.2.14

Steuerungsfunktion

(en: **control function**)

Funktion, die Eingangsinformationen oder Signale auswertet und Ausgangsinformationen oder Aktivitäten erzeugt

3.2.15

Sicherheitsfunktion

(en: **safety function**)

Funktion einer Maschine, wobei ein Ausfall dieser Funktion zur unmittelbaren Erhöhung des Risikos (der Risiken) führen kann

[ISO 12100-1:2003, 3.28]

ANMERKUNG Diese Definition weicht von den Definitionen in IEC 61508-4 und ISO 13849-1 ab.

3.2.16

sicherheitsbezogene Steuerungsfunktion

SRCF

(en: **Safety-Related Control Function (SRCF)**)

vom SRECS ausgeführte Steuerungsfunktion mit einem festgelegten Integritätslevel, die dazu vorgesehen ist, den sicheren Zustand der Maschine aufrechtzuerhalten oder einen unmittelbaren Anstieg des (der) Risikos (Risiken) zu verhindern

3.2.17

SRECS-Diagnosefunktion

(en: **SRECS diagnostic function**)

Funktion, die dazu vorgesehen ist, Fehler in dem SRECS zu erkennen und eine festgelegte Ausgangsinformation oder Aktivität zu erzeugen, wenn ein Fehler erkannt wird

ANMERKUNG Diese Funktion ist zur Erkennung von Fehlern, die zu einem gefährbringenden Ausfall einer SRCF führen können, und zur Einleitung einer festgelegten Fehlerreaktionsfunktion vorgesehen.

3.2.18

SRECS-Fehlerreaktionsfunktion

(en: **SRECS fault reaction function**)

Funktion, die eingeleitet wird, falls durch die SRECS-Diagnosefunktion ein Fehler innerhalb eines SRECS erkannt wird

3.2.19

Sicherheitsintegrität

(en: **safety integrity**)

Wahrscheinlichkeit, dass ein SRECS oder sein Teilsystem die erforderlichen sicherheitsbezogenen Steuerungsfunktionen unter allen festgelegten Bedingungen zufrieden stellend ausführt

[IEC 61508-4, 3.5.2 modifiziert]

ANMERKUNG 1 Je höher der Sicherheits-Integritätslevel der Betrachtungseinheit ist, desto geringer ist die Wahrscheinlichkeit, dass die Betrachtungseinheit die erforderliche sicherheitsbezogene Steuerungsfunktion nicht ausführen kann.

ANMERKUNG 2 Sicherheitsintegrität umfasst Sicherheitsintegrität der Hardware (siehe 3.2.20) und systematische Sicherheitsintegrität (siehe 3.2.22).

3.2.20**Sicherheitsintegrität der Hardware**(en: **hardware safety integrity**)

Teil der Sicherheitsintegrität eines SRECS oder seiner Teilsysteme, der sowohl Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle als auch zu strukturellen Einschränkungen umfasst

[IEC 61508-4, 3.5.5 modifiziert]

3.2.21**Sicherheitsintegrität der Software**(en: **software safety integrity**)

Teil der systematischen Sicherheitsintegrität eines SRECS oder seiner Teilsysteme in Bezug auf die Fähigkeit von Software, in einem programmierbaren elektronischen System ihre sicherheitsbezogenen Steuerungsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes auszuführen

[IEC 61508-4, 3.5.3 modifiziert]

ANMERKUNG Die Sicherheitsintegrität der Software kann üblicherweise nicht präzise quantifiziert werden.

3.2.22**systematische Sicherheitsintegrität**(en: **systematic safety integrity**)

Teil der Sicherheitsintegrität eines SRECS oder seiner Teilsysteme in Bezug auf seine/ihre Widerstandsfähigkeit gegenüber systematischen Ausfällen (siehe 3.2.45) mit gefahrbringenden Auswirkungen

[IEC 61508-4, 3.5.4 modifiziert]

ANMERKUNG 1 Die systematische Sicherheitsintegrität kann üblicherweise nicht präzise quantifiziert werden.

ANMERKUNG 2 Anforderungen zur systematischen Sicherheitsintegrität betreffen sowohl Hardware- als auch Softwareaspekte eines SRECS oder seiner Teilsysteme.

3.2.23**Sicherheits-Integritätslevel****SIL**(en: **Safety Integrity Level (SIL)**)

diskrete Stufe (eine von drei möglichen) zur Festlegung der Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen Steuerungsfunktionen, die dem SRECS zugeordnet wird, wobei der Sicherheits-Integritätslevel 3 den höchsten und der Sicherheits-Integritätslevel 1 den niedrigsten Sicherheits-Integritätslevel darstellt

[IEC 61508-4, 3.5.6 modifiziert]

ANMERKUNG SIL 4 wird in dieser Norm nicht betrachtet, da er für die Anforderungen zur Risikominderung, die sich normalerweise für Maschinen ergeben, nicht relevant ist. Für auf SIL 4 zutreffende Anforderungen siehe IEC 61508-1 und IEC 61508-2.

3.2.24**SIL-Anspruchsgrenze (für ein Teilsystem)****SILCL**(en: **SIL Claim Limit (for a subsystem) (SILCL)**)

maximaler SIL, der für ein SRECS-Teilsystem in Bezug auf strukturelle Einschränkungen und systematische Sicherheitsintegrität beansprucht werden kann

3.2.25**Anforderung**(en: **demand**)

Ereignis, das das SRECS veranlasst, seine SRCF auszuführen

3.2.26

Betriebsart mit niedriger Anforderungsrate

(en: **low demand mode**)

Betriebsart, in der die Häufigkeit von Anforderungen an ein SRECS nicht mehr als einmal pro Jahr beträgt und die Häufigkeit der Anforderungen nicht größer als die doppelte Häufigkeit des Proof-Tests ist

ANMERKUNG Einrichtungen, die nur in Übereinstimmung mit den Anforderungen zur Betriebsart mit niedriger Anforderungsrate gemäß IEC 61508-1 und IEC 61508-2 entworfen worden sind, können für die Verwendung als Teil eines SRECS nach dieser Norm ungeeignet sein. Die Betriebsart mit niedriger Anforderungsrate wird für die Anwendung von SRECS an Maschinen als nicht relevant betrachtet.

3.2.27

Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung

(en: **high demand or continuous mode**)

Betriebsart, in der die Häufigkeit von Anforderungen an ein SRECS mehr als einmal pro Jahr beträgt oder die Häufigkeit der Anforderungen größer als die doppelte Häufigkeit des Proof-Tests ist

[IEC 61508-4, 3.5.12 modifiziert]

ANMERKUNG 1 Die Betriebsart mit niedriger Anforderungsrate wird für die Anwendung von SRECS an Maschinen als nicht relevant betrachtet. Daher werden in dieser Norm SRECS nur in der Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung betrachtet.

ANMERKUNG 2 Betriebsart mit Anforderungsrate bedeutet, dass eine sicherheitsbezogene Steuerungsfunktion nur auf Anfrage (Anforderung) ausgeführt wird, um die Maschine in einen festgelegten Zustand zu überführen. Das SRECS hat keinen Einfluss auf die Maschine, bis eine Anforderung an die sicherheitsbezogene Steuerungsfunktion vorliegt.

ANMERKUNG 3 Betriebsart mit kontinuierlicher Anforderung bedeutet, dass eine sicherheitsbezogene Steuerungsfunktion dauernd (kontinuierlich) ausgeführt wird, d. h. das SRECS steuert kontinuierlich die Maschine und ein (gefahrbringender) Ausfall seiner Funktion kann zu einer Gefährdung führen.

3.2.28

Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde

PFH_D

(en: **Probability of dangerous Failure per Hour (PFH_D)**)

mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls innerhalb einer Stunde

ANMERKUNG PFH_D sollte nicht mit der Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFD) verwechselt werden.

3.2.29

Ausfallgrenzwert

(en: **target failure value**)

vorgesehene PFH_D , die zu erreichen ist, um die Anforderung(en) zur Sicherheitsintegrität zu erreichen

ANMERKUNG Der Ausfallgrenzwert ist als die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde festgelegt.

[IEC 61508-4, 3.5.13 modifiziert]

3.2.30

Fehler

(en: **fault**)

anomale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit eines SRECS, eines Teilsystems oder eines Teilsystem-Elements verursachen kann, eine geforderte Funktion auszuführen

[IEC 61508-4, 3.6.1 modifiziert]

3.2.31**Fehlertoleranz**(en: **fault tolerance**)

Fähigkeit eines SRECS, eines Teilsystems oder Teilsystem-Elements, eine geforderte Funktion beim Vorhandensein von Fehlern oder Ausfällen weiter auszuführen

[IEC 61508-4, 3.6.3 modifiziert]

3.2.32**Funktionsblock**(en: **function block**)

kleinstes Element einer SRCF, dessen Ausfall zu einem Ausfall der SRCF führen kann

ANMERKUNG 1 In dieser Norm kann eine SRCF (F) als die logische Summe (UND) der Funktionsblöcke (FB) betrachtet werden, d. h. $F = FB_1 \text{ UND } FB_2 \text{ UND } FB_n$.

ANMERKUNG 2 Diese Definition eines Funktionsblocks unterscheidet sich von der in IEC 61131-3 und anderen Normen verwendeten Definition.

3.2.33**Funktionsblock-Element**(en: **function block element**)

Teil eines Funktionsblocks

3.2.34**mittlere Zeit bis zum Ausfall****MTTF**(en: **Mean Time To Failure (MTTF)**)

Erwartung der mittleren Zeit bis zum Ausfall

[IEV 191-12-07, modifiziert]

ANMERKUNG Die MTTF wird üblicherweise als ein Mittelwert der erwarteten Zeit bis zum Ausfall ausgedrückt.

3.2.35**Architektur**(en: **architecture**)

spezifische Konfiguration von Hardware- und Softwareelementen in einem SRECS

[IEC 61508-4, 3.3.5 modifiziert]

3.2.36**strukturelle Einschränkung**(en: **architectural constraint**)

Anzahl von strukturellen Anforderungen, die den SIL einschränken, der für ein Teilsystem geltend gemacht werden kann

ANMERKUNG Anforderungen zu strukturellen Einschränkungen sind in 6.7.6 enthalten.

3.2.37**Proof-Test**(en: **proof test**)

Prüfung, die Fehler oder eine Verschlechterung in einem SRECS und seinen Teilsystemen erkennen kann, so dass, falls notwendig, das SRECS und seine Teilsysteme in einen „Wie-Neu-Zustand“ oder so nah wie praktisch möglich diesen Zustand entsprechend, wiederhergestellt werden können

[IEC 61508-4, 3.8.5 modifiziert]

ANMERKUNG Ein Proof-Test ist zur Bestätigung vorgesehen, dass das SRECS sich in einem Zustand befindet, der die festgelegte Sicherheitsintegrität garantiert.

NATIONALE ANMERKUNG In **DIN EN 61508-4:2002** ist der englische Begriff „proof test“ mit „Wiederholungsprüfung“ übersetzt. Da dieser Begriff im Maschinenbereich jedoch nicht üblich ist, wurde in dieser Übersetzung der EN 62061 der englische Begriff beibehalten.

3.2.38

Diagnosedeckungsgrad

(en: **diagnostic coverage**)

Abnahme der Wahrscheinlichkeit gefahrbringender Hardwareausfälle, die aus der Ausführung der automatischen Diagnosetests resultiert

[IEC 61508-4, 3.8.6 modifiziert]

ANMERKUNG Der Diagnosedeckungsgrad (DC) kann nach folgender Gleichung berechnet werden:

$$DC = \sum \lambda_{DD} / \lambda_{Dtotal}$$

wobei λ_{DD} die Rate erkannter gefahrbringender Hardwareausfälle ist und λ_{Dtotal} die Rate aller gefahrbringenden Hardwareausfälle ist.

3.2.39

Ausfall

(en: **failure**)

Beendigung der Fähigkeit eines SRECS, eines Teilsystems oder eines Teilsystem-Elements, eine geforderte Funktion zu auszuführen

[IEC 61508-4, 3.6.4 modifiziert und ISO 12100-1:2003, 3.32]

ANMERKUNG Ausfälle sind entweder zufällig (in Hardware) oder systematisch (in Hardware oder Software) bedingt.

3.2.40

gefahrbringender Ausfall

(en: **dangerous failure**)

Ausfall eines SRECS, eines Teilsystems oder eines Teilsystem-Elements mit dem Potenzial eine Gefährdung oder einen funktionsunfähigen Zustand zu verursachen

[IEC 61508-4, 3.6.7 modifiziert]

ANMERKUNG 1 Ob sich die Auswirkungen ergeben oder nicht, kann von der Kanalstruktur des Systems abhängen, zum Beispiel ist es in Systemen mit mehreren Kanälen zur Erhöhung der Sicherheit weniger wahrscheinlich, dass ein gefahrbringender Ausfall der Hardware zu dem gefahrbringenden Gesamtzustand oder einem Zustand des Ausfalls der Funktion führt.

ANMERKUNG 2 In einem Teilsystem mit mehreren Kanälen kann die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Teilsystems geringer als die gefahrbringende Ausfallrate eines Kanals sein, der das Teilsystem bildet. Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls eines SRECS kann nicht geringer als die irgendeines Teilsystems sein, das Teil des SRECS ist. (Diese Tatsache ist durch die spezielle Definition eines „Teilsystems“ in dieser Norm begründet.)

ANMERKUNG 3 Ein gefahrbringender Ausfall führt üblicherweise zu einem Ausfall oder zu einem möglichen Ausfall in der Ausführung der SRCF.

3.2.41

sicherer Ausfall

(en: **safe failure**)

Ausfall eines SRECS, eines Teilsystems oder eines Teilsystem-Elements, der nicht das Potenzial hat, eine Gefährdung zu verursachen

[IEC 61508-4, 3.6.8 modifiziert]

ANMERKUNG Ein sicherer Ausfall führt nicht zu einem Ausfall oder möglichen Ausfall in der Ausführung der SRCF.

3.2.42**Anteil sicherer Ausfälle****SFF**(en: **Safe Failure Fraction (SFF)**)

Anteil an der Gesamtausfallrate eines Teilsystems, der nicht zu einem gefahrbringenden Ausfall führt

ANMERKUNG Der Anteil sicherer Ausfälle (*SFF*) kann nach folgender Gleichung berechnet werden:

$$(\sum \lambda_S + \sum \lambda_{DD}) / (\sum \lambda_S + \sum \lambda_D)$$

wobei

 λ_S die Rate sicherer Ausfälle ist, $\sum \lambda_S + \sum \lambda_D$ die Gesamtausfallrate ist, λ_{DD} die Rate gefahrbringender Ausfälle ist, die durch die Diagnosefunktionen erkannt werden und λ_D die Rate gefahrbringender Ausfälle ist.

Der Diagnosedeckungsgrad (soweit vorhanden) jedes Teilsystems des SRECS wird bei der Berechnung der Wahrscheinlichkeit zufälliger Hardwareausfälle berücksichtigt. Der Anteil sicherer Ausfälle wird bei der Festlegung der strukturellen Einschränkungen der Sicherheitsintegrität der Hardware berücksichtigt (siehe 6.7.7).

3.2.43**Ausfall in Folge gemeinsamer Ursache****CCF**(en: **Common Cause Failure (CCF)**)

Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die gleichzeitig Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen Teilsystem (redundante Architektur) verursachen und zu einem Ausfall eines SRECS führen

[IEC 61508-4, 3.6.10 modifiziert]

ANMERKUNG Diese Definition unterscheidet sich von den in ISO 12100-1 und IEC 191-04-23 angegebenen.

3.2.44**zufälliger Hardwarefehler**(en: **random hardware failure**)

Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Verschlechterungsmechanismen in der Hardware resultiert

[IEC 61508-4, 3.6.5]

3.2.45**systematischer Ausfall**(en: **systematic failure**)

Ausfall, der eindeutig mit einer bestimmten Ursache in Beziehung steht, die nur durch eine Änderung des Entwurfs oder des Fertigungsprozesses, der Betriebsverfahren, der Dokumentation oder anderer relevanter Faktoren beseitigt werden kann

[IEC 61508-4, 3.6.6]

ANMERKUNG 1 Eine verbessernde Instandhaltung ohne Modifikation beseitigt in der Regel nicht die Ursache eines Ausfalls.

ANMERKUNG 2 Durch die Simulation der Ursache eines Ausfalls kann ein systematischer Ausfall ausgelöst werden.

ANMERKUNG 3 Beispiele von Ursachen für systematische Ausfälle schließen menschliches Versagen in Folgendem ein:

- der Spezifikation der Sicherheitsanforderungen;
- dem Entwurf, der Herstellung, der Installation und/oder dem Betrieb der Hardware;
- dem Entwurf und/oder der Implementierung der Software.

3.2.46

Anwendungssoftware

(en: **application software**)

Software speziell für die Anwendung, die durch den Entwickler des SRECS implementiert wird und im Allgemeinen logische Abfolgen, Grenzen und Ausdrücke enthält, die die passende Eingabe, Ausgabe, Berechnungen und Entscheidungen steuern, welche erforderlich sind, um die funktionalen Anforderungen des SRECS zu erreichen

3.2.47

Embedded-Software

(en: **embedded software**)

vom Hersteller gelieferte Software, die Teil des SRECS ist und die üblicherweise nicht für Modifikationen zugänglich ist

ANMERKUNG Firmware und Betriebssystemsoftware sind Beispiele für Embedded-Software.

3.2.48

Programmiersprache mit uneingeschränktem Sprachumfang

FVL

(en: **Full Variability Language (FVL)**)

Sprachentypus, der die Möglichkeit zur Verfügung stellt, eine große Vielfalt von Funktionen und Anwendungen auszuführen

[IEC 61511-1, 3.2.81.1.3 modifiziert]

ANMERKUNG 1 Typisches Beispiel für Systeme, die FVL verwenden, sind Rechner für allgemeine Anwendungen.

ANMERKUNG 2 FVL findet sich üblicherweise in Embedded-Software und wird selten in Anwendungssoftware verwendet.

ANMERKUNG 3 Beispiele für FVL schließen ein: Ada, C, Pascal, Anweisungsliste, Assemblersprachen, C++, Java, SQL.

3.2.49

Programmiersprache mit eingeschränktem Sprachumfang

LVL

(en: **Limited Variability Language (LVL)**)

Sprachentypus, der die Möglichkeit zur Verfügung stellt, vordefinierte, anwendungsspezifische und Bibliotheksfunktionen zu kombinieren, um die Spezifikationen der Sicherheitsanforderungen auszuführen

[IEC 61511-1, 3.2.81.1.2 modifiziert]

ANMERKUNG 1 Eine LVL ergibt eine enge funktionale Übereinstimmung mit den Funktionen, die zum Ausführen der Anwendung erforderlich sind.

ANMERKUNG 2 Typische Beispiele für LVL sind in IEC 61131-3 enthalten. Diese schließen Kontaktplan, Funktionsblockdiagramm und Funktionsablaufplan ein. Anweisungslisten und strukturierter Text werden nicht als LVL betrachtet.

ANMERKUNG 3 Typisches Beispiel für Systeme, die LVL verwenden: Speicherprogrammierbare Steuerung (SPS) im Einsatz zur Maschinensteuerung.

3.2.50**sicherheitsbezogene Software**(en: **safety-related software**)

Software, die zur Ausführung von sicherheitsbezogenen Steuerungsfunktionen in einem sicherheitsbezogenen System verwendet wird

3.2.51**Verifikation**(en: **verification**)

Bestätigung durch Untersuchung (z. B. Tests, Analysen), dass das SRECS, seine Teilsysteme oder Teilsystem-Elemente die durch die zugehörige Spezifikation gestellten Anforderungen erfüllen

[IEC 61508-4, 3.8.1 modifiziert und IEC 61511-1, 3.2.92 modifiziert]

ANMERKUNG Die Verifikationsergebnisse sollten einen dokumentierten Nachweis der Ziele liefern.

BEISPIEL: Verifikationsaktivitäten schließen ein:

- Überprüfungen von Ergebnissen (Dokumente aus allen Phasen), um Übereinstimmung mit den Zielen und Anforderungen der Phase unter Berücksichtigung der spezifischen Eingaben für diese Phase sicherzustellen;
- Überprüfungen des Entwurfs;
- Tests, die an den entworfenen Produkten ausgeführt werden, um sicherzustellen, dass die Produkte entsprechend ihrer Spezifikation arbeiten;
- Ausführung von Integrationstests, wo verschiedene Teile eines Systems schrittweise zusammengefügt werden und durch die Ausführung von Prüfungen zu Umgebungseinflüssen sicherzustellen, dass alle Teile in der festgelegten Art und Weise zusammenwirken.

3.2.52**Validierung**(en: **validation**)

Bestätigung durch Untersuchung (z. B. Tests, Analysen), dass das SRECS die Anforderungen zur funktionalen Sicherheit der spezifischen Anwendung erfüllt

[IEC 61508-4, 3.8.2 modifiziert]

3.3 Abkürzungen

Die folgenden Abkürzungen werden in dieser Norm verwendet.

CCF	Ausfall (Ausfälle) in Folge gemeinsamer Ursache
DC	Diagnosedeckungsgrad
EMV	Elektromagnetische Verträglichkeit
FB	Funktionsblock
FVL	Programmiersprache mit uneingeschränktem Sprachumfang
E/A	Eingang/Ausgang
LVL	Programmiersprache mit eingeschränktem Sprachumfang
PFH_D	Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde
MTTF	mittlere Zeit bis zum Ausfall
MTTR	mittlere Zeit bis zur Wiederherstellung
P_{TE}	Wahrscheinlichkeit eines gefahrbringenden Übertragungsfehlers
SFF	Anteil sicherer Ausfälle
SIL	Sicherheits-Integritätslevel
SILCL	Sicherheits-Integritätslevel (SIL) Anspruchsgrenze (für Teilsysteme)
SI	sicherheitsbezogen
SRECS	sicherheitsbezogenes elektrisches Steuerungssystem
SRCF	sicherheitsbezogene Steuerungsfunktion
SRS	Spezifikation der Sicherheitsanforderungen
SYS	System

4 Management der funktionalen Sicherheit

4.1 Ziel

Dieser Abschnitt legt Managementaktivitäten und technische Aktivitäten fest, die für das Erreichen der erforderlichen funktionalen Sicherheit des SRECS notwendig sind.

4.2 Anforderungen

4.2.1 Es muss ein Plan der funktionalen Sicherheit erstellt und für jedes SRECS-Entwurfsprojekt dokumentiert und wie erforderlich aktualisiert werden. Der Plan muss Verfahren für die Steuerung der in den [Abschnitten 5 bis 9](#) festgelegten Aktivitäten einschließen.

ANMERKUNG 1 Der Inhalt des Plans der funktionalen Sicherheit sollte von den jeweiligen Umständen abhängen, diese können Folgendes einschließen:

- Größe des Projektes;
- Grad der Komplexität;
- Innovationsgrad des Entwurfs und der Technologie;
- Normungsstand zu den Charakteristika des Entwurfs;
- mögliche Auswirkung(en) beim Auftreten eines Ausfalls.

Im Einzelnen muss der Plan:

- a) die in den [Abschnitten 5 bis 9](#) festgelegten relevanten Aktivitäten identifizieren;
- b) die Vorgehensweise und die Strategie zur Erfüllung der festgelegten Anforderungen zur funktionalen Sicherheit beschreiben;
- c) die Strategie zum Erreichen der funktionalen Sicherheit für die Anwendungssoftware, Entwicklung, Integration, Verifikation und Validierung beschreiben;
- d) Personen, Abteilungen oder andere Einheiten und Ressourcen, die für die Ausführung und Überprüfung aller in den [Abschnitten 5 bis 9](#) festgelegten Aktivitäten verantwortlich sind, bestimmen;
- e) die Verfahren und Ressourcen zur Protokollierung und Pflege der für die funktionale Sicherheit eines SRECS relevanten Informationen identifizieren oder festsetzen;

ANMERKUNG 2 Folgendes sollte betrachtet werden:

- die Ergebnisse der Ermittlung der Gefährdungen und der Risikobeurteilung;
 - die für die sicherheitsbezogenen Funktionen verwendeten Einrichtungen zusammen mit ihren Sicherheitsanforderungen;
 - die für das Bewahren der funktionalen Sicherheit verantwortliche Organisation;
 - die Verfahren, die notwendig sind, um die funktionale Sicherheit zu erreichen und aufrechtzuerhalten (einschließlich SRECS-Modifikationen).
- f) die Strategie für ein Konfigurationsmanagement (siehe [9.3](#)) unter Berücksichtigung der relevanten organisatorischen Aspekte, wie zum Beispiel autorisierte Personen und interne Strukturen der Organisation, beschreiben;
 - g) einen Verifikationsplan einrichten, der Folgendes einschließen muss:
 - Einzelheiten, wann die Verifikation stattfinden muss;
 - Einzelheiten zu den Personen, Abteilungen oder Einheiten, die die Verifikation ausführen müssen;
 - die Auswahl der Verifikationsstrategien und Verifikationstechniken;
 - die Auswahl und Verwendung von Testeinrichtungen;
 - die Auswahl der Verifikationsaktivitäten;
 - Akzeptanzkriterien und
 - die zu verwendenden Mittel zur Bewertung der Verifikationsergebnisse;
 - h) einen Validierungsplan einrichten, bestehend aus:
 - Einzelheiten, wann die Validierung stattfinden muss;
 - Identifizierung der relevanten Betriebsarten der Maschine (z. B. Normalbetrieb, Einrichten);
 - Anforderungen, gegen die das SRECS zu validieren ist;
 - der technischen Strategie zur Validierung, zum Beispiel analytische Verfahren oder statistische Tests;
 - Akzeptanzkriterien und
 - auszuführenden Aktionen bei Nichterreichen der Akzeptanzkriterien.

ANMERKUNG 3 Der Validierungsplan sollte anzeigen, ob das SRECS und seine Teilsysteme Gegenstand einer Routineprüfung, einer Bauartprüfung und/oder einer Stichprobenprüfung sein sollen.

4.2.2 Der Plan der funktionalen Sicherheit muss implementiert werden, um eine sofortige Weiterverfolgung und zufrieden stellende Lösung der für ein SRECS relevanten Punkte sicherzustellen, die von Folgendem herrühren:

- in den [Abschnitten 5 bis 9](#) festgelegten Aktivitäten;
- Verifikationsaktivitäten und
- Validierungsaktivitäten.

5 Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen (SRCFs)

5.1 Ziel

Dieser Abschnitt beschreibt die Verfahren zur Spezifikation der Anforderungen für SRCF(s), die durch das SRECS zu implementieren sind.

5.2 Spezifikation der Anforderungen für SRCFs

5.2.1 Allgemeines

5.2.1.1 Jede Notwendigkeit für Sicherheitsfunktionen ergibt sich aus der in ISO 12100-1, ISO 12100-2 und ISO 14121 skizzierten Strategie zur Risikominderung.

5.2.1.2 Wo Sicherheitsfunktionen ausgewählt werden, um durch SRECS ausgeführt zu werden (vollständig oder teilweise), muss (müssen) das (die) zugehörige(n) SRCF(s) (siehe [3.2.16](#)) spezifiziert werden.

5.2.1.3 Die Spezifikationen jeder SRCF müssen einschließen:

- Spezifikation der funktionalen Anforderungen (siehe [5.2.3](#));
- Spezifikation der Anforderungen zur Sicherheitsintegrität (siehe [5.2.4](#))

und diese müssen in der Spezifikation der Sicherheitsanforderungen (SRS) dokumentiert werden.

ANMERKUNG 1 Wo nichtelektrische Einrichtungen zur Ausführung einer Sicherheitsfunktion in Kombination mit elektrischen Mitteln beitragen, wird (werden) der (die) auf nichtelektrische Einrichtungen bezogene(n) Ausfallgrenzwert(e) im Rahmen dieser Norm nicht betrachtet. Elektrische Mittel umfassen alle Geräte oder Systeme, die auf Basis elektrischer Prinzipien arbeiten, einschließlich:

- elektromechanische Einrichtungen;
- nichtprogrammierbare elektronische Einrichtungen;
- programmierbare elektronische Einrichtungen.

ANMERKUNG 2 Die SRS muss als Teil der Konfigurationsmanagementverfahren (siehe [9.3](#)) Gegenstand der Versionskontrolle sein.

5.2.1.4 Die Spezifikation der Sicherheitsanforderungen muss verifiziert werden, um Konsistenz und Vollständigkeit für ihre vorgesehene Verwendung sicherzustellen.

ANMERKUNG Dies kann zum Beispiel durch Inspektion, Analyse, Checklisten erreicht werden. Siehe auch [B.2.6 von IEC 61508-7](#).

5.2.2 Benötigte Informationen

Die folgenden Informationen müssen verwendet werden, um sowohl die Spezifikation der funktionalen Anforderungen als auch die Spezifikation der Anforderungen zur Sicherheitsintegrität jeder SRCF zu erstellen:

- Ergebnisse der Risikobeurteilung für die Maschine einschließlich aller für den Prozess der Risikominderung für jede spezielle Gefährdung als notwendig bestimmten Sicherheitsfunktionen;
- Betriebscharakteristika der Maschine, einschließlich:
 - Betriebsarten,
 - Zykluszeit,
 - Leistungsfähigkeit in Bezug auf Reaktionszeit,
 - Umgebungsbedingungen,
 - Zusammenwirken der Person(en) und der Maschine (z. B. Reparatur, Einrichten, Reinigung);

- alle in Bezug auf die SRCFs relevanten Informationen, die einen Einfluss auf den Entwurf des SRECS haben können, einschließlich zum Beispiel:
 - eine Beschreibung des Verhaltens der Maschine, das eine SRCF erreichen oder verhindern soll;
 - alle Schnittstellen zwischen den SRCFs und zwischen SRCFs und jeder anderen Funktion (entweder innerhalb oder außerhalb der Maschine);
 - erforderliche Fehlerreaktionsfunktionen der SRCF.

ANMERKUNG Einige Informationen sind eventuell nicht vorhanden oder ausreichend definiert, bevor der iterative Entwurfsprozess des SRECS beginnt, so dass es erforderlich sein kann, die Spezifikation der SRECS-Sicherheitsanforderungen während des Entwurfsprozesses zu aktualisieren.

5.2.3 Spezifikation der funktionalen Anforderungen für SRCFs

5.2.3.1 Die Spezifikation der funktionalen Anforderungen für SRCFs muss Details jeder auszuführenden SRCF beschreiben, einschließlich soweit zutreffend:

- die Bedingung(en) (z. B. Betriebsart) der Maschine, unter der (denen) die SRCF aktiv oder unwirksam sein muss;
- die Priorität derjenigen Funktionen, die gleichzeitig aktiv sein können und die in Widerspruch stehende Aktionen auslösen können;
- Häufigkeit der Ausführung jeder SRCF;
- die erforderliche Reaktionszeit jeder SRCF;
- die Schnittstelle(n) der SRCFs zu anderen Maschinenfunktionen;
- die erforderlichen Reaktionszeiten (z. B. von Eingabe- und Ausgabegeräten);
- eine Beschreibung jeder SRCF;
- eine Beschreibung der Fehlerreaktionsfunktion(en) und aller Einschränkungen für zum Beispiel Wiederanlauf oder weiteren Betrieb der Maschine in Fällen, in denen die ursprüngliche Fehlerreaktion die Maschine stillsetzen soll;
- eine Beschreibung der Betriebsumgebung (z. B. Temperatur, Feuchtigkeit, Staub, chemische Substanzen, mechanische Vibrationen und Schock);
- Tests und alle zugehörigen Einrichtungen (z. B. Testeinrichtungen, Testschnittstellen);
- Rate der Betriebszyklen, Nutzungsfaktor und/oder Gebrauchskategorie für elektromechanische Komponenten, die zum Einsatz in der SRCF vorgesehen sind.

5.2.3.2 Zusätzlich zu den Anforderungen der [IEC 61000-6-2](#) sind für den Fall, dass ein SRCS für die Verwendung in industrieller Umgebung vorgesehen ist, in Anhang E elektromagnetische (EM) Störfestigkeitsgrade angegeben. Für SRECS, die zur Verwendung in anderen elektromagnetischen Umgebungen (z. B. Wohnbereich) vorgesehen sind, sollten Störfestigkeitsgrade angewendet werden, die auf Werten basieren, die in anderen EMV-Normen festgelegt wurden (z. B. für den Wohnbereich, [IEC 61000-6-1](#)).

ANMERKUNG 1 Bei der Festlegung von EM-Störfestigkeitsgraden ist es erforderlich zu betrachten, ob die in verschiedenen EMV-Normen verwendeten Grade Fälle umfassen, die in einer SRECS-Anwendung auftreten können, selbst wenn die Auftrittswahrscheinlichkeit gering ist.

ANMERKUNG 2 Das Bewertungskriterium der elektromagnetischen Störfestigkeit für funktionale Sicherheit eines SRECS ist in [6.4.3](#) angegeben.

5.2.4 Spezifikation der Anforderungen zur Sicherheitsintegrität für SRCFs

5.2.4.1 Die Anforderungen zur Sicherheitsintegrität für jede SRCF müssen aus der Risikobeurteilung abgeleitet werden, um sicherzustellen, dass die notwendige Risikominderung erreicht werden kann. In dieser Norm ist eine Anforderung zur Sicherheitsintegrität als ein Ausfallgrenzwert für die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde jeder SRCF ausgedrückt.

5.2.4.2 Die Anforderungen zur Sicherheitsintegrität für jede SRCF müssen in Form eines SIL in Übereinstimmung mit Tabelle 3 festgelegt und dokumentiert werden. Ein Beispiel einer Methodologie ist in [Anhang A](#) angegeben.

Tabelle 3 – Sicherheits-Integritätslevels: Ausfallgrenzwerte für SRCFs

Sicherheits-Integritätslevel	Wahrscheinlichkeit eines gefährbringenden Ausfalls pro Stunde (PFH_D)
3	$\geq 10^{-8}$ bis $< 10^{-7}$
2	$\geq 10^{-7}$ bis $< 10^{-6}$
1	$\geq 10^{-6}$ bis $< 10^{-5}$

ANMERKUNG Wenn die erforderliche Sicherheitsintegrität einer SRCF geringer als SIL 1 ist, sollten zumindest die Anforderungen der Kategorie B nach ISO 13849-1 erfüllt sein.

5.2.4.3 Wenn eine Produktnorm einen SIL für eine SRCF festlegt, muss diese Festlegung Vorrang gegenüber [Anhang A](#) haben.

6 Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)

6.1 Ziel

Dieser Abschnitt legt Anforderungen für die Auswahl oder den Entwurf eines SRECS fest, um die in der Spezifikation der Sicherheitsanforderungen (siehe [5.2](#)) festgelegten funktionalen Anforderungen und die Anforderungen zur Sicherheitsintegrität zu erfüllen.

6.2 Allgemeine Anforderungen

6.2.1 Das SRECS muss unter Berücksichtigung der zutreffenden Anforderungen dieser Norm so ausgewählt oder entworfen werden, dass die Spezifikation der Sicherheitsanforderungen (siehe [5.2](#)) und wo relevant die Spezifikation der Software-Sicherheitsanforderungen (siehe [6.10](#)) erfüllt werden.

6.2.2 Die Auswahl oder der Entwurf des SRECS (einschließlich der gesamten Hardware- und Softwarearchitektur, Sensoren, Aktoren, programmierbarer Elektronik, Embedded-Software, Anwendungssoftware usw.) muss entweder [6.5](#) oder [6.6](#) entsprechen. Unabhängig davon, welches Verfahren verwendet wird, muss das SRECS die folgenden Anforderungen erfüllen:

- a) die Anforderungen zur Sicherheitsintegrität der Hardware, bestehend aus:
 - den strukturellen Einschränkungen zur Sicherheitsintegrität der Hardware (siehe [6.6.3.3](#)) und
 - den Anforderungen zur Wahrscheinlichkeit gefährbringender zufälliger Hardwareausfälle (siehe [6.6.3.2](#));
- b) die Anforderungen zur systematischen Sicherheitsintegrität (siehe [6.4](#)), bestehend aus:
 - den Anforderungen zur Vermeidung von Ausfällen und
 - den Anforderungen zur Beherrschung systematischer Fehler;
- c) die Anforderungen zum SRECS-Verhalten bei Erkennung eines Fehlers (siehe [6.3](#));
- d) die Anforderungen für den Entwurf und die Entwicklung von sicherheitsbezogener Software (siehe [6.10](#) und [6.11](#)).

6.2.3 Der Entwurf des SRECS muss menschliche Fähigkeiten und Einschränkungen (einschließlich vernünftigerweise vorhersehbare Fehlanwendung) berücksichtigen und muss für die notwendigen Handlungen des Bedien- und Instandhaltungspersonals und anderen, die auf das SRECS einwirken könnten, geeignet sein. Der Entwurf aller Bedienerschnittstellen muss guter praktischer Erfahrung folgen (siehe Normenreihe IEC 60310) und muss auf den wahrscheinlichen Ausbildungsstand oder das Bewusstsein der Benutzer abgestimmt sein, besonders bei in großen Stückzahlen produzierten Teilsystemen, wo der Benutzer ein Teil der Öffentlichkeit sein kann.

ANMERKUNG Es sollte Entwurfsziel sein, dass vernünftigerweise vorhersehbare Irrtümer, die von Benutzern oder dem Instandhaltungspersonal gemacht werden, durch den Entwurf verhindert oder beseitigt werden. Wo dies nicht möglich ist, sollten auch andere Maßnahmen angewendet werden (z. B. manuelle Handlungen mit nachfolgender Bestätigung vor Ausführung), um die Möglichkeit des durch den Bediener bedingten Versagens zu minimieren und sicherzustellen, dass vorhersehbare Irrtümer nicht zu einem gesteigerten Risiko führen.

6.2.4 Während des Entwurfs und der Integration müssen Instandhaltbarkeit und Testbarkeit berücksichtigt werden, um die Implementierung dieser Eigenschaften in das SRECS zu erleichtern.

6.2.5 Der Entwurf des SRECS einschließlich seiner Diagnose- und Fehlerreaktionsfunktionen muss dokumentiert werden. Diese Dokumentation muss:

- genau, vollständig und knapp sein;
- für ihren vorgesehenen Zweck geeignet sein;
- verfügbar und pflegbar sein;
- der Versionskontrolle unterliegen.

6.2.6 Die Ergebnisse der während des Entwurfs, der Entwicklung und der Implementierung des SRECS ausgeführten Aktivitäten müssen an angemessenen Stufen verifiziert werden.

6.3 Anforderungen zum Verhalten (des SRECS) bei Erkennung eines Fehlers im SRECS

6.3.1 Die Erkennung eines gefahrbringenden Fehlers in irgendeinem Teilsystem, das eine Hardware-Fehlertoleranz von mehr als null besitzt, muss zur Ausführung der spezifizierten Fehlerreaktionsfunktion führen.

Die Spezifikation kann eine Isolation des fehlerhaften Bestandteils des Teilsystems vorsehen, um den sicheren Betrieb der Maschine fortzusetzen, während der fehlerhafte Bestandteil repariert wird. Ist dies vorgesehen, und die Reparatur wird nicht innerhalb der maximal veranschlagten Zeit, wie in der Berechnung der Wahrscheinlichkeit eines zufälligen Hardwareausfalls (siehe 6.7.8) angenommen, abgeschlossen, muss eine zweite Fehlerreaktion ausgeführt werden, um einen sicheren Zustand aufrechtzuerhalten.

Wenn das SRECS für Reparatur während des Betriebs vorgesehen ist, darf Isolation eines fehlerhaften Bestandteils nur angewendet werden, wenn dies nicht zu einem Anstieg der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls über die in der SRS festgelegte Wahrscheinlichkeit führt.

Nach dem Auftreten von Fehlern, die die Hardware-Fehlertoleranz zu null reduzieren, müssen die Anforderungen aus 6.3.2 angewendet werden.

ANMERKUNG Die mittlere Zeit bis zur Wiederherstellung (siehe IEC 191-13-08), die im Zuverlässigkeitsmodell betrachtet wird, muss das Diagnose-Testintervall, die Reparaturzeit und alle anderen Verzögerungen vor der Wiederherstellung berücksichtigen.

6.3.2 Wenn eine (mehrere) Diagnosefunktion(en) zum Erreichen der erforderlichen Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls notwendig ist (sind) und das Teilsystem eine Hardware-Fehlertoleranz von null besitzt, muss die Fehlererkennung und spezifizierte Fehlerreaktion ausgeführt werden, bevor die Gefährdungssituation in Bezug auf die SRCF auftreten kann.