DIN EN 62061 (VDE 0113-50)

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.

ICS 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)

Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin · 10.05 vwu

Preisgr. 54 K
VDE-Vertr.-Nr. 0113016

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 Datenverarbeitssysteme – 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, Bregriffe, 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 –

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN 62061

April 2005

ICS 13.110; 25.040.99; 29.020

Deutsche Fassung

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

Ref. Nr. EN 62061:2005 D

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

Seite

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.

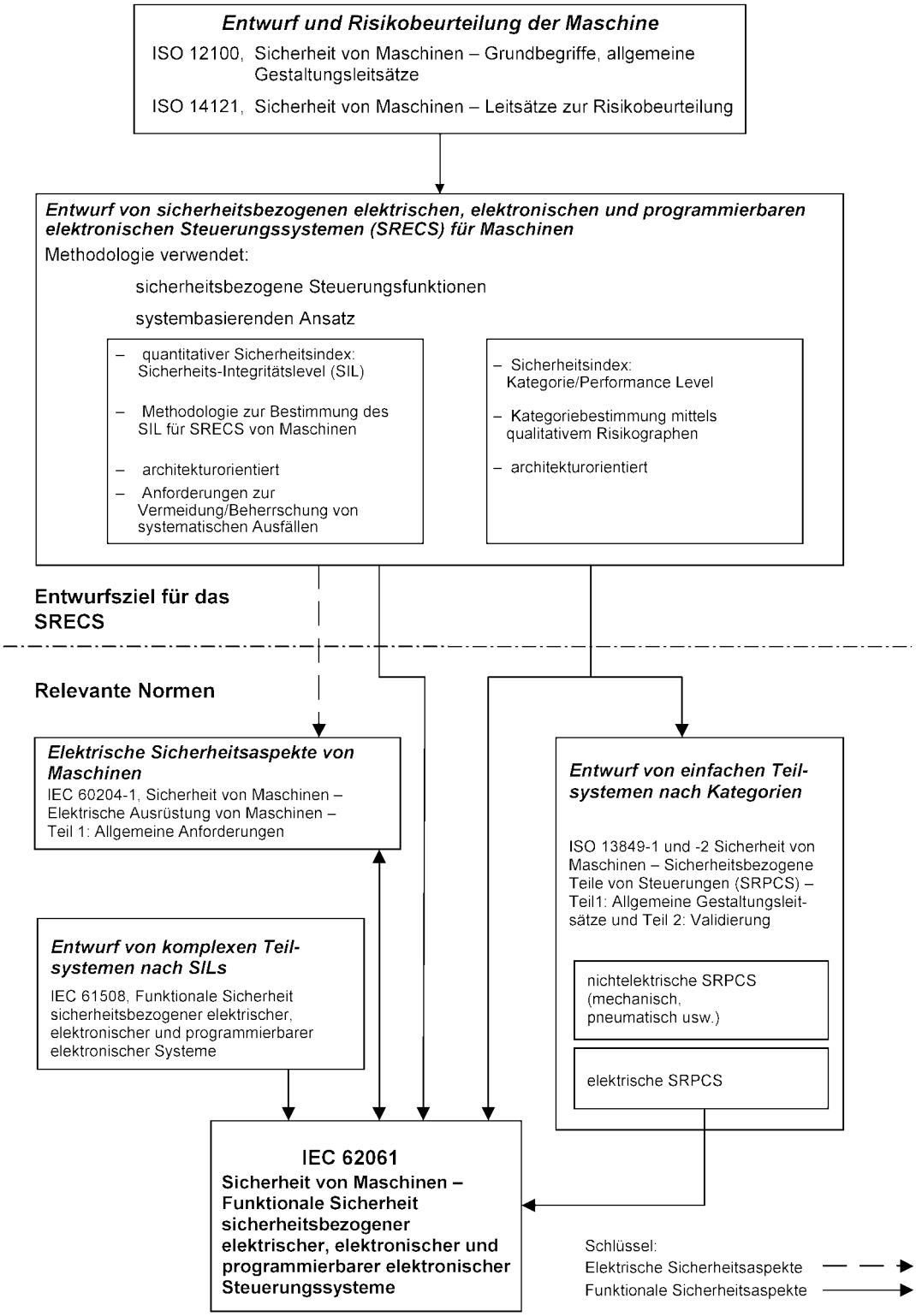


Bild 1 – Verhältnis der IEC 62061 zu anderen relevanten Normen

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 sicherheitsbezogene(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 sicherheits-bezogenen 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 sicherheits-bezogenen 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 Grenzschalter 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 unvertretbaren 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 gefahrbringenden 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. $F = FB_1$ UND FB_2 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:

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

wobei λ_{DD} die Rate erkannter gefahrbringender Hardwareausfälle ist und $\lambda_{\mathrm{Dtotal}}$ 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:

$$\left(\Sigma\lambda_S + \Sigma\lambda_{DD}\right) / \left(\Sigma\lambda_S + \Sigma\lambda_D\right)$$

wobei

λ_S die Rate sicherer Ausfälle ist,

$\Sigma\lambda_S + \Sigma\lambda_D$ 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 IEV 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 gefahrbringenden 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 gefahrbringender 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 IEV 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.

AUSNAHME zu 6.3.2: Im Falle eines Teilsystems, das eine bestimmte SRCF ausführt, bei der die Hardware-Fehlertoleranz null beträgt und das Verhältnis der Diagnose-Testrate zur Anforderungsrate den Wert 100 überschreitet, muss das Diagnose-Testintervall dieses Teilsystems so gewählt sein, dass das Teilsystem die Anforderung zur Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls erfüllt.

6.3.3 Wenn die Ausführung einer Fehlerreaktionsfunktion als Teil einer SRCF, die als SIL 3 festgelegt ist, zu einem Stopp der Maschine geführt hat, darf der nachfolgende Normalbetrieb der Maschine über das SRECS (z. B. Zustimmung zum Wiederanlauf der Maschine) nicht möglich sein, bevor der Fehler repariert oder korrigiert worden ist. Für SRCFs mit einer festgelegten Sicherheitsintegrität geringer als SIL 3 muss das Verhalten der Maschine nach Ausführung einer Fehlerreaktionsfunktion (z. B. Wiederingangsetzen des Normalbetriebs) von der Spezifikation der relevanten Fehlerreaktionsfunktionen (siehe 5.2.3) abhängen.

6.4 Anforderungen zur systematischen Sicherheitsintegrität des SRECS

ANMERKUNG Diese Anforderungen sind auf „Systemebene“ anwendbar, wo Teilsysteme miteinander verbunden werden, um ein SRECS zu realisieren. Für Anforderungen in Bezug auf die Realisierung von Teilsystemen siehe 6.7.8.

6.4.1 Anforderungen zur Vermeidung von systematischen Hardwareausfällen

6.4.1.1 Die folgenden Maßnahmen müssen angewendet werden:

a) das SRECS muss in Übereinstimmung mit dem Plan der funktionalen Sicherheit (siehe 4.2) entworfen und implementiert werden;

b) richtige Auswahl, Kombination, Anordnungen, Zusammenbau und Installation von Teilsystemen, einschließlich Verkabelung, Verdrahtung und anderer Verbindungen;

c) Verwendung des SRECS innerhalb der Spezifikation des Herstellers;

d) Beachtung der Anwendungshinweise des Herstellers, zum Beispiel Katalogangaben, Installationsanweisungen und Anwendung bewährter Konstruktionspraxis (siehe auch ISO 13849-2, D.1);

e) Verwendung von Teilsystemen, die vergleichbare Betriebseigenschaften haben (siehe auch ISO 13849-2, D.1);

f) das SRECS muss gemäß IEC 60204-1 geschützt sein;

g) Verhinderung des Verlusts funktionaler Erdungsverbindung(en) in Übereinstimmung mit IEC 60204-1;

h) undokumentierte Anwendungen von Bauteilen dürfen nicht verwendet werden (z. B. „reservierte“ Register von programmierbaren Einrichtungen) und

i) Berücksichtigung von vorhersehbarer Fehlanwendung, Änderung der Umgebungsbedingungen und Modifikation(en).

6.4.1.2 Zusätzlich müssen mindestens eines der folgenden Verfahren und/oder Maßnahmen unter Berücksichtigung der Komplexität des SRECS und des (der) SIL(s) für diejenigen Funktionen, die durch das SRECS implementiert werden müssen, angewendet werden:

a) Überprüfung des Entwurfs der SRECS-Hardware (z. B. durch Inspektion oder Walkthrough): Feststellung aller Unstimmigkeiten zwischen der Spezifikation und der Implementierung durch Überprüfungen und/oder Analysen;

ANMERKUNG 1 Um Unstimmigkeiten zwischen der Spezifikation und der Implementierung aufzudecken, werden alle zweifelhaften Punkte oder mögliche Schwachstellen in Bezug auf die Realisierung, die Implementierung und die Verwendung des Produkts dokumentiert, so dass sie gelöst werden können. Es sollte berücksichtigt werden, dass der Autor beim Inspektionsverfahren passiv und der Inspizierende aktiv ist, wogegen bei einem Walkthrough der Autor aktiv und der Inspizierende passiv ist.

b) Hilfswerkzeuge wie rechnerunterstützte Entwurfspakete zur Durchführung von Simulation oder Analyse und/oder die Verwendung von rechnerunterstützten Entwurfswerkzeugen zur systematischen Durchführung der Entwurfsverfahren unter Verwendung von bereits entworfenen Elementen, die bereits vorhanden und getestet sind;

ANMERKUNG 2 Die Integrität dieser Werkzeuge kann durch spezielle Prüfungen oder eine umfassende Historie zufrieden stellender Verwendung oder durch eine unabhängige Verifikation ihrer Ergebnisse für das jeweilige entworfene SRECS gezeigt werden. Siehe 6.11.3.4.

c) Simulation: Ausführung einer vollständigen systematischen Assimilation eines SRECS-Entwurfs im Hinblick sowohl auf funktionale Leistungsfähigkeit als auch auf korrekte Dimensionierung und Wechselwirkung zwischen seinen Teilsystemen.

BEISPIEL Die Schaltungsfunktion des SRECS kann mit einem Rechner durch ein softwarebasierendes Verhaltensmodell simuliert werden (siehe 6.11.3.4), wobei einzelne Teilsysteme oder Teilsystem-Elemente ihr eigenes simuliertes Verhalten besitzen und die Reaktion des Schaltkreises, in dem sie verbunden sind, untersucht wird, in dem die Grenzwerte jedes Teilsystems oder Teilsystem-Elements betrachtet werden.

6.4.2 Anforderungen zur Beherrschung systematischer Fehler

Die folgenden Maßnahmen müssen angewendet werden:

a) Nutzung von Energieabschaltung: das SRECS muss so entworfen sein, dass bei einem Verlust der elektrischen Versorgung ein sicherer Zustand der Maschine erreicht oder beibehalten wird;

b) Maßnahmen zur Beherrschung der Auswirkungen vorübergehender Teilsystemausfälle: das SRECS muss so entworfen sein, dass zum Beispiel:

- Spannungsänderungen (z. B. Unterbrechungen, Einbrüche) an einem einzelnen Teilsystem oder Teil eines Teilsystems nicht zu einer Gefährdung führen (z. B. darf eine Spannungsunterbrechung, die sich auf einen Motorstromkreis auswirkt, nicht zu einem unerwarteten Anlauf führen, wenn die Versorgung wiederhergestellt wird) und

  ANMERKUNG 1 Siehe auch relevante Anforderungen von IEC 60204-1, insbesondere:

  Überspannung oder Unterspannung sollte früh genug erkannt werden, so dass alle Ausgänge durch die Power-down-Routine in einen sicheren Zustand geschaltet werden können oder eine Umschaltung auf eine zweite Energieversorgung erfolgen kann und/oder

  wo erforderlich, sollte Überspannung oder Unterspannung früh genug erkannt werden, um den internen Zustand in einem Festspeicher sichern zu können, so dass alle Ausgänge durch die Power-down-Routine in einen sicheren Zustand gesetzt werden können oder alle Ausgänge durch die Power-down-Routine in einen sicheren Zustand geschaltet werden können oder eine Umschaltung auf eine zweite Energieversorgung erfolgen kann.

- die Auswirkungen elektromagnetischer Beeinflussung durch die physikalische Umgebung oder durch ein (mehrere) Teilsystem(e) nicht zu einer Gefährdung führen;

c) Maßnahmen zur Beherrschung der Auswirkungen von Fehlern und anderer Effekte, die von irgendeinem Datenkommunikationsprozess herrühren, einschließlich Übertragungsfehler, Wiederholungen, Verlust, Einfügung, falsche Abfolge, Verfälschung, Verzögerung und Masquerade;

ANMERKUNG 2 Weitere Informationen sind in IEC 60870-5-1, EN 50159-1, EN 50159-2 und IEC 61508-2 zu finden.

ANMERKUNG 3 Der Begriff „Masquerade“ besagt, dass die wahren Inhalte einer Nachricht nicht korrekt identifiziert werden. Zum Beispiel wird eine Nachricht von einem nichtsicheren Teilnehmer fälschlicherweise als eine Nachricht von einem sicheren Teilnehmer identifiziert.

d) wenn an einer Schnittstelle ein gefahrbringender Fehler auftritt, muss die Fehlerreaktionsfunktion ausgeführt werden, bevor die Gefährdung durch diesen Fehler auftreten kann. Wenn ein Fehler auftritt, der die Hardware-Fehlertoleranz zu null reduziert, muss diese Fehlerreaktion stattfinden, bevor die geschätzte MTTR (siehe 6.7.4.4.2g)) überschritten ist.

Die Anforderungen aus Punkt d) gelten für Schnittstellen, die Eingänge und Ausgänge von Teilsystemen sind und alle anderen Einheiten von Teilsystemen, die während der Integration eine Verkabelung einschließen oder erfordern (zum Beispiel Ausgangsschaltelemente eines Lichtvorhangs oder der Ausgang eines Positionssensors einer trennenden Schutzeinrichtung).

ANMERKUNG 4 Dies erfordert nicht, dass ein Teilsystem oder Teilsystem-Element die Erkennung eines Fehlers an seinem Ausgang (seinen Ausgängen) selbst durchführen muss. Die Fehlerreaktionsfunktion kann auch von irgendeinem nachfolgenden Teilsystem nach der Ausführung eines Diagnosetests eingeleitet werden.

6.4.3 Elektromagnetische (EM) Störfestigkeit

Zusätzlich zu den Anforderungen nach IEC 61000-6-2 und den in Anhang E angegebenen EM-Phänomenen muss das folgende Bewertungskriterium für funktionale Sicherheit durch ein SRECS erfüllt werden:

– es dürfen keine unsicheren Bedingungen oder Gefährdungen entstehen und

– kein Verlust der SRCF(s) oder

– die vom SRECS ausgeführte(n) SRCF(s) dürfen vorübergehend oder dauerhaft gestört sein, vorausgesetzt, dass ein sicherer Zustand der Maschine aufrechterhalten oder erreicht wird, bevor eine Gefährdung auftreten kann. Wo die EM-Phänomene zu einer Zerstörung von Bauteilen führen können, muss sichergestellt werden (z. B. durch Analyse), dass die funktionale Sicherheit nicht betroffen ist. Dies gilt auch für niedrige Werte der EM-Phänomene, die zu einer teilweisen Zerstörung führen können.

ANMERKUNG Das Verhalten des SRECS als Reaktion auf die EM-Phänomene sollte für alle Werte bis hin zu den in Anhang E angegebenen berücksichtigt werden.

6.5 Auswahl eines sicherheitsbezogenen elektrischen Steuerungssystems

Wenn ein Lieferant ein SRECS für eine spezifische Funktion vorsieht, die in der Spezifikation der Sicherheitsanforderungen angegeben ist, kann ein bereits entwickeltes SRECS anstatt einer eigenen Entwicklung gewählt werden, vorausgesetzt, es erfüllt die Anforderungen der Spezifikation der Sicherheitsanforderungen und 6.3, 6.4 und 6.6.1.

ANMERKUNG Die Auswahl eines bereits entwickelten SRECS ist eine Alternative zu Entwurf und Entwicklung eines spezifischen SRECS in Übereinstimmung mit 6.6.

6.6 Entwurf und Entwicklung eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)

6.6.1 Allgemeine Anforderungen

6.6.1.1 Das SRECS muss in Übereinstimmung mit der Spezifikation der SRECS-Sicherheitsanforderungen (siehe 5.2) entworfen und entwickelt werden.

6.6.1.2 Ein klar strukturierter Entwurfsprozess muss befolgt und dokumentiert werden (siehe 6.6.2).

6.6.1.3 Wo die Verwendung von Diagnose notwendig ist, um die erforderliche Sicherheitsintegrität zu erreichen, muss, wenn ein Fehler erkannt wird, das SRECS die spezifizierte Fehlerreaktionsfunktion (siehe 5.2 und 6.3) ausführen.

6.6.1.4 Wo ein SRECS oder Teile eines SRECS (d. h. sein(e) Teilsystem(e)) sowohl SRCFs als auch andere Funktionen enthalten sollen, muss seine bzw. müssen ihre gesamte Hardware und Software als sicherheitsbezogen behandelt werden, es sei denn, es kann gezeigt werden, dass die Implementierung der SRCFs und der anderen Funktionen ausreichend unabhängig voneinander ist (d. h., dass der normale Betrieb oder der Ausfall irgendwelcher anderer Funktionen nicht die SRCFs beeinflusst).

ANMERKUNG Eine ausreichende Unabhängigkeit der Implementierung kann angenommen werden, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen den nichtsicherheitsbezogenen und sicherheitsbezogenen Teilen gleichwertig zu der des Sicherheits-Integritätslevels des SRECS ist.

6.6.1.5 Für ein SRECS oder seine Teilsysteme, das (die) sicherheitsbezogene Steuerungsfunktionen verschiedener Sicherheits-Integritätslevels ausführt (ausführen), muss die Hardware und Software als zum höchsten Sicherheits-Integritätslevel zugehörig betrachtet werden, es sei denn, es kann gezeigt werden, dass die Implementierung von sicherheitsbezogenen Steuerungsfunktionen verschiedener Sicherheits-Integritätslevel ausreichend unabhängig voneinander ist.

ANMERKUNG Eine ausreichende Unabhängigkeit der Implementierung kann angenommen werden, wenn gezeigt wird, dass die Wahrscheinlichkeit eines abhängigen Ausfalls zwischen den Teilen, die SRCFs unterschiedlicher Sicherheits-Integritätslevels ausführen, gleichwertig zu der des vom SRECS erreichten Sicherheits-Integritätslevels ist.

6.6.1.6 Verbindungen (z. B. Verdrahtung, Verkabelung), außer digitaler Datenkommunikation, müssen als Teil eines der Teilsysteme, mit dem sie verbunden sind, betrachtet werden (siehe auch 6.4.2 d)).

6.6.1.7 Wenn digitale Datenkommunikation als Teil einer SRECS-Implementierung verwendet wird, muss sie die relevanten Anforderungen der IEC 61508-2 in Übereinstimmung mit dem (den) SIL-Zielwert(en) der SRCF(s) erfüllen.

6.6.1.8 Die Benutzerinformationen des SRECS müssen diejenigen Verfahren und Maßnahmen festlegen, die während des konzipierten Lebens des SRECS notwendig sind, um den Sicherheits-Integritätslevel aufrechtzuerhalten.

6.6.2 Entwurfs- und Entwicklungsprozess

Der Entwurf und die Entwicklung müssen einem eindeutig definierten Prozess folgen, der alle Aspekte berücksichtigt, die von dem in Bild 2 gezeigten Prozess abgedeckt werden.

ANMERKUNG Der Ansatz dieser Norm ist es, einen strukturierten Entwurfsprozess für das SRECS anzuwenden, ausgehend von den Anforderungen, die in der Spezifikation der Sicherheitsanforderungen festgelegt sind. Bild 3 zeigt den Ablauf des Entwurfsprozesses und die zu den verschiedenen Stufen zugehörige Terminologie.

6.6.2.1 Entwurf der Systemarchitektur

6.6.2.1.1 Jede in der Spezifikation der SRECS-Sicherheitsanforderungen spezifizierte SRCF muss, wie zum Beispiel in Bild 3 gezeigt, in eine Struktur von Funktionsblöcken zerlegt werden. Diese Struktur muss dokumentiert werden einschließlich:

– der Beschreibung der Struktur;

– den Sicherheitsanforderungen (Funktionalität, Integrität) für jeden Funktionsblock;

– Definition der Eingaben und Ausgaben jedes Funktionsblocks.

ANMERKUNG 1 Der Aufteilungsprozess sollte zu einer Struktur von Funktionsblöcken führen, die die funktionalen Anforderungen und die Anforderungen zur Integrität der SRCF vollständig beschreibt. Dieser Prozess sollte bis auf die Stufe herab angewendet werden, die es erlaubt, die für jeden Funktionsblock festgelegten funktionalen Anforderungen und die Anforderungen zur Integrität Teilsystemen zuzuordnen, wo die Zuordnung der vollständigen funktionalen Anforderungen eines Funktionsblocks zu einem Teilsystem möglich ist. Es ist jedoch möglich, mehr als einen Funktionsblock einem einzelnen Teilsystem zuzuordnen, aber es ist nicht möglich, einen Funktionsblock mehreren Teilsystemen zuzuordnen, wo es beabsichtigt ist, dass diese Teilsysteme getrennte funktionale Anforderungen und Anforderungen zur Integrität haben. Wo die Absicht besteht, die funktionalen Anforderungen eines Funktionsblocks zu redundanten Teilsystem-Elementen zuzuordnen, ist 6.7.4 in Bezug zu nehmen.

ANMERKUNG 2 Die Eingaben und Ausgaben jedes Funktionsblocks stellen die übermittelten Informationen dar, zum Beispiel Geschwindigkeit, Position, Betriebsart usw.

ANMERKUNG 3 Die Funktionsblöcke sind eine Darstellung von Funktionen der SRCF (siehe 3.2.16) und umfassen nicht SRECS-Diagnosefunktionen (siehe 3.2.17). Im Rahmen dieser Norm werden die Diagnosefunktionen als gesonderte Funktionen betrachtet, die eine andere Struktur als die SRCF haben können (siehe 6.8).

6.6.2.1.2 In Übereinstimmung mit der Struktur der Funktionsblöcke muss ein erstes Konzept für eine Architektur des SRECS geschaffen werden.

ANMERKUNG Es sollte eine fortlaufende Zusammenarbeit zwischen dem Entwickler der sicherheitsbezogenen Steuerungsarchitektur, der Organisation, die für die Konfiguration der Geräte zuständig ist, und dem Softwareentwickler geben. Wenn die Software-Sicherheitsanforderungen und die mögliche Softwarearchitektur präziser werden, kann ein Einfluss auf die SRECS-Hardwarearchitektur erfolgen. Aus diesem Grunde kann eine enge Zusammenarbeit zwischen dem Entwickler der SRECS-Architektur, dem (den) Teilsystemlieferanten, dem Softwareentwickler und, falls notwendig, dem Maschinenkonstrukteur oder dem Anwender helfen, die Möglichkeit für einen systematischen Ausfall (Ausfälle) zu verringern.

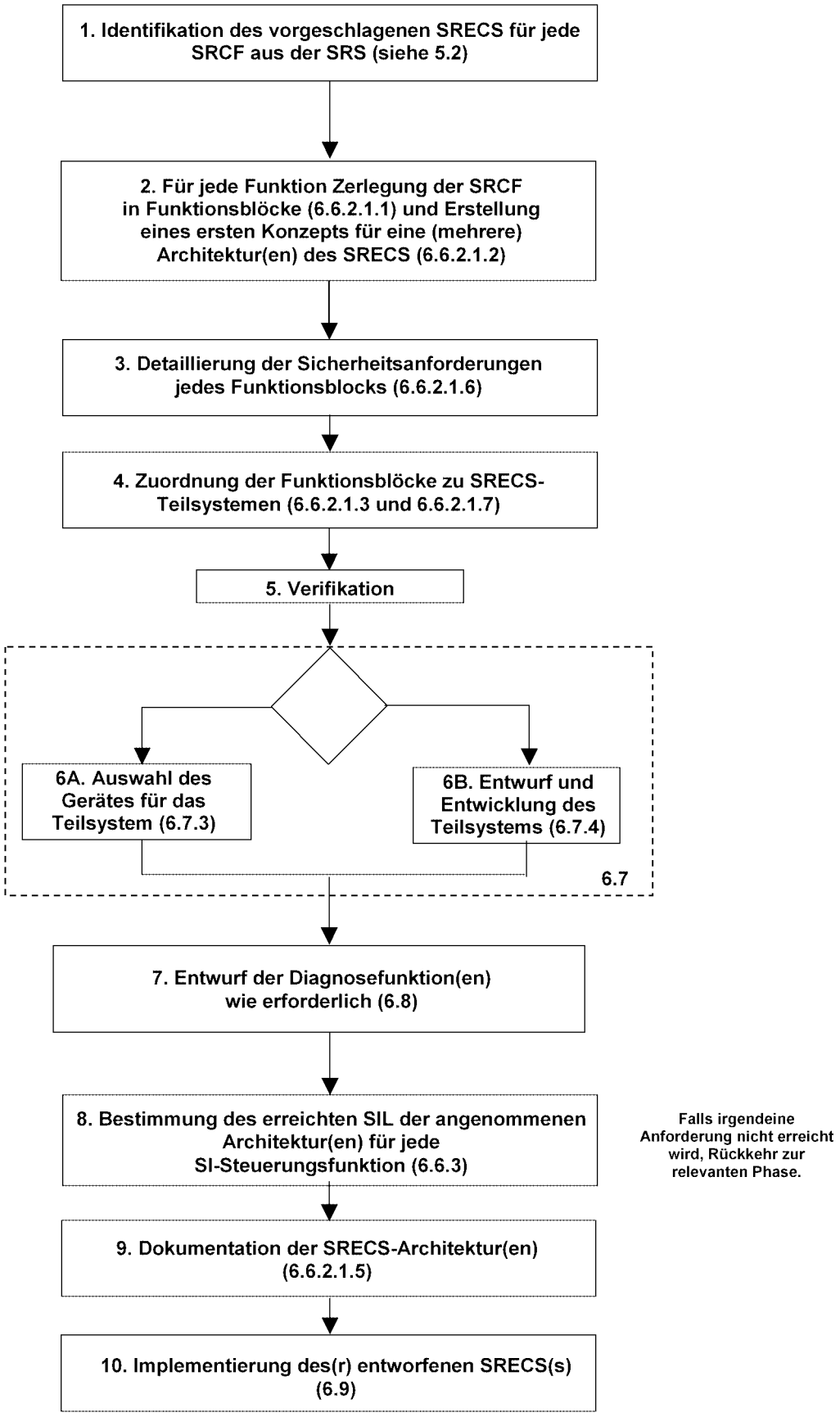


Bild 2 – Ablauf des SRECS-Entwurfs- und Entwicklungsprozesses

6.6.2.1.3 Jeder Funktionsblock muss innerhalb der Architektur des SRECS einem Teilsystem zugeordnet werden. Einem Teilsystem kann mehr als ein Funktionsblock zugeordnet werden.

6.6.2.1.4 Jedes Teilsystem und die ihm zugeordneten Funktionsblöcke müssen klar identifiziert werden.

6.6.2.1.5 Die Architektur muss unter Beschreibung ihrer Teilsysteme und deren Beziehung untereinander dokumentiert werden.

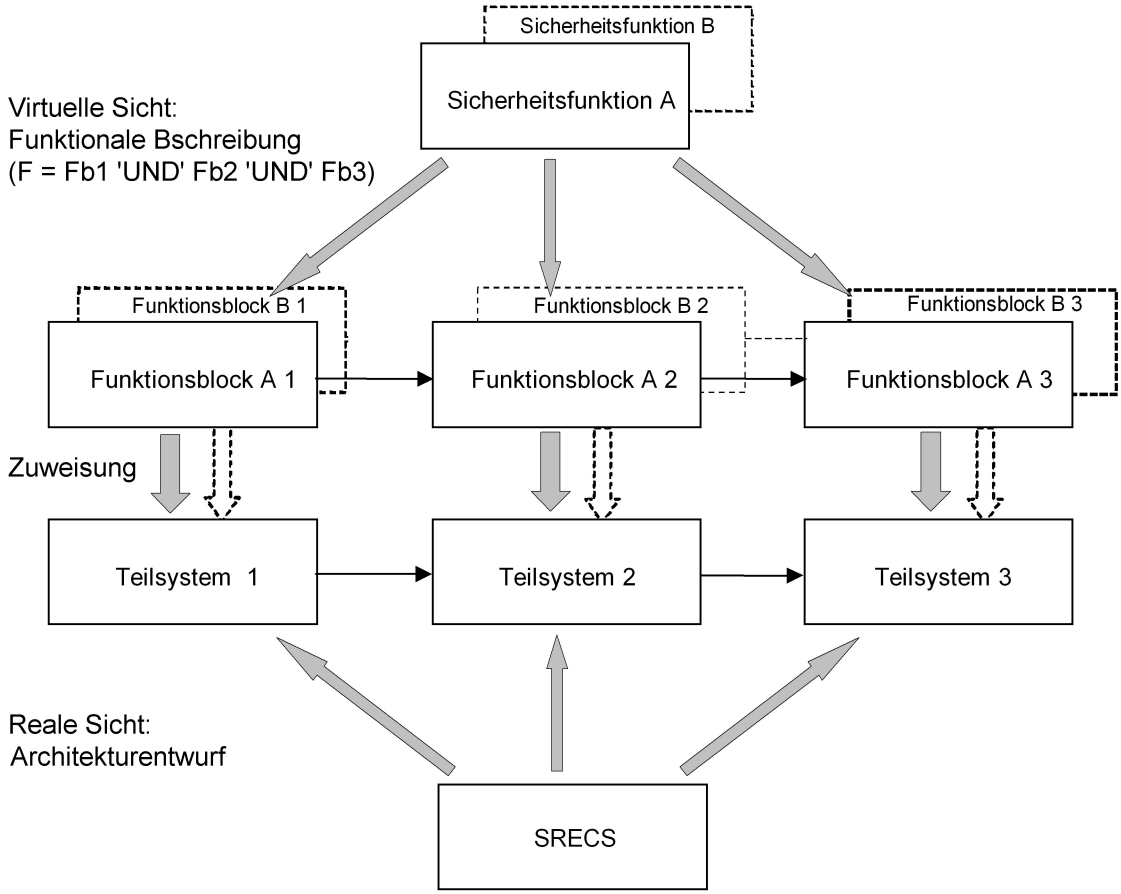


Bild 3 – Zuordnung von Sicherheitsanforderungen der Funktionsblöcke zu Teilsystemen (siehe 6.6.2.1.1)

6.6.2.1.6 Die Sicherheitsanforderungen für jeden Funktionsblock müssen wie in der Spezifikation der Sicherheitsanforderungen der entsprechenden SRCF spezifiziert sein, in Form von:

– funktionalen Anforderungen (z. B. Eingangsinformation, interne Verarbeitung (Logik) und Ausgang des Funktionsblocks);

– Anforderungen zur Sicherheitsintegrität.

6.6.2.1.7 Die Sicherheitsanforderungen für ein Teilsystem müssen diejenigen des (der) ihm zugeordneten Funktionsblocks (Funktionsblöcke) sein. Wenn einem Teilsystem mehr als ein Funktionsblock zugeordnet ist, ist die höchste Anforderung in Bezug auf die Integrität zutreffend (siehe 6.6.3). Diese Anforderungen müssen als die Spezifikation der Sicherheitsanforderungen des Teilsystems dokumentiert werden.

6.6.3 Anforderungen für die Abschätzung der durch ein SRECS erreichten Sicherheitsintegrität

6.6.3.1 Allgemeines

Der SIL, der durch das SRECS erreicht werden kann, muss für jede SRCF, die durch das SRECS ausgeführt werden soll, getrennt betrachtet werden.

Der SIL, der durch das SRECS erreicht werden kann, muss aus der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls, den strukturellen Einschränkungen und der systematischen Sicherheitsintegrität der Teilsysteme, aus denen das SRECS besteht, festgelegt werden. Der erreichte SIL ist geringer als oder gleich dem geringsten Wert der SILCLs irgendeines der Teilsysteme für systematische Sicherheitsintegrität und strukturelle Einschränkungen.

6.6.3.2 Sicherheitsintegrität der Hardware

6.6.3.2.1 Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls jeder SRCF in Folge gefahrbringender zufälliger Hardwareausfälle muss gleich oder kleiner als der in der Spezifikation der Sicherheitsanforderungen festgelegte Ausfallgrenzwert sein.

ANMERKUNG Die mit den SILs verbundenen Grenzwerte sind in Tabelle 3 angegeben.

6.6.3.2.2 Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls jeder SRCF in Folge gefahrbringender zufälliger Hardwareausfälle muss unter Berücksichtigung von Folgendem abgeschätzt werden:

a) der Architektur des SRECS in Bezug zu jeder betrachteten SRCF;

   ANMERKUNG Dies schließt die Entscheidung ein, welche Ausfallarten der Teilsysteme in einer seriellen Konfiguration vorhanden sind (d. h. jeder Ausfall führt dazu, dass die Ausführung der relevanten SRCF ausfällt) und welche in einer parallelen (redundanten) Konfiguration vorhanden sind (d. h. es sind gemeinsam auftretende Ausfälle notwendig, damit die relevante SRCF ausfällt).

b) der geschätzten Ausfallrate jedes Teilsystems seinen (seine) zugeordneten Funktionsblock (Funktionsblöcke) in allen Modi auszuführen, die zu einem gefahrbringenden Ausfall des SRECS führen können.

6.6.3.2.3 Die Abschätzung der Wahrscheinlichkeit eines gefahrbringenden Ausfalls muss auf der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls jedes relevanten Teilsystems basieren, wie aus den in 6.7.2.2 erforderlichen Informationen, einschließlich wo zutreffend 6.7.2.2 (k) für digitale Datenkommunikationsprozesse zwischen Teilsystemen, abgeleitet. Die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls des SRECS ist die Summe der Wahrscheinlichkeiten gefahrbringender zufälliger Hardwareausfälle aller Teilsysteme, die an der Ausführung der SRCF beteiligt sind und muss, wo zutreffend, die Wahrscheinlichkeit gefahrbringender Übertragungsfehler für digitale Datenkommunikationsprozesse einschließen:

$$PFH_{\mathrm{D}} = PFH_{\mathrm{D1}} + \ldots + PFH_{\mathrm{Dn}} + P_{\mathrm{TE}}$$

ANMERKUNG 1 Dieser Ansatz basiert auf der Definition eines Funktionsblocks, die aussagt, dass ein Ausfall irgendeines Funktionsblocks zu einem Ausfall der SRCF führt (siehe 3.2.16).

ANMERKUNG 2 Andere Verbindungen als digitale Datenkommunikation werden als ein Teil der Teilsysteme betrachtet.

6.6.3.3 Strukturelle Einschränkungen

Der SIL, der durch das SRECS auf Grund der strukturellen Einschränkungen erreicht wird, ist geringer als oder gleich der niedrigsten SILCL irgendeines Teilsystems (siehe 6.7.6), das an der Ausführung der SRCF beteiligt ist.

ANMERKUNG Zum Beispiel besteht ein SRECS aus zwei seriell verbundenen Teilsystemen (Teilsystem 1 und Teilsystem 2), wobei der SFF und die Fehlertoleranz jedes Teilsystems so wie in Tabelle 4 gezeigt angenommen werden. Die abgeschätzte PFH_{D} für das SRECS ist 8×10^{-8}, was SIL 3 entspricht. Jedoch beschränkt gemäß Tabelle 5 die strukturelle Einschränkung von Teilsystem 2 den SIL, der von dem SRECS erreicht werden kann, auf SIL 2.

Tabelle 4 – Merkmale der in diesem Beispiel verwendeten Teilsysteme 1 und 2 (siehe vorstehende Anmerkung)

Teilsystem	Hardware-Fehlertoleranz	SFF	SIL-Anspruchsgrenze gemäß den strukturellen Einschränkungen (siehe Tabelle 5)
1	1	95 %	SIL 3
2	1	80 %	SIL 2

6.6.3.4 Systematische Sicherheitsintegrität

Der SIL, der durch das SRECS erreicht wird, ist geringer als oder gleich der niedrigsten SILCL irgendeines Teilsystems, das an der Ausführung der SRCF beteiligt ist.

ANMERKUNG Die in 6.7.9 beschriebenen Maßnahmen ergeben eine SILCL bis zu SIL 3 für die systematische Sicherheitsintegrität eines nach 6.7.4 realisierten Teilsystems.

6.7 Realisierung von Teilsystemen

6.7.1 Ziel

Das Ziel ist es, ein Teilsystem zu realisieren, das alle Sicherheitsanforderungen der zugeordneten Funktionsblöcke (siehe Bild 3) erfüllt. Zwei Lösungsansätze sind vorgesehen:

– Auswahl eines Geräts, das den Anforderungen an das Teilsystem genügt, d. h. es muss die Spezifikation der Sicherheitsanforderungen von jedem der ihm zugeordneten Funktionsblöcke und die Anforderungen dieser Norm erfüllen oder

– Entwurf und Entwicklung eines Teilsystems durch Kombination von Funktionsblock-Elementen und Spezifikation, wie sie angeordnet werden und wie sie zusammenwirken.

6.7.2 Allgemeine Anforderungen für die Realisierung eines Teilsystems

6.7.2.1 Das Teilsystem muss entweder durch Auswahl (siehe 6.7.3) oder Entwurf (siehe 6.7.4) in Übereinstimmung mit seiner Spezifikation der Sicherheitsanforderungen (siehe 6.6.2.1.7), unter Berücksichtigung aller Anforderungen aus 6.2 realisiert werden. Ein (mehrere) Teilsystem(e), das (die) komplexe Bauteile enthält (enthalten), muss (müssen) entsprechend dem erforderlichen SIL mit IEC 61508-2 und IEC 61508-3 übereinstimmen.

AUSNAHME: Wo der Entwurf eines Teilsystems ein komplexes Bauteil als ein Teilsystem-Element enthält, ist 6.7.4.2.3 anwendbar.

6.7.2.2 Die folgenden Informationen müssen für jedes Teilsystem vorhanden sein:

a) eine funktionale Spezifikation derjenigen Funktionen und Schnittstellen des Teilsystems, die von den SRCFs verwendet werden können;

b) die abgeschätzten Ausfallraten (in Folge von zufälligen Hardwareausfällen) angegeben in allen Modi, die zu einem gefahrbringenden Ausfall des SRECS führen können;

ANMERKUNG 1 Für elektromechanische Teilsysteme sollte die Ausfallwahrscheinlichkeit unter Berücksichtigung der vom Hersteller angegebenen Anzahl von Betriebszyklen und dem Nutzungsfaktor abgeschätzt werden (siehe 5.2.3). Diese Informationen sollten auf dem B10-Wert basieren (d. h. dem erwarteten Zeitpunkt, an dem 10 % des Bestandes ausgefallen sein werden). Siehe auch IEC 61810-2[1)]

[1)] noch zu veröffentlichen

c) Einschränkungen für das Teilsystem in Bezug auf:

- die Umgebung und Betriebsbedingungen, die beachtet werden sollten, um die Gültigkeit der geschätzten Ausfallraten auf Grund zufälliger Hardwareausfälle zu erhalten und
- die Gebrauchsdauer des Teilsystems, die nicht überschritten werden sollte, um die Gültigkeit der geschätzten Ausfallraten auf Grund zufälliger Hardwareausfälle zu erhalten;

d) alle Anforderungen zu Test und/oder Instandhaltung;

e) der Diagnosedeckungsgrad und das Diagnose-Testintervall (falls erforderlich, siehe Anmerkung 2);

ANMERKUNG 2 Der obige Punkt e) bezieht sich auf externe Diagnosefunktionen eines Teilsystems. Diese Informationen sind nur erforderlich, wenn in dem Zuverlässigkeitsmodell des SRECS aus der Durchführung von Diagnosefunktionen in dem Teilsystem Kredit gezogen wird.

f) alle zusätzlichen Informationen (z. B. Reparaturzeiten), die notwendig sind, um die Ableitung einer mittleren Zeit bis zur Wiederherstellung (MTTR) zu ermöglichen, die auf die Erkennung eines Fehlers durch die Diagnose folgt;

ANMERKUNG 3 Die Punkte b) bis f) sind notwendig, um die Abschätzung der Wahrscheinlichkeit eines Ausfalls der SRCF pro Stunde zu erlauben.

g) die SILCL in Bezug auf strukturelle Einschränkungen (siehe 6.7.6) oder:

- alle Informationen, die notwendig sind, um die Ableitung des Anteils sicherer Ausfälle (SFF) des Teilsystems, wie es im SRECS Verwendung findet, zu ermöglichen und

  ANMERKUNG 4 Erforderliche Informationen sind die möglichen Ausfallarten des Teilsystems. Basierend auf den Ausfallarten des Teilsystems lässt sich entscheiden, ob der Ausfall des Teilsystems zu einem sicheren oder einem gefahrbringenden Ausfall des SRECS führt.

  ANMERKUNG 5 Siehe 6.7.7 zu Einzelheiten der Abschätzung des SFF.

- die Hardware-Fehlertoleranz des Teilsystems;

h) alle Grenzen für die Anwendung des Teilsystems, die zur Vermeidung von systematischen Ausfällen beachtet werden sollten;

i) den höchsten Sicherheits-Integritätslevel, der für eine SRCF in Anspruch genommen werden kann, die das Teilsystem verwendet, auf der Basis von:

- Maßnahmen und Techniken, die verwendet werden, um zu verhindern, dass während des Entwurfs und der Implementierung der Hardware und der Software des Teilsystems systematische Fehler verursacht werden;
- den Entwurfsmerkmalen, die das Teilsystem gegenüber systematischen Fehlern tolerant machen;

ANMERKUNG 6 Die Punkte h) und i) sind notwendig, um den höchsten Sicherheits-Integritätslevel, der für eine SRCF in Anspruch genommen werden kann, gemäß den strukturellen Einschränkungen festzulegen. Weiterhin können diese Punkte dazu verwendet werden, eine Verbindung (siehe Tabellen 4 und 5) zu den Kategorieanforderungen von ISO 13849-1 im Hinblick sowohl auf Fehlererkennung als auch auf Hardware-Fehlertoleranz bereitzustellen.

j) alle Informationen, die erforderlich sind, um die Hardware- und Softwarekonfiguration des Teilsystems zu identifizieren, um das Konfigurationsmanagement eines SRECS in Übereinstimmung mit 6.11.3.2 zu ermöglichen;

k) die Wahrscheinlichkeit gefahrbringender Übertragungsfehler für digitale Datenkommunikationsprozesse, soweit zutreffend.

6.7.3 Anforderungen zur Auswahl vorhandener (bereits entwickelter) Teilsysteme

6.7.3.1 Wo ein Lieferant ein Teilsystem für eine spezifische SRCF, die in der Spezifikation der Sicherheitsanforderungen aufgeführt ist, vorsieht, kann ein solches bereits entwickeltes Teilsystem anstatt eines kundenspezifischen Entwurfs ausgewählt werden, vorausgesetzt, es erfüllt die Spezifikation der Sicherheitsanforderungen für das Teilsystem 6.4.3 und 6.7.3.2 oder 6.7.3.3.

6.7.3.2 Teilsysteme, die komplexe Bauteile enthalten, müssen entsprechend dem erforderlichen SIL mit IEC 61508-2 und IEC 61508-3 übereinstimmen.

AUSNAHME: Wo der Entwurf eines Teilsystems ein komplexes Bauteil als ein Teilsystem-Element enthält, ist 6.7.4.2.3 anwendbar.

6.7.3.3 Teilsysteme, die aus einfachen Bauteilen bestehen, müssen nur mit 6.7.4.4.1, 6.7.6.2, 6.7.6.3, 6.7.7, 6.7.8 und 6.8 dieser Norm übereinstimmen.

6.7.4 Entwurf und Entwicklung von Teilsystemen

6.7.4.1 Ziele

6.7.4.1.1 Das erste Ziel ist es, ein Teilsystem zu entwerfen, das die Sicherheitsanforderungen des (der) zugeordneten Funktionsblocks (Funktionsblöcke) erfüllt.

6.7.4.1.2 Das zweite Ziel ist es, eine Architektur in Form von Teilsystem-Elementen zu erstellen, die in Kombination zusammenwirken, um die funktionalen Anforderungen und die Anforderungen zur Sicherheitsintegrität aller dem Teilsystem zugeordneten Funktionsblöcke zu erfüllen.

6.7.4.2 Allgemeine Anforderungen

6.7.4.2.1 Das Teilsystem muss in Übereinstimmung mit seiner Spezifikation der Sicherheitsanforderungen entworfen werden.

6.7.4.2.2 Das Teilsystem muss so gestaltet sein, dass es die gesamten Anforderungen a) bis c) wie folgt erfüllt:

a) die Anforderungen zur Sicherheitsintegrität der Hardware, bestehend aus:
   - den strukturellen Einschränkungen zur Sicherheitsintegrität der Hardware (siehe 6.7.6) und
   - den Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle (siehe 6.7.8);

b) die Anforderungen zur systematischen Sicherheitsintegrität, bestehend aus:
   - den Anforderungen zur Vermeidung von Ausfällen (siehe 6.7.9.1) und den Anforderungen zur Beherrschung systematischer Fehler (siehe 6.7.9.2) oder
   - dem Nachweis, dass die Einrichtungen „betriebsbewährt“ sind; in diesem Fall muss das Teilsystem die relevanten Anforderungen der IEC 61508-2 erfüllen (siehe IEC 61508-2, 7.4.7.5 bis 7.4.7.12);

c) die Anforderungen an das Verhalten des Teilsystems bei Erkennung eines Fehlers (Fehlerreaktion) (siehe 6.3).

6.7.4.2.3 Wenn der Entwurf eines Teilsystems ein komplexes Bauteil (als ein Teilsystem-Element) enthält, das alle relevanten Anforderungen aus IEC 61508-2 und IEC 61508-3 in Bezug auf die SILCL erfüllt, kann dieses Teilsystem als einfaches Bauteil im Zusammenhang mit dem Entwurf eines Teilsystems betrachtet werden, da seine relevanten Ausfallarten, sein Verhalten bei Erkennung eines Fehlers, seine Ausfallrate und andere sicherheitsbezogene Informationen bekannt sind. Solche Bauteile dürfen nur in Übereinstimmung mit ihrer Spezifikation und den vom Lieferanten zur Verfügung gestellten relevanten Benutzerinformationen verwendet werden.

6.7.4.3 Entwurfs- und Entwicklungsprozess des Teilsystems

Der Entwurf und die Entwicklung des Teilsystems müssen einem eindeutig definierten Prozess folgen, der alle Aspekte berücksichtigt, die von dem in Bild 4 gezeigten Prozess abgedeckt werden.

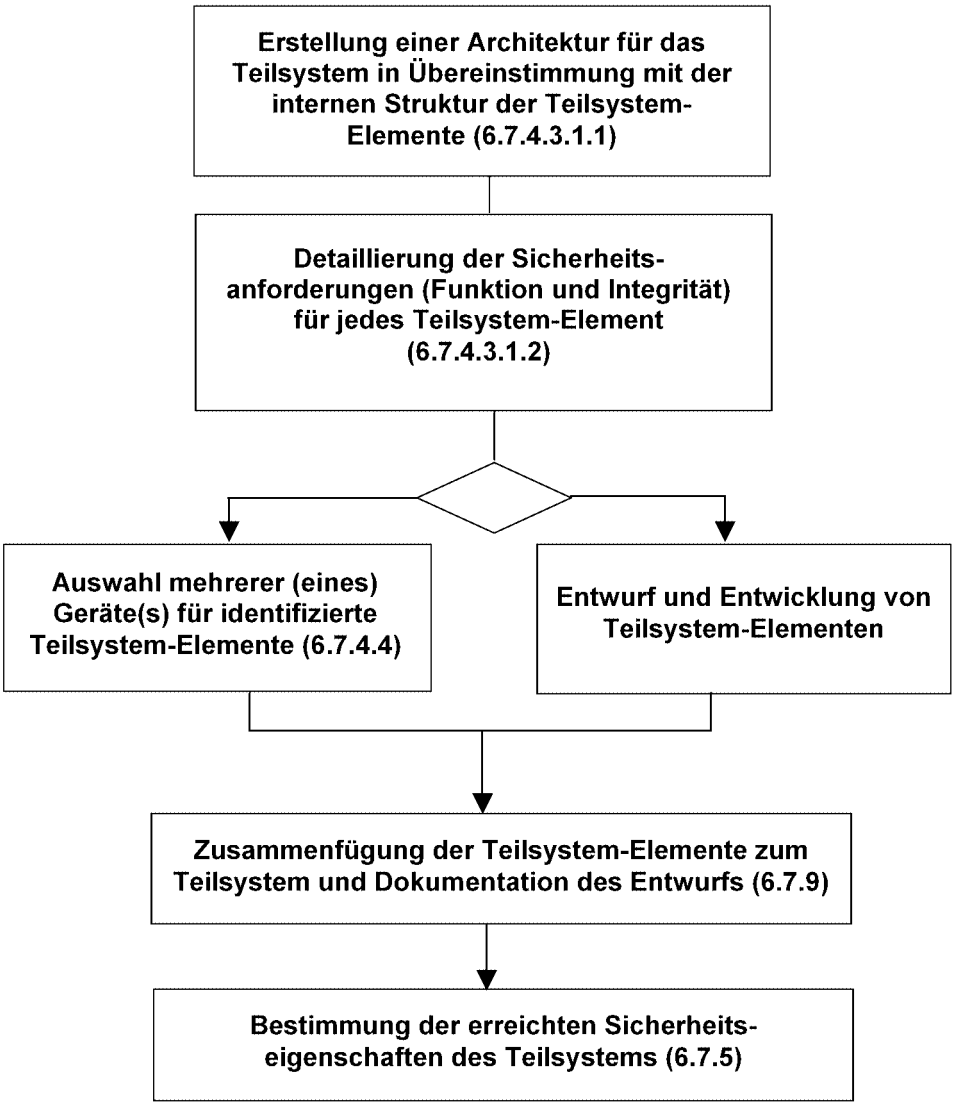


Bild 4 – Ablauf für Entwurf und Entwicklung eines Teilsystems (siehe Kästchen 6B von Bild 2)

6.7.4.3.1 Architekturentwurf des Teilsystems

6.7.4.3.1.1 Während des Entwurfs der Architektur des Teilsystems sollte der Aufteilungsprozess zu einer Struktur von Funktionsblock-Elementen führen, die die funktionalen Anforderungen des Funktionsblocks vollständig darstellt. Dieser Prozess sollte bis auf die Ebene angewendet werden, die es erlaubt, die für jedes Funktionsblock-Element festgelegten funktionalen Anforderungen Teilsystem-Elementen zuzuordnen (siehe Beispiel in Bild 5).

ANMERKUNG Der Ablauf des Entwurfsprozesses ist in Bild 4 gezeigt.

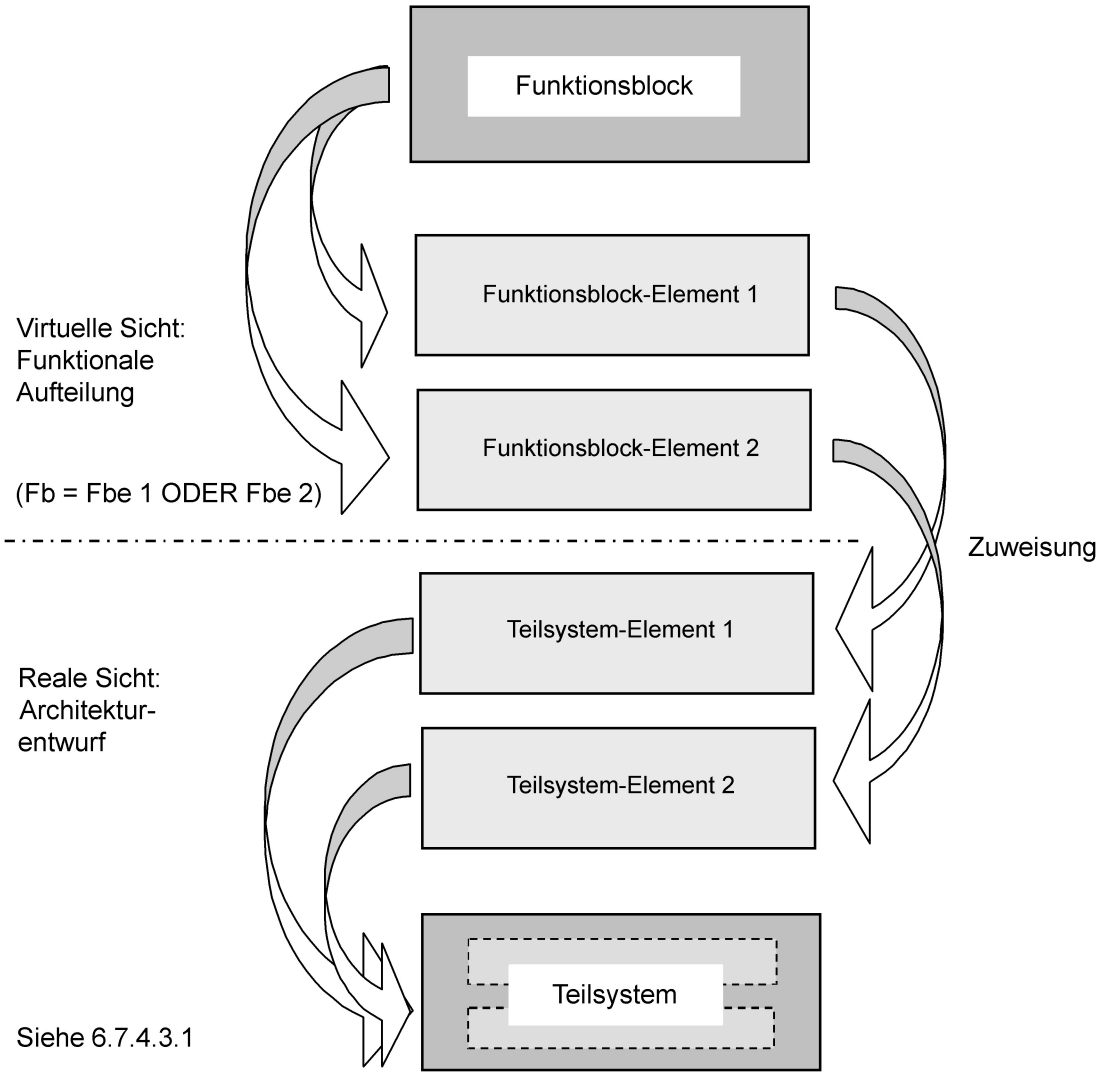


Bild 5 – Aufteilung eines Funktionsblocks in redundante Funktionsblock-Elemente und ihre zugehörigen Teilsystem-Elemente

6.7.4.3.1.2 Die Architektur des Teilsystems muss in Form ihrer Elemente und ihrer gegenseitigen Beziehungen dokumentiert werden. Wo notwendig, muss dies auch Informationen bezüglich Funktionsblock-Elementen, die zu Teilsystem-Elementen zugeordnet sind, einschließen.

6.7.4.4 Anforderungen für die Auswahl und den Entwurf von Teilsystem-Elementen

6.7.4.4.1 Teilsystem-Elemente müssen für ihre vorgesehene Verwendung geeignet sein und müssen mit relevanten internationalen Normen, soweit diese existieren, übereinstimmen.

6.7.4.4.2 Die folgenden Informationen müssen für jedes Teilsystem-Element vorhanden sein:

a) eine funktionale Spezifikation des Teilsystem-Elements;

b) Spezifikation der Schnittstellen des Teilsystem-Elements (z. B. elektrische Eigenschaften);

c) jeder Ausfallmodus und seine Auftrittswahrscheinlichkeit und wo relevant (z. B. für komplexe Bauteile, die in Übereinstimmung mit 6.7.4.2.3 verwendet werden), der Diagnosedeckungsgrad und die Wahrscheinlichkeit gefahrbringender Ausfälle;

ANMERKUNG Für elektromechanische Teilsysteme sollte die Ausfallwahrscheinlichkeit unter Berücksichtigung der vom Hersteller angegebenen Anzahl von Betriebszyklen und dem Nutzungsfaktor in der Anwendung abgeschätzt werden (siehe 5.2.3). Diese Informationen sollten auf dem B10-Wert basieren (d. h. dem erwarteten Zeitpunkt, an dem 10 % des Bestandes ausgefallen sein werden). Siehe auch IEC 61810-2[2)].

d) Einschränkungen für das Teilsystem-Element in Bezug auf:

– die Umgebung und die Betriebsbedingungen, die beachtet werden sollten, um die Gültigkeit der unter Punkt c) angegebenen Informationen zu gewährleisten und

– die Gebrauchsdauer des Teilsystem-Elements, die nicht überschritten werden sollte, um die Gültigkeit der unter Punkt c) angegebenen Informationen zu gewährleisten;

e) jeder wiederkehrende Proof-Test und/oder alle Instandhaltungsanforderungen;

f) Eigenschaften, die zur Diagnose beitragen können (z. B. mechanisch verbundene Kontakte);

g) alle zusätzlichen Informationen (z. B. Reparaturzeiten), die notwendig sind, um die Ableitung einer mittleren Zeit bis zur Wiederherstellung (MTTR) zu ermöglichen, die auf die Erkennung eines Fehlers durch die Diagnose folgt;

h) alle Grenzen für die Anwendung des Teilsystem-Elements, die zur Vermeidung von systematischen Ausfällen beachtet werden sollten;

i) Hardware-Fehlertoleranz.

6.7.5 Festlegung der sicherheitsbezogenen Leistungsfähigkeit des Teilsystems

Die sicherheitsbezogene Leistungsfähigkeit eines Teilsystems ist durch die SILCL gekennzeichnet, die durch seine strukturellen Einschränkungen (6.7.6), seine SILCL auf Grund systematischer Integrität (6.7.9) und seine Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls (6.7.8) festgelegt ist.

ANMERKUNG 1 Die SILCL eines Teilsystems setzt eine Grenze für den maximalen Sicherheits-Integritätslevel, der für eine sicherheitsbezogene Steuerungsfunktion in Anspruch genommen werden kann, die dieses Teilsystem verwendet.

ANMERKUNG 2 Informationen über alle drei Aspekte sind notwendig, um den durch das sicherheitsbezogene Steuerungssystem, das die zugeordnete SRCF ausführt, erreichten Sicherheits-Integritätslevel zu bestimmen.

6.7.6 Strukturelle Einschränkungen der Sicherheitsintegrität der Hardware von Teilsystemen

6.7.6.1 Im Kontext der Sicherheitsintegrität der Hardware ist der höchste Sicherheits-Integritätslevel, der für eine SRCF in Anspruch genommen werden kann, durch die Fehlertoleranzen der Hardware und die Anteile sicherer Ausfälle der Teilsysteme, die die SRCF ausführen, begrenzt. Tabelle 5 legt den höchsten Sicherheits-Integritätslevel fest, der für eine SRCF in Anspruch genommen werden kann, die ein Teilsystem verwendet. Dabei werden die Hardware-Fehlertoleranz und der Anteil sicherer Ausfälle dieses Teilsystems betrachtet. Die in Tabelle 5 angegebenen strukturellen Einschränkungen müssen auf jedes Teilsystem angewendet werden. Im Hinblick auf diese strukturellen Anforderungen:

a) bedeutet eine Hardware-Fehlertoleranz von N, dass $N + 1$ Fehler zu einem Verlust der SRCF führen können. Bei der Bestimmung der Hardware-Fehlertoleranz erfolgt keine Berücksichtigung von anderen Maßnahmen, die die Auswirkungen von Fehlern beherrschen könnten, wie zum Beispiel Diagnoseeinrichtungen und

b) müssen, wo ein Fehler direkt zu einem oder mehreren nachfolgenden Fehlern führt, diese Fehler als ein Einzelfehler betrachtet werden;

[2)] noch zu veröffentlichen

c) können bei der Bestimmung der Hardware-Fehlertoleranz bestimmte Fehler unter der Voraussetzung ausgeschlossen werden, dass die Wahrscheinlichkeit ihres Auftretens sehr gering ist im Verhältnis zu den Anforderungen zur Sicherheitsintegrität des Teilsystems. Jeder einzelne Fehlerausschluss muss begründet und dokumentiert werden (siehe auch 6.7.7).

6.7.6.2 Die strukturellen Einschränkungen der Tabelle 5 müssen auf jedes Teilsystem, das einen Funktionsblock einer SRCF ausführt, angewendet werden.

6.7.6.3 Ein Teilsystem, das nur ein einzelnes Teilsystem-Element enthält, muss die Anforderungen aus Tabelle 5 erfüllen. Ein SFF von größer als 99 % muss besonders bei einem solchen Teilsystem, das eine Hardware-Fehlertoleranz von null besitzt (d. h. $N = 0$), durch eine (mehrere) SRECS-Diagnosefunktion(en) erreicht werden.

ANMERKUNG Diese Anforderung ist notwendig, um sicherzustellen, dass eine angemessene Form der strukturellen Einschränkungen auf Teilsysteme angewendet wird, die nur ein einzelnes Teilsystem-Element umfassen, um eine SILCL von SIL 3 zu begründen.

Tabelle 5 – Strukturelle Einschränkungen von Teilsystemen: maximal in Anspruch nehmbarer SIL für eine SRCF, die dieses Teilsystem verwendet

Anteil sicherer Ausfälle	Hardware-Fehlertoleranz (siehe Anmerkung 1)		
	0	1	2
< 60 %	nicht erlaubt (siehe Anmerkung 3)	SIL 1	SIL 2
60 % bis < 90 %	SIL 1	SIL 2	SIL 3
90 % bis < 99 %	SIL 2	SIL 3	SIL 3 (siehe Anmerkung 2)
≥ 99 %	SIL 3	SIL 3 (siehe Anmerkung 2)	SIL 3 (siehe Anmerkung 2)

ANMERKUNG 1 Eine Hardware-Fehlertoleranz von N bedeutet, dass $N + 1$ Fehler zu einem Verlust der SRCF führen können.

ANMERKUNG 2 Eine SIL 4-Anspruchsgrenze wird in dieser Norm nicht betrachtet. Zu SIL 4 siehe IEC 61508-1.

ANMERKUNG 3 Ausnahme siehe 6.7.7.

6.7.6.4 Wenn ein Teilsystem in Übereinstimmung mit ISO 13849-1:1999 entworfen und gemäß ISO 13849-2:2003 validiert worden ist, kann die folgende Beziehung allein in Bezug auf die strukturellen Einschränkungen in Übereinstimmung mit Tabelle 6 angewendet werden.

Es wird angenommen, dass ein Teilsystem mit einer speziellen Kategorie, das ISO 13849-1 entspricht, die in Tabelle 6 angegebene zugehörige Hardware-Fehlertoleranz und den Anteil sicherer Ausfälle besitzt.

ANMERKUNG Um einen erforderlichen SIL zu erreichen, ist es ebenso notwendig, die Anforderungen zur Wahrscheinlichkeit gefahrbringender Ausfälle und zur systematischen Sicherheitsintegrität zu erfüllen.

Tabelle 6 – Strukturelle Einschränkungen: SILCL in Bezug auf Kategorien

Kategorie	Hardware-Fehlertoleranz	SFF	Maximale SIL-Anspruchsgrenze in Bezug auf strukturelle Einschränkungen
	Es wird angenommen, dass Teilsysteme mit der angegebenen Kategorie die unten angegebenen Merkmale besitzen.		
1	0	< 60 %	siehe Anmerkung 1
2	0	60 % bis 90 %	SIL 1
3	1	< 60 %	SIL 1
	1	60 % bis 90 %	SIL 2
4	> 1	60 % bis 90 %	SIL 3 (siehe Anmerkung 3)
	1	> 90 %	SIL 3 (siehe Anmerkung 4)

ANMERKUNG 1 Die Fälle von Kategorie 1 und 2, bei denen der Anteil sicherer Ausfälle < 60 % beträgt, werden im Zusammenhang von ISO 13849-1 als nicht relevant betrachtet, und Teilsysteme, die in Übereinstimmung mit ISO 13849-1 entworfen sind, werden in der Praxis einen SFF erreichen, der oberhalb von 60 % liegt.

ANMERKUNG 2 Es wird angenommen, dass der Fall einer Kategorie 2, bei der der Anteil sicherer Ausfälle > 90 % beträgt, durch die Entwurfsanforderungen von ISO 13849-1 nicht erreicht wird.

ANMERKUNG 3 Der Diagnosedeckungsgrad wird als kleiner 90 % für Teilsysteme der Kategorie 4 angenommen, bei denen mehr als eine einfache Hardware-Fehlertoleranz (d. h. akkumulierte Fehler) betrachtet wird.

ANMERKUNG 4 Kategorie 4 erfordert einen SFF von mehr als 90 %, jedoch weniger als 99 %, wenn eine einfache Hardware-Fehlertoleranz betrachtet wird.

ANMERKUNG 5 Kategorie B in Übereinstimmung mit ISO 13849-1 wird als nicht ausreichend betrachtet, um SIL 1 zu erreichen.

6.7.7 Abschätzung des Anteils sicherer Ausfälle (SFF)

6.7.7.1 Der SFF muss abgeschätzt werden, um wo erforderlich die SILCL auf Grund struktureller Einschränkungen zu bestimmen.

6.7.7.2 Zur Abschätzung des SFF muss eine Analyse (z. B. Fehlerbaumanalyse, Ausfallarten- und Effektanalyse) jedes Teilsystems ausgeführt werden, um alle relevanten Fehler und ihre korrespondierenden Ausfallarten zu bestimmen. Ob ein Ausfall ein sicherer oder ein gefahrbringender Ausfall ist, hängt vom SRECS und den beabsichtigten sicherheitsbezogenen Steuerungsfunktionen einschließlich der Fehlerreaktionsfunktion ab. Die Wahrscheinlichkeit jeder Ausfallart muss auf Basis der Wahrscheinlichkeit des (der) zugehörigen Fehler(s) unter Berücksichtigung der vorgesehenen Verwendung bestimmt werden und kann aus Quellen wie folgenden hergeleitet werden:

a) verlässliche Daten zu Ausfallraten, die durch Felderfahrung vom Hersteller gewonnen wurden und für die vorgesehene Verwendung relevant sind;

b) Bauteilausfalldaten, die aus einer anerkannten industriellen Quelle (siehe Referenzen in Anhang D) stammen und für die vorgesehene Verwendung relevant sind;

c) Daten zu Ausfallarten nach Angabe in Anhang D;

d) Daten zu Ausfallraten, die aus den Ergebnissen von Tests und Analyse abgeleitet sind.

AUSNAHME: Für ein Teilsystem, das eine Hardware-Fehlertoleranz von null besitzt und für das Fehlerausschlüsse zu Fehlern, die zu einem gefahrbringenden Ausfall führen können, angewendet worden sind, ist die SILCL in Bezug auf strukturelle Einschränkungen für dieses Teilsystem auf ein Maximum von SIL 2 beschränkt.

6.7.7.3 Die Anwendung von Fehlerausschlüssen muss begründet (z. B. durch Analyse) und dokumentiert werden.

ANMERKUNG Es ist zulässig, Fehler in Übereinstimmung mit 3.3 und Tabelle D.5 von ISO 13849-2 auszuschließen.

6.7.8 Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen

6.7.8.1 Allgemeine Anforderungen

6.7.8.1.1 Die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls muss gleich oder kleiner dem in der Spezifikation der Sicherheitsanforderungen des Teilsystems (siehe 6.6.2.1.7) festgelegten Ausfallgrenzwert sein.

6.7.8.1.2 Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls jedes Teilsystems in Folge zufälliger Hardwareausfälle in der Ausführung der zugeordneten Funktionsblöcke muss unter Berücksichtigung von Folgendem abgeschätzt werden:

a) der Architektur des Teilsystems in Bezug zu den betrachteten zugeordneten Funktionsblöcken;

ANMERKUNG 1 Dies schließt die Entscheidung ein, ob eine Hardware-Fehlertoleranz vorhanden ist oder nicht.

b) der Ausfallrate jedes Teilsystem-Elements in allen Modi, die zu einem gefahrbringenden Ausfall des Teilsystems führen, jedoch durch Diagnosetests erkannt werden (siehe 6.3);

c) der Ausfallrate jedes Teilsystem-Elements in allen Modi, die zu einem gefahrbringenden Ausfall des Teilsystems führen und welche durch Diagnosetests nicht erkannt werden (siehe 6.3);

d) der Anfälligkeit des Teilsystems für Ausfälle in Folge gemeinsamer Ursache, die einen gefahrbringenden Ausfall des Teilsystems verursachen würden (siehe Anmerkungen 2 und 3);

ANMERKUNG 2 Wo ein Vergleich redundanter Komponenten zur Fehlererkennung verwendet wird, kann ein Ausfall der Fehlererkennungsmaßnahmen erfolgen, wenn die redundanten Komponenten zur selben Zeit in gleicher Art ausfallen. Dies kann durch eine gemeinsame Ursache, bezeichnet als Ausfall in Folge gemeinsamer Ursache (CCF), erfolgen und wird als Betafaktor (ß) ausgedrückt. Ein vereinfachter Ansatz zur Abschätzung der Anfälligkeit für Ausfälle in Folge gemeinsamer Ursache ist in 6.7.8.3 angegeben. Für weitere Anleitung zur Quantifizierung der Auswirkung von hardwarebezogenen Ausfällen in Folge gemeinsamer Ursache siehe auch IEC 61508-6, Anhang D.

e) dem Diagnosedeckungsgrad der Diagnosetests (siehe 3.2.28) und dem zugehörigen Diagnose-Testintervall;

f) den Intervallen, innerhalb denen Proof-Tests ausgeführt werden, um gefahrbringende Fehler zu erkennen, die durch Diagnosetests nicht erkannt werden und/oder der Einsatzdauer des (der) Teilsystem-Elements (Teilsystem-Elemente), die nicht überschritten werden sollten, um die Gültigkeit der unter den Punkten b) und c) angegebenen Informationen beizubehalten;

g) den Reparaturzeiten für erkannte Fehler, wenn das Teilsystem für Reparatur im Betrieb entworfen ist.

ANMERKUNG 3 Die maximale Reparaturzeit bildet einen Teil der Zeit bis zur Wiederherstellung (siehe IEV 191-10-05), die auch die Zeit bis zur Erkennung eines Fehlers und jede Zeitdauer, in der eine Reparatur nicht möglich ist, einschließt (siehe IEC 61508-6, Anhang B für ein Beispiel, wie die mittlere Zeit bis zur Wiederherstellung in der Berechnung der Wahrscheinlichkeit eines Ausfalls verwendet werden kann). In Fällen, in denen eine Reparatur nur während einer speziellen Zeitspanne ausgeführt werden kann, während die Maschine abgeschaltet ist und sich in einem sicheren Zustand befindet, ist es besonders wichtig, dass die Zeitdauer, in der keine Reparatur durchgeführt werden kann, vollständig berücksichtigt wird. Besonders wichtig ist dies, wenn diese Zeitdauer relativ groß ist.

ANMERKUNG 4 Ein vereinfachter Ansatz zur Abschätzung der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls von Teilsystemen ist in 6.7.8.2 angegeben. Es stehen andere Verfahren zur Verfügung und die Auswahl des am besten passenden Verfahrens wird von den Umständen abhängen. Brauchbare Verfahren schließen ein:

a) Fehlerbaum-Analyse (siehe B.6.6.5 von IEC 61508-7 und IEC 61025);

b) Markov-Modelle (siehe C.6.4 von IEC 61508-7 und IEC 61125-13);

c) Zuverlässigkeits-Blockdiagramme (siehe C.6.5 von IEC 61508-7).

ANMERKUNG 5 Ausfälle in Folge gemeinsamer Ursachenfolgen und Datenkommunikationsprozesse können von anderen Effekten als tatsächlichen Ausfällen von Hardwarebauteilen herrühren (z. B. elektromagnetischer Beeinflussung, Softwarefehlern usw.). Siehe 6.7.9.

6.7.8.1.3 Für Teilsysteme oder Teilsystem-Elemente, bei denen die Wahrscheinlichkeit eines Ausfalls in Beziehung zu einer Anzahl von Betriebszyklen angegeben ist, müssen diese Werte unter Verwendung des festgelegten Nutzungsfaktors für die relevanten SRCFs in zeitbezogene Werte transformiert werden (siehe 5.2.3).

6.7.8.1.4 Das Diagnose-Testintervall jedes Teilsystems, das eine Hardware-Fehlertoleranz von mehr als null besitzt, muss so gewählt sein, dass das Teilsystem die Anforderung zur Wahrscheinlichkeit eines zufälligen Hardwareausfalls erfüllen kann (siehe 6.3.1).

ANMERKUNG Dieses Diagnose-Testintervall sollte so gewählt sein, dass ein Fehler vor dem Auftreten eines nachfolgenden Fehlers, der zu einem gefahrbringenden Ausfall des Teilsystems führen kann und den Ausfallgrenzwert überschreitet, erkannt wird.

6.7.8.1.5 Das Diagnose-Testintervall jedes Teilsystems, das eine Hardware-Fehlertoleranz von null besitzt, muss so gewählt sein, dass die Anforderungen aus 6.3.2 erfüllt werden.

6.7.8.1.6 Wenn ein Teilsystem niedriger Komplexität in Übereinstimmung mit ISO 13849-1 entworfen und gemäß ISO 13849-2 validiert worden ist und weiterhin die Anforderungen zu strukturellen Einschränkungen (siehe 6.7.6) und zur systematischen Sicherheitsintegrität (siehe 6.7.9) erfüllt, können die in Tabelle 7 angegebenen Grenzwerte zur Wahrscheinlichkeit eines gefahrbringenden Ausfalls (PFH_{D}) verwendet werden, um die Sicherheitsintegrität der Hardware (siehe 6.6.3.2) abzuschätzen.

Tabelle 7 – Wahrscheinlichkeit eines gefahrbringenden Ausfalls

Kategorie	Hardware-Fehlertoleranz	DC	PFH_D Grenzwerte (pro Stunde), die für das Teilsystem in Anspruch genommen werden können PFH_D (MTTF$_{Teilsystem}$, T$_{Test}$, DC) (siehe Anmerkung 1)
	Es wird angenommen, dass Teilsysteme mit der angegebenen Kategorie die unten angegebenen Merkmale besitzen.		
1	0	0 %	vom Lieferanten anzugeben oder Verwendung von allgemeingültigen Daten (siehe Anhang D)
2	0	60 % bis 90 %	≥ 10^{-6}
3	1	60 % bis 90 %	≥ 2 x 10^{-7}
4	> 1	60 % bis 90 %	≥ 3 x 10^{-8}
	1	> 90 %	≥ 3 x 10^{-8}

ANMERKUNG 1 Der PFH_D-Grenzwert ist eine Funktion der MTTF des Teilsystems (durch den Hersteller des Teilsystems oder aus Datenbüchern relevanter Bauteile herzuleiten), der Test/Überprüfungszykluszeit wie in der Spezifikation der Sicherheitsanforderungen festgelegt (diese Information ist auch für Validierung des Teilsystems in Übereinstimmung mit ISO 13849-2, 3.5 erforderlich) und dem Diagnosedeckungsgrad wie in dieser Tabelle gezeigt (diese Werte basieren auf den Anforderungen der in ISO 13849-1 beschriebenen Kategorien).

ANMERKUNG 2 Kategorie B in Übereinstimmung mit ISO 13849-1 kann nicht als ausreichend betrachtet werden, um SIL 1 zu erreichen.

6.7.8.2 Vereinfachter Ansatz zur Abschätzung der Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen

6.7.8.2.1 Allgemeines

Dieser Unterabschnitt beschreibt einen vereinfachten Ansatz zur Abschätzung der Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle für eine Anzahl von grundlegenden Teilsystemarchitekturen und enthält Formeln, die für Teilsysteme verwendet werden können, die entweder aus Teilsystem-Elementen niedriger Komplexität oder komplexen Teilsystem-Elementen zusammengesetzt sind. Die Formeln selbst stellen eine Vereinfachung der Theorie der Zuverlässigkeitsanalyse dar und sind dazu bestimmt, Abschätzungen in die sichere Richtung bereitzustellen. Die Vorbedingung für die Gültigkeit aller in diesem Unterabschnitt angegebenen Formeln ist, dass 1 >> $\lambda \times T_1$, wobei T_1 der kleinere Wert des Intervalls für den Proof-Test oder der Gebrauchsdauer ist und das Teilsystem in der „Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung“ betrieben wird (siehe 3.2.27). Siehe auch 6.8.6.

ANMERKUNG 1 Die erhaltenen Ergebnisse stellen eine Einschränkung in Bezug auf die Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen dar und in Fällen, wo dies nicht akzeptabel erscheint, ist es möglich, genauere Modellierungsverfahren anzuwenden (siehe 6.7.8.1.1).

ANMERKUNG 2 Für die in 6.7.8.2 angegebenen Gleichungen (A) bis (D) sind konstante und ausreichend geringe (1 >> $\lambda \times T$) Ausfallraten (λ) der Teilsystem-Elemente angenommen (dies bedeutet, dass die mittlere Zeit bis zum gefahrbringenden Ausfall sehr viel größer als das Intervall für den Proof-Test oder als die Gebrauchsdauer des Teilsystems zu sein hat). Daher können die folgenden Basisgleichungen verwendet werden:

– λ = 1/MTTF

Für elektromechanische Geräte wird die Ausfallrate durch Verwendung des B10-Wertes und der Anzahl der für die Anwendung festgelegten Betriebszyklen C (siehe 5.2.3) bestimmt.

– $\lambda = 0{,}1 \times C/B_{10}$

ANMERKUNG 3 Die Ausdrücke werden wie folgt verwendet:

– $\lambda = \lambda_S + \lambda_D$; wobei λ_S die Rate sicherer Ausfälle und λ_D die Rate gefahrbringender Ausfälle darstellt,

– $PFH_D = \lambda_D \times 1h$; mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls innerhalb einer Stunde,

– T_2: Diagnose-Testintervall,

– T_1: der kleinere Wert von Proof-Test-Intervall oder Gebrauchsdauer.

6.7.8.2.2 Basis-Teilsystemarchitektur A: Nullfehlertoleranz ohne Diagnosefunktion

In dieser Architektur verursacht jeder gefahrbringende Ausfall eines Teilsystem-Elements einen Ausfall der SRCF. Für Architektur A ergibt sich die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Teilsystems aus der Summe der Wahrscheinlichkeiten gefahrbringender Ausfälle aller Teilsystem-Elemente:

$$\lambda_{DssA} = \lambda_{Del} + ... + \lambda_{Den} \quad \text{(A)}$$

$$PFH_{DssA} = \lambda_{DssA} \times 1\,h$$

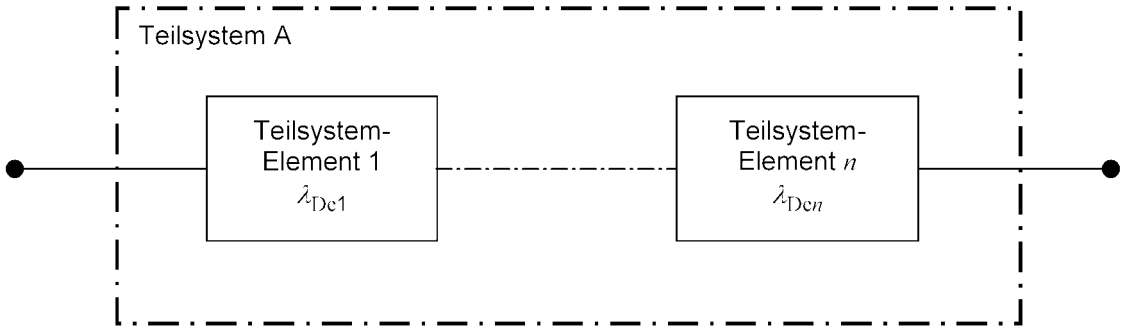


Bild 6 – Logische Darstellung Teilsystem A

ANMERKUNG Bild 6 stellt eine logische Darstellung der Architektur des Teilsystems A dar und sollte nicht als seine physikalische Implementierung betrachtet werden.

6.7.8.2.3 Basis-Teilsystemarchitektur B: Einfehlertoleranz ohne Diagnosefunktion

Diese Architektur ist so ausgelegt, dass ein einzelner Ausfall irgendeines Teilsystem-Elements keinen Verlust der SRCF verursacht. Deshalb müsste ein gefahrbringender Ausfall in mehr als einem Element vorliegen, bevor ein Ausfall der SRCF auftreten kann. Für Architektur B beträgt die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Teilsystems:

$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{Del} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{Del} + \lambda_{De2})/2 \quad \text{(B)}$$

$$PFH_{DssB} = \lambda_{DssB} \times 1h$$

wobei

T_1 der kleinere Wert von Proof-Test-Intervall oder Gebrauchsdauer ist,

β die Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache ist.

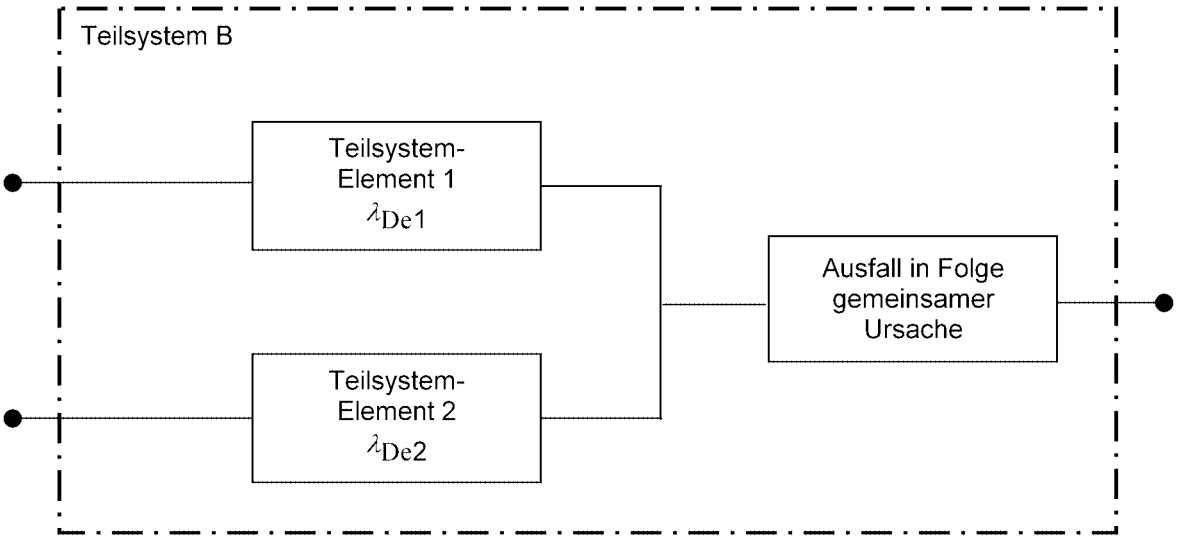


Bild 7 – Logische Darstellung Teilsystem B

ANMERKUNG Bild 7 stellt eine logische Darstellung der Architektur des Teilsystems B dar und sollte nicht als seine physikalische Implementierung betrachtet werden.

6.7.8.2.4 Basis-Teilsystemarchitektur C: Nullfehlertoleranz mit Diagnosefunktion

Jeder unerkannte gefahrbringende Fehler des Teilsystem-Elements führt zu einem gefahrbringenden Ausfall der SRCF. Wenn ein Fehler eines Teilsystem-Elements erkannt wird, leitet (leiten) die Diagnosefunktion(en) eine Fehlerreaktionsfunktion ein (siehe 6.3.2). Für Architektur C beträgt die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Teilsystems:

$$\lambda_{DssC} = \lambda_{Del} + (1 - DC_1) + ... + \lambda_{Den} (1 - DC_n) \qquad \text{(C)}$$

$$PFH_{DssC} = \lambda_{DssC} \times 1\ h$$

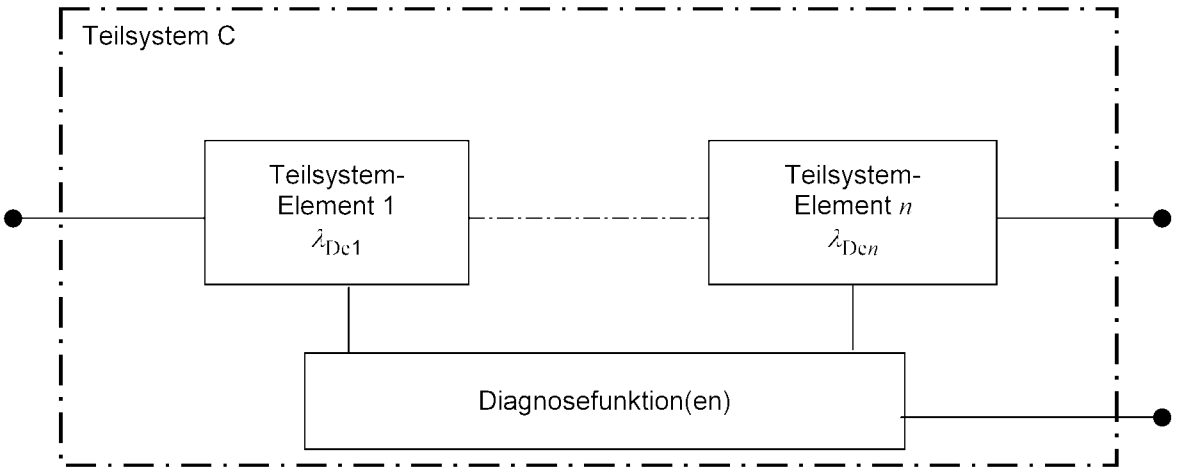


Bild 8 – Logische Darstellung Teilsystem C

ANMERKUNG Bild 8 stellt eine logische Darstellung der Architektur des Teilsystems C dar und sollte nicht als seine physikalische Implementierung betrachtet werden. Die gezeigte Diagnosefunktion kann ausgeführt werden durch:

– das Teilsystem, für das die Diagnose erforderlich ist oder

– andere Teilsysteme des SRECS oder

– Teilsysteme, die nicht an der Ausführung der sicherheitsbezogenen Steuerungsfunktion beteiligt sind.

6.7.8.2.5 Basis-Teilsystemarchitektur D: Einfehlertoleranz mit Diagnosefunktion(en)

Diese Architektur ist so ausgelegt, dass ein einzelner Ausfall irgendeines Teilsystem-Elements keinen Verlust der SRCF verursacht, wobei

T_2 das Diagnose-Testintervall ist,

T_1 der kleinere Wert von Proof-Test-Intervall oder Gebrauchsdauer ist,

β die Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache ist; $\lambda_D = \lambda_{DD} + \lambda_{DU}$; wobei λ_{DD} die Rate erkennbarer gefahrbringender Ausfälle und λ_{DU} die Rate nicht erkennbarer gefahrbringender Ausfälle darstellt,

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

$\lambda_{DU} = \lambda_D \times (1 - DC)$

Für Teilsystem-Elemente unterschiedlicher Konstruktion:

λ_{De1} entspricht der Rate gefahrbringender Ausfälle von Teilsystem-Element 1;

DC_1 entspricht dem Diagnosedeckungsgrad von Teilsystem-Element 1;

λ_{De2} entspricht der Rate gefahrbringender Ausfälle von Teilsystem-Element 2;

DC_2 entspricht dem Diagnosedeckungsgrad von Teilsystem-Element 2.

$$\lambda_{DssD} = (1-\beta)^2 \left\{ \left[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \right] \times T_2/2 + \left[\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \right] \times T_1/2 \right\} + \beta \times (\lambda_{De1} \times \lambda_{De2})/2 \quad \text{(D.1)}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

Für Teilsystem-Elemente gleicher Konstruktion:

λ_{De} entspricht der Rate gefahrbringender Ausfälle von Teilsystem-Element 1 oder 2;

DC entspricht dem Diagnosedeckungsgrad von Teilsystem-Element 1 oder 2.

$$\lambda_{DssD} = (1-\beta)^2 \left\{ \left[\lambda_{De}^2 \times 2 \times DC \right] \times T_2/2 + \left[\lambda_{De}^2 \times (1 - DC) \right] \times T_1 \right\} + \beta \times \lambda_{De} \quad \text{(D.2)}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

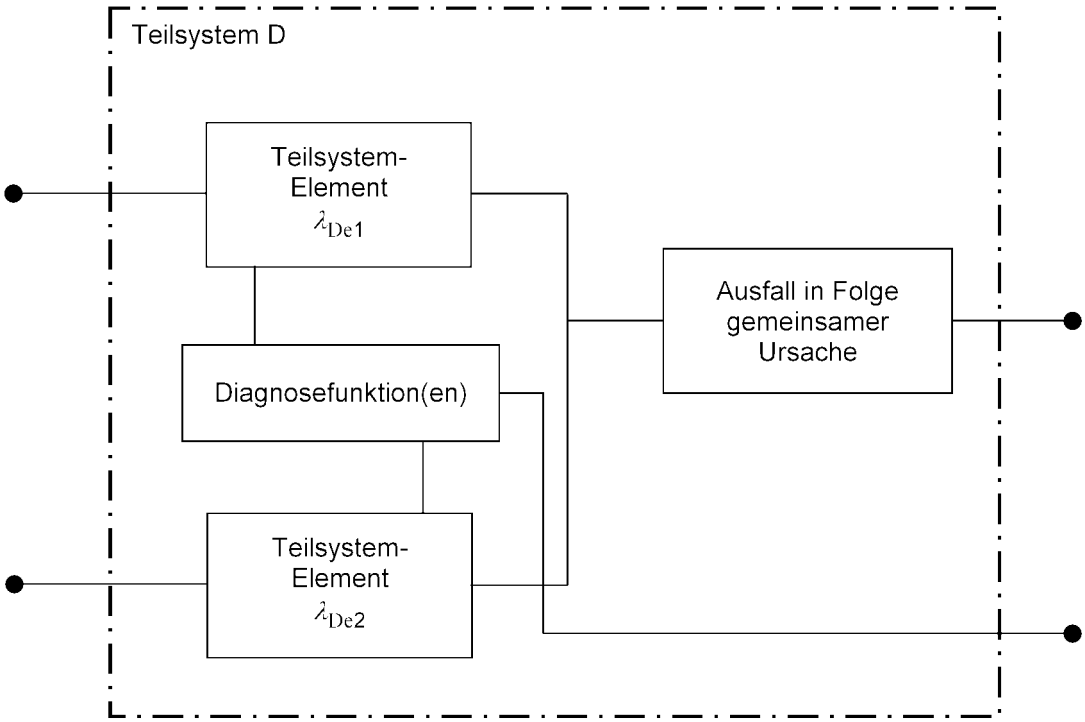


Bild 9 – Logische Darstellung Teilsystem D

ANMERKUNG 1 Bild 9 stellt eine logische Darstellung der Architektur des Teilsystems D dar und sollte nicht als seine physikalische Implementierung betrachtet werden. Die gezeigte(n) Diagnosefunktion(en) kann (können) ausgeführt werden durch:

– das Teilsystem, für das die Diagnose erforderlich ist oder

– andere Teilsysteme des SRECS oder

– Teilsysteme, die nicht an der Ausführung der sicherheitsbezogenen Steuerungsfunktion beteiligt sind.

ANMERKUNG 2 Als Fehlerreaktion für dieses Teilsystem wird, wie nach 6.3.1 erforderlich, die Beendigung des relevanten Betriebs angenommen. Wenn eine Reparatur während des Betriebs im Entwurf enthalten ist, bei der die Fehlerreaktion den Fehler meldet, aber nicht den relevanten Betrieb beendet, sollte für die verbleibende Architektur eine neue PFH_D des Teilsystems nach dem Auftreten eines ersten Fehlers bestimmt werden.

6.7.8.3 Vereinfachter Ansatz zur Abschätzung des Beitrags von Ausfällen in Folge gemeinsamer Ursache (CCF)

6.7.8.3.1 Es sind Kenntnisse über die Anfälligkeit eines Teilsystems für CCF erforderlich, um zur Abschätzung der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls eines Teilsystems (siehe 6.7.8.1) beizutragen.

6.7.8.3.2 Wenn eine redundante Architektur verwendet wird, um die erforderliche Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls eines Teilsystems zu erreichen und ein (mehrere) CCF(s) die Wirkung dieser Redundanz beseitigen kann (können), muss die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls auf Basis des Auftretens der gemeinsamen Ursache zur Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls eines Teilsystems auf Basis der Verwendung von Redundanz addiert werden.

6.7.8.3.3 Die Wahrscheinlichkeit des Auftretens des CCF wird normalerweise von einer Kombination aus Technologie, Architektur, Anwendung und Umgebung abhängen. Die Anwendung von Anhang F wird zur Vermeidung vieler Arten von CCF wirksam sein.

6.7.8.3.4 Anhang F enthält eine Punktetabelle und eine zugehörige Methodologie, die verwendet werden kann, um die Wirksamkeit der im Entwurf des Teilsystems zur Begrenzung der Anfälligkeit für CCF angewendeten Maßnahmen abzuschätzen.

6.7.9 Anforderungen zur systematischen Sicherheitsintegrität von Teilsystemen

Die SILCL in Bezug auf systematische Sicherheitsintegrität eines Teilsystems beträgt bis zu SIL 3, wenn die Anforderungen in 6.7.9.1 und 6.7.9.2 erfüllt sind.

ANMERKUNG Diese Anforderungen sind auf der „Ebene von Teilsystemen“ anwendbar, auf der Teilsystem-Elemente miteinander verbunden werden, um ein Teilsystem zu realisieren. Zu anderen, für die Realisierung eines SRECS relevanten Anforderungen, siehe 6.4.

6.7.9.1 Anforderungen zur Vermeidung von systematischen Ausfällen

6.7.9.1.1 Die folgenden Maßnahmen müssen angewendet werden:

a) richtige Auswahl, Kombination, Anordnung, Montage und Installation von Komponenten einschließlich Verkabelung, Verdrahtung und aller Verbindungen: Beachtung der Herstellerangaben zur Anwendung und Anwendung bewährter Praktiken;

b) Verwendung von Teilsystemen und Teilsystem-Elementen im Rahmen der Spezifikation des Herstellers und der Installationsanweisungen;

c) Verträglichkeit: Verwendung von Bauteilen mit passenden Betriebseigenschaften;

d) Widerstandsfähigkeit gegenüber festgelegten Umgebungsbedingungen: Entwurf des Teilsystems in der Art, dass es fähig ist, in allen erwarteten Umgebungen und unter allen vorhersehbaren widrigen Bedingungen betrieben zu werden, zum Beispiel Temperatur, Feuchtigkeit, Vibration und elektromagnetische Beeinflussung (EMI) (siehe ISO 13849-2, D.1);

e) Verwendung von Bauteilen, die in Übereinstimmung mit einer zutreffenden Norm übereinstimmen und deren Ausfallarten klar definiert sind: Reduzierung des Risikos unerkannter Fehler durch die Verwendung von Bauteilen mit spezifischen Eigenschaften;

f) Verwendung von geeigneten Materialien und passender Verarbeitung: Auswahl des Materials, Verarbeitungsmethoden und Behandlung in Bezug auf zum Beispiel Beanspruchung, Haltbarkeit, Elastizität, Reibung, Abnutzung, Korrosion, Temperatur, Leitfähigkeit, dielektrische Festigkeit;

g) korrekte Dimensionierung und Gestaltung: Betrachtung der Einflüsse von zum Beispiel Beanspruchung, Belastung, Abnutzung, Temperatur, Oberflächenrauigkeit, Herstellungstoleranzen.

6.7.9.1.2 Zusätzlich müssen eine oder mehrere der folgenden Maßnahmen unter Berücksichtigung der Komplexität des Teilsystems angewendet werden:

a) Hardware-Entwurfsüberprüfung (z. B. durch Inspektion oder Walkthrough): Aufdeckung von Unstimmigkeiten zwischen der Spezifikation und der Implementierung durch Reviews und/oder Analyse;

ANMERKUNG 1 Um Unstimmigkeiten zwischen der Spezifikation und Implementierung aufzudecken, werden alle zweifelhaften Punkte oder mögliche Schwachpunkte in Bezug auf die Realisierung, die Implementierung und die Verwendung des Produkts dokumentiert, so dass sie gelöst werden können. In Betracht zu ziehen ist, dass bei einem Inspektionsverfahren der Autor passiv und der Inspektor aktiv ist, während bei einem Walkthrough-Verfahren der Autor aktiv und der Inspektor passiv ist.

b) rechnergestützte Entwurfswerkzeuge mit der Fähigkeit zur Simulation oder Analyse: Systematische Ausführung der Entwurfsverfahren und Einbeziehung passender automatischer Konstruktionselemente, die bereits verfügbar und getestet sind;

ANMERKUNG 2 Die Integrität dieser Werkzeuge kann durch spezifische Tests, durch eine umfassende Historie zufrieden stellender Verwendung oder durch eine unabhängige Verifikation ihrer Ausgaben demonstriert werden. Siehe 6.11.3.4.

c) Simulation: Ausführung einer systematischen Simulation eines Teilsystementwurfs sowohl im Hinblick auf die funktionale Leistungsfähigkeit als auch auf die korrekte Dimensionierung seiner Bauteile.

ANMERKUNG 3 Die Funktion des Teilsystems kann auf einem Rechner durch ein Softwareverhaltensmodell (siehe 6.11.3.4) simuliert werden, in dem einzelne Bauteile der Schaltung ihr eigenes simuliertes Verhalten haben und die Reaktion des Teilsystems, in dem sie verbunden sind, untersucht wird, indem die Grenzdaten jedes Bauteils betrachtet werden.

6.7.9.2 Anforderungen zur Beherrschung von systematischen Ausfällen

6.7.9.2.1 Die folgenden Maßnahmen müssen angewendet werden:

a) Maßnahmen zur Beherrschung der Einflüsse von Isolationsversagen, Spannungsänderungen und -einbrüchen, Überspannung und Unterspannung: Das Verhalten des Teilsystems als Reaktion auf Isolationsverlust, Spannungsänderungen und -einbrüchen, Überspannungs- und Unterspannungsbedingungen muss vorbestimmt sein, so dass das Teilsystem einen sichereren Zustand des SRECS erreichen oder aufrechterhalten kann.

ANMERKUNG 1 Siehe auch relevante Anforderungen von IEC 60204-1, insbesondere:

– Überspannung sollte früh genug erkannt werden, so dass alle Ausgänge durch die Power-down-Routine in einen sicheren Zustand umgeschaltet werden können oder eine Umschaltung auf eine zweite Energieversorgung erfolgen kann und/oder

– die Steuerkreisspannung sollte überwacht werden und wenn sie sich nicht innerhalb ihres spezifizierten Bereiches befindet, sollte eine Energieabschaltung oder eine Umschaltung auf eine zweite Energieversorgung eingeleitet werden und/oder

– Überspannung oder Unterspannung sollte früh genug erkannt werden, um den internen Zustand in einem Festspeicher sichern zu können (falls erforderlich), so dass alle Ausgänge durch die Power-down-Routine in einen sicheren Zustand gesetzt werden können oder eine Umschaltung auf eine zweite Energieversorgung erfolgen kann.

b) Maßnahmen zur Beherrschung oder Vermeidung von Einflüssen der physikalischen Umgebung (zum Beispiel Temperatur, Feuchtigkeit, Wasser, Vibration, Staub, korrosive Substanzen, elektromagnetische Beeinflussung und ihre Auswirkungen): Das Verhalten des Teilsystems als Reaktion auf die Einflüsse der physikalischen Umgebung muss vorbestimmt sein, so dass das SRECS einen sichereren Zustand der Maschine erreichen oder aufrechterhalten kann. Siehe auch IEC 60204-1.

c) Maßnahmen zur Beherrschung oder Vermeidung der Einflüsse eines Temperaturanstiegs oder -abfalls, falls Temperaturänderungen auftreten können: Das Teilsystem sollte so entworfen werden, dass zum Beispiel Übertemperaturen erkannt werden können, bevor es außerhalb der Spezifikation betrieben wird.

ANMERKUNG 2 Weitere Informationen sind in IEC 61508-7, A.10 enthalten.

6.7.9.2.2 Zusätzlich müssen die folgenden Maßnahmen, soweit zutreffend, zur Beherrschung systematischer Ausfälle angewendet werden:

– Erkennung von Ausfällen durch Überwachung während des Betriebs;
– Tests durch Vergleich von redundanter Hardware;
– diversitäre Hardware;
– zwangläufiger Betätigungsmodus (z. B. ein Grenzschalter wird betätigt, wenn eine trennende Schutzeinrichtung geöffnet wird);
– gerichtete Ausfälle;
– Überdimensionierung mit einem geeigneten Faktor, wo der Hersteller aufzeigen kann, dass Unterlastung die Zuverlässigkeit erhöhen wird.

ANMERKUNG 1 Wo Überdimensionierung angemessen ist, sollte mindestens ein Überdimensionierungsfaktor von 1,5 verwendet werden.

ANMERKUNG 2 Weitere Informationen sind in ISO 13849-2, D.3 enthalten.

6.7.10 Teilsystemmontage

Die Teilsystem-Elemente müssen in Übereinstimmung mit 6.7.4.3.1.2 und dem dokumentierten detaillierten Entwurf kombiniert werden, um das Teilsystem zu bilden.

6.8 Realisierung von Diagnosefunktionen

6.8.1 Jedes Teilsystem muss mit zugehörigen Diagnosefunktionen ausgestattet sein, die notwendig sind, um die Anforderungen zu den strukturellen Einschränkungen (6.7.6) und zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle (6.7.8) zu erfüllen.

6.8.2 Die Diagnosefunktionen werden als separate Funktionen betrachtet, die eine andere Struktur als die SRCF haben können und die ausgeführt werden können durch:

– das gleiche Teilsystem, für das die Diagnose erforderlich ist oder

– andere Teilsysteme des SRECS oder

– Teilsysteme des SRECS, die nicht an der Ausführung der SRCF beteiligt sind.

ANMERKUNG Siehe auch Anmerkung 3 von 6.6.2.1.

6.8.3 Diagnosefunktionen müssen folgenden Punkten, die auf ihre zugehörigen SRCFs anwendbar sind, genügen:

– Anforderungen für die Vermeidung von systematischen Ausfällen (siehe 6.7.9.1) und

– Anforderungen für die Beherrschung von systematischen Ausfällen (siehe 6.7.9.2).

6.8.4 Die Wahrscheinlichkeit eines Ausfalls der SRECS-Diagnosefunktion(en) muss bei der Abschätzung der Wahrscheinlichkeit gefahrbringender Ausfälle der SRCF berücksichtigt werden.

ANMERKUNG 1 Siehe auch Anmerkung 3 von 6.6.2.1.

ANMERKUNG 2 Zeitliche Einschränkungen, die auf die Testung des Teilsystems, das eine Diagnosefunktion ausführt, anwendbar sind, können von denjenigen, die auf die SRCFs anwendbar sind, abweichen. Allgemein sollte das Testintervall Anforderungen erfüllen, die auf ein Teilsystem mit einer Hardware-Fehlertoleranz von eins anwendbar sind.

ANMERKUNG 3 Der Ausfall einer (mehrerer) Diagnosefunktion(en) sollte erkannt werden, und es sollte eine angemessene Reaktion erfolgen, um sicherzustellen, dass der Beitrag der Diagnosefunktion zur Sicherheitsintegrität der SRCF erhalten bleibt. Der Ausfall einer (mehrerer) Diagnosefunktion(en) kann eventuell durch Tests während des Betriebs, Kreuzvergleich bei redundanter Hardware usw. erkannt werden.

6.8.5 Es muss eine klare Beschreibung der SRECS-Diagnosefunktion(en), ihrer Ausfallerkennung und ihrer Reaktion auf den Ausfall sowie eine Analyse ihres Beitrages zur Sicherheitsintegrität der zugehörigen SRCFs bereitgestellt werden.

6.8.6 Um den vereinfachten Ansatz zur Abschätzung der Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen (6.7.8.2) anzuwenden, muss Folgendes zutreffen:

– wenn eine (mehrere) SRECS-Diagnosefunktion(en) notwendig ist(sind), um die erforderliche Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls zu erreichen und das Teilsystem eine Hardware-Fehlertoleranz von null aufweist, müssen die Fehlererkennung und die festgelegte Fehlerreaktion erfolgen, bevor die Gefährdung durch diesen Fehler auftreten kann, und

– eine (mehrere) SRECS-Diagnosefunktion(en) muss (müssen) mindestens so implementiert werden, dass die Wahrscheinlichkeit eines zufälligen Hardwareausfalls und die systematische Sicherheitsintegrität gleich sind mit den für die entsprechenden SRCF(s) festgelegten oder

ANMERKUNG 1 Strukturelle Einschränkungen zur Sicherheitsintegrität der Hardware müssen nicht auf die Realisierung von Diagnosefunktion(en) angewendet werden.

– wenn die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls eine Größenordnung größer als die für die SRCF spezifizierte ist, muss ein Test durchgeführt werden, um festzustellen, ob die Diagnosefunktion(en) oder die Diagnoseeinrichtung(en) noch in Betrieb sind. Es wird vorausgesetzt, dass ein solcher Test der Diagnosefunktion(en) oder Diagnoseeinrichtung(en) mindestens 10-mal während des Zeitraums zwischen auf das Teilsystem angewendeten Proof-Tests ausgeführt wird.

ANMERKUNG 2 Ein Test der Diagnosefunktion(en) sollte soweit möglich 100 % derjenigen Teile, die Diagnosefunktion(en) ausführen, abdecken.

ANMERKUNG 3 Wo eine Diagnosefunktion von einer Logikeinheit des SRECS ausgeführt wird, kann es unnötig sein, einen getrennten Test der Diagnosefunktion durchzuführen, da ihr Ausfall wie ein Ausfall der SRCF aufgedeckt werden kann.

ANMERKUNG 4 Ein Test kann entweder durch externe Mittel (z. B. Testeinrichtungen) oder interne dynamische Überprüfungen (z. B. eingebettet innerhalb der Logikeinrichtung) des SRECS durchgeführt werden.

6.9 Hardware-Implementierung des SRECS

Das SRECS muss in Überstimmung mit dem dokumentierten SRECS-Entwurf implementiert werden.

6.9.1 SRECS-Verbindungen

6.9.1.1 Das SRECS muss so verbunden werden, dass die entsprechenden Teile der Spezifikation der SRECS-Sicherheitsanforderungen und die relevanten Anforderungen in Bezug auf die Handhabung von Leitern, Verkabelung und Verdrahtung nach IEC 60204-1 eingehalten werden.

6.9.1.2 Maßnahmen zur Vermeidung und Beherrschung von Ausfällen von Verbindungsleitungen und Kabeln müssen in Übereinstimmung mit 6.4.1 und 6.4.2 realisiert werden.

6.10 Spezifikation der Software-Sicherheitsanforderungen

6.10.1 Allgemeines

Wenn Software in irgendeinem Teil eines SRECS, das eine (mehrere) sicherheitsbezogene Steuerungsfunktion(en) ausführt, verwendet wird, muss eine Spezifikation der Software-Sicherheitsanforderungen entwickelt und dokumentiert werden.

6.10.2 Anforderungen

6.10.2.1 Es muss eine Spezifikation der Software-Sicherheitsanforderungen für jedes Teilsystem auf der Basis der SRECS-Spezifikation und Architektur entwickelt werden.

6.10.2.2 Die Spezifikation der Anforderungen zur Softwaresicherheit für jedes Teilsystem muss aus (1) den spezifizierten Sicherheitsanforderungen der SRCF, (2) den Anforderungen, die aus der SRECS-Architektur resultieren und (3) allen Anforderungen des Plans der funktionalen Sicherheit (siehe 4.2) abgeleitet werden. Diese Informationen müssen dem Entwickler der Anwendungssoftware zur Verfügung gestellt werden.

6.10.2.3 Die Spezifikation der Anforderungen an die Anwendungssoftware bezüglich der Sicherheit muss hinreichend genau sein, um es dem Entwurf und der Implementierung des SRECS zu ermöglichen, die erforderliche Sicherheitsintegrität zu erreichen und um Verifikation zu erlauben.

6.10.2.4 Der Entwickler der Anwendungssoftware muss die Informationen in der Spezifikation überprüfen, um sicherzustellen, dass die Anforderungen angemessen spezifiziert sind. Insbesondere muss der Softwareentwickler Übereinstimmung mit dieser Norm durch Einbeziehung von Folgendem herstellen:

– SRCFs;
– Konfiguration oder Architektur des Systems;
– Kapazität und Leistungsfähigkeit in Bezug auf Reaktionszeit;
– Einrichtungen und Anwenderschnittstellen;
– aller relevanten Betriebsmodi der Maschine wie in der Spezifikation der Sicherheitsanforderungen festgelegt;
– Diagnosetests externer Geräte (z. B. Sensoren und Stellglieder).

6.10.2.5 Die spezifizierten Anforderungen zur Software-Sicherheit müssen so beschrieben und strukturiert werden, dass sie wie folgt sind:

– verständlich, verifizierbar, testbar, pflegbar, betriebsfähig und angemessen zum Sicherheits-Integritätslevel;
– rückführbar auf die Spezifikation der Sicherheitsanforderungen des SRECS;
– frei von missverständlichen Ausdrücken und Beschreibungen.

6.10.2.6 Die Spezifikation der Software-Sicherheitsanforderungen muss die geforderten Eigenschaften jedes Teilsystems durch Angabe von Informationen beschreiben, die eine richtige Auswahl der Ausrüstung erlaubt. Die Anforderungen zu den folgenden softwarebasierenden SRCFs müssen spezifiziert werden:

– die Logik (d. h. die Funktionalität) aller zu jedem Teilsystem zugewiesenen Funktionsblöcke;
– zu jedem Funktionsblock zugewiesene Eingabe- und Ausgabeschnittstellen;
– Format und Wertebereiche von Eingabe- und Ausgabedaten und ihre Beziehung zu Funktionsblöcken;
– relevante Daten zur Beschreibung irgendwelcher Grenzen jedes Funktionsblocks, zum Beispiel maximale Reaktionszeit, Grenzwerte für Plausibilitätsprüfungen;
– Diagnosefunktionen anderer Geräte innerhalb des SRECS (z. B. Sensoren und Stellglieder), die durch das Teilsystem auszuführen sind;
– Funktionen, die es der Maschine ermöglichen, einen sicheren Zustand zu erreichen oder aufrechtzuerhalten;
– Funktionen bezüglich der Erkennung, Meldung und Behandlung von Fehlern;
– Funktionen bezüglich periodischer Tests von SRCFs während des Betriebs und Off-Line;
– Funktionen, die unbefugte Modifikationen des SRECS verhindern;
– Schnittstellen zu Nicht-SRCFs und
– Kapazität und Leistungsfähigkeit in Bezug auf Reaktionszeit.

ANMERKUNG Schnittstellen umfassen sowohl während des Betriebs verwendete als auch Off-Line-Programmiereinrichtungen.

6.10.2.7 Wo angemessen, müssen in der Dokumentation semi-formale Methoden wie Logik-, Funktionsblock- oder Ablaufdiagramme verwendet werden.

ANMERKUNG Hinweise zur Softwaredokumentation sind in IEC 61506, ISO/IEC 15910 und ISO/IEC 9254 angegeben.

6.11 Software-Entwurf und Entwicklung

6.11.1 Entwurf und Entwicklung von Embedded-Software

In Teilsystemen enthaltene Embedded-Software muss IEC 61508-3, passend zu dem erforderlichen SIL, entsprechen.

ANMERKUNG 1 Siehe auch 6.7.3.2.

ANMERKUNG 2 Anhang C ist dazu vorgesehen, bei Entwurf und Entwicklung von Embedded-Software, die dazu verwendet wird, SRCFs innerhalb eines SRECS auszuführen, Unterstützung zu liefern.

6.11.2 Softwarebasierende Parametrisierung

6.11.2.1 Softwarebasierende Parametrisierung sicherheitsbezogener Parameter muss als ein sicherheitsbezogener Aspekt des SRECS-Entwurfs betrachtet werden, der in der Spezifikation der Software-Sicherheitsanforderungen (siehe 6.10) beschrieben wird. Parametrisierung muss unter Verwendung eines zugehörigen Werkzeugs ausgeführt werden, das vom Lieferanten des SRECS oder des (der) zugehörigen Teilsystems (Teilsysteme) bereitgestellt wird. Dieses Tool muss eine eigene Kennzeichnung besitzen (Name, Version usw.). Das Parametrisierungswerkzeug muss unbefugte Modifikation verhindern, zum Beispiel durch Verwendung eines Passwortes.

6.11.2.2 Die Integrität aller für die Parametrisierung verwendeten Daten muss aufrechterhalten werden. Dies muss durch Anwendung von Maßnahmen zu Folgendem erreicht werden:

– Kontrolle des Bereiches gültiger Eingaben;
– Beherrschung von Datenverfälschung vor der Datenübertragung;
– Beherrschung der Auswirkungen von Fehlern durch den Parameterübertragungsprozess;
– Beherrschung der Auswirkungen von unvollständiger Parameterübertragung und
– Beherrschung der Auswirkungen von Fehlern und Ausfällen der Hardware und Software des für die Parametrisierung verwendeten Werkzeugs.

6.11.2.3 Das für die Parametrisierung verwendete Werkzeug muss die folgenden Anforderungen erfüllen:

– alle relevanten Anforderungen für ein Teilsystem nach dieser Norm, um eine korrekte Parametrisierung sicherzustellen, oder
– es muss ein besonderes Verfahren für die Einstellung der sicherheitsbezogenen Parameter verwendet werden. Dieses Verfahren muss die Bestätigung von Eingabeparametern für das SRECS einschließen, entweder durch:
  – Rückübertragung der modifizierten Parameter zum Parametrisierungswerkzeug oder
  – andere Maßnahmen zur Bestätigung der Integrität der Parameter;

  und nachfolgende Bestätigung (z. B. durch eine ausreichend geschulte Person und eine automatische Überprüfung durch ein Parametrisierungswerkzeug);

  ANMERKUNG Dies ist von besonderer Wichtigkeit, wo die Parametrisierung unter Verwendung eines Gerätes ausgeführt wird, das nicht speziell für diesen Zweck vorgesehen ist (z. B. PC oder Ähnliches).
– die Softwaremodule, die für Codierung/Decodierung innerhalb des Übertragungs-/Rückübertragungsprozesses verwendet werden, und Softwaremodule, die für die Anzeige von sicherheitsbezogenen Parametern für den Anwender verwendet werden, müssen mindestens Diversität für die Funktion(en) verwenden, um systematische Ausfälle zu verhindern.

6.11.2.4 Die Dokumentation einer softwarebasierenden Parametrisierung muss die verwendeten Daten (z. B. vordefinierte Parametersätze) und notwendige Informationen zur Identifikation der dem SRECS zugeordneten Parameter, der Person(en), die die Parametrisierung ausgeführt hat (haben), zusammen mit anderen relevanten Informationen wie Datum der Parametrisierung aufzeigen.

6.11.2.5 Die folgenden Verifikationsaktivitäten müssen für eine softwarebasierende Parametrisierung angewendet werden:

– Verifikation der korrekten Einstellung für jeden sicherheitsbezogenen Parameter (Minimal-, Maximal- und repräsentative Werte);

– Verifikation, dass die sicherheitsbezogenen Parameter auf Plausibilität überprüft werden, zum Beispiel durch Aufdeckung ungültiger Werte usw.;

– Verifikation, dass unbefugte Modifikation von sicherheitsbezogenen Parametern verhindert ist;

– Verifikation, dass die Daten/Signale einer Parametrisierung so erzeugt und verarbeitet werden, dass Fehler nicht zu einem Verlust der SRCF(s) führen können.

ANMERKUNG Dies ist von besonderer Wichtigkeit, wo die Parametrisierung unter Verwendung eines Gerätes ausgeführt wird, das nicht speziell für diesen Zweck vorgesehen ist (z. B. Personalcomputer oder Ähnliches).

6.11.3 Entwurf und Entwicklung von Anwendungssoftware

ANMERKUNG Dieser Unterabschnitt basiert auf IEC 61508-3.

6.11.3.1 Allgemeine Anforderungen

6.11.3.1.1 Die Anforderungen von IEC 61508-3 treffen auf Programmiersprachen mit uneingeschränktem Sprachumfang (FVL) zu. Die nachfolgenden Anforderungen müssen für Anwendungssoftware, die auf einer Programmiersprache mit eingeschränktem Sprachumfang (LVL) beruht, angewendet werden.

6.11.3.1.2 Die Ergebnisse der während der Entwicklung der Anwendungssoftware ausgeführten Aktivitäten müssen an angemessenen Entwicklungsstufen verifiziert werden.

6.11.3.1.3 Die zur Erfüllung des erforderlichen SIL der SRCF gewählte Entwurfsmethode und Programmiersprache müssen für die Anwendung relevante Merkmale enthalten, die Folgendes erleichtern:

a) Abstraktion, Modularität und andere Merkmale, die die Komplexität begrenzen; wo immer möglich muss die Software auf bewährten Logikfunktionen, die Anwenderbibliotheksfunktionen einschließen können, und präzise festgelegten Regeln für das Linken von Logikfunktionen basieren;

b) Ausdruck von:
   – Funktionalität, idealerweise als eine logische Beschreibung oder als algorithmische Funktionen;
   – Informationsfluss zwischen modularen Elementen;
   – Reihenfolge und zeitbezogenen Anforderungen;
   – zeitlichen Einschränkungen;
   – Datenstrukturen und ihren Eigenschaften, einschließlich Datentypen, Gültigkeit von Datenbereichen;

c) Verstehen durch Entwickler und andere, die den Entwurf verstehen müssen, sowohl von einem funktionalen Verständnis der Anwendung her als auch von einem Wissen um die Einschränkungen der SRECS-Technologie;

d) Verifikation und Validierung, einschließlich struktureller Tests (White-Box) der Anwendungssoftware, funktionaler Tests (Black-Box) des integrierten Anwendungsprogramms und Schnittstellentests (Grey-Box) der Wechselwirkung mit dem SRECS und seiner anwendungsspezifischen Hardwarekonfiguration;

e) sichere Modifikation.

6.11.3.1.4 Testen muss die für die Anwendungssoftware hauptsächlich verwendete Verifikationsmethode sein. Die Testplanung muss Folgendes betrachten:

– die Grundsätze für die Verifikation der Integration von Software und Hardware;

– Testfälle und Testergebnisse;

– Arten der auszuführenden Tests;

– Testeinrichtungen einschließlich Werkzeuge, Software zur Unterstützung und eine Beschreibung der Konfiguration;

– Testkriterien, nach denen die Vollständigkeit der Tests beurteilt werden muss;
– physikalischer Platz bzw. physikalische Plätze (z. B. Fabrik oder Standort);
– Abhängigkeit von externer Funktionalität;
– Umfang der erforderlichen Testfälle und
– Vollständigkeit im Hinblick auf die in Bezug stehenden Funktionen und Anforderungen.

6.11.3.1.5 Wenn die Anwendungssoftware sowohl nicht-sicherheitsgerichtete als auch sicherheitsgerichtete Steuerungsfunktionen enthält, muss die gesamte Anwendungssoftware als sicherheitsbezogen behandelt werden, sofern nicht ausreichende Unabhängigkeit zwischen diesen Funktionen im Entwurf aufgezeigt werden kann.

6.11.3.1.6 Der Entwurf muss Überprüfungen der Datenintegrität und vernünftige Überprüfungen auf der Anwendungsebene einschließen (z. B. Überprüfungen in Kommunikationsverbindungen, Grenzwertüberprüfungen für Eingangssensoren, Grenzwertüberprüfungen für Datenparameter).

6.11.3.1.7 Der Entwurf der Anwendungssoftware muss Eigenüberwachung des Kontrollflusses und des Datenflusses beinhalten, falls solche Funktionen nicht in der Embedded-Software enthalten sind. Bei Erkennung eines Ausfalls müssen angemessene Aktionen durchgeführt werden, um einen sicheren Zustand zu erreichen oder aufrechtzuerhalten.

6.11.3.1.8 Wenn bereits entwickelte Software-Bibliotheksfunktionen als Teil des Entwurfs verwendet werden sollen, muss ihre Eignung zur Einhaltung der Spezifikation der Anforderungen zur Softwaresicherheit begründet werden. Die Eignung muss auf dem Nachweis ordnungsgemäßen Betriebs in ähnlichen Anwendungen basieren, für die gezeigt wurde, dass sie ähnliche Funktionalität besitzen oder muss Gegenstand gleicher Verifikations- und Validierungsverfahren sein, wie sie für jede neu entwickelte sicherheitsbezogene Software erwartet würden. Einschränkungen aus der früheren Softwareumgebung (z. B. Betriebssystem und Abhängigkeiten des Compilers) müssen bewertet werden.

6.11.3.1.9 Alle Modifikationen oder Änderungen der Anwendungssoftware müssen Gegenstand einer Einflussanalyse sein, die alle betroffenen Softwaremodule und die notwendigen Reverifikationsaktivitäten identifiziert, um zu bestätigen, dass die Spezifikation der Software-Sicherheitsanforderungen immer noch erfüllt wird.

6.11.3.2 Software-Konfigurationsmanagement

6.11.3.2.1 Der Plan der funktionalen Sicherheit muss die Strategie für die Entwicklung, Integration, Verifikation und Validierung der Software definieren.

6.11.3.2.2 Das Software-Konfigurationsmanagement muss:

– sicherstellen, dass alle notwendigen Tätigkeiten durchgeführt wurden, um aufzuzeigen, dass die erforderliche Sicherheitsintegrität der Software erreicht wurde;
– genau und mit einzigartiger Kennzeichnung alle Dokumente zu Einzelheiten der Konfiguration behandeln, die notwendig sind, um die Integrität des SRECS zu erhalten. Die Einzelheiten der Konfiguration müssen mindestens Folgendes umfassen:
  – Sicherheitsanalyse und Sicherheitsanforderungen;
  – Spezifikation der Software und Entwurfsdokumente;
  – Software-Quellcodemodule;
  – Testpläne und Testergebnisse;
  – bereits existierende Softwaremodule und Softwarepakete, die in das SRECS integriert werden sollen;
  – alle Werkzeuge und Entwicklungsumgebungen, die verwendet werden, um die Software zu erstellen, zu testen oder irgendeine Arbeit an der Anwendungssoftware durchzuführen;

- Änderungskontrollverfahren anwenden, um:
  - unbefugte Modifikationen zu verhindern;
  - Modifikationsanforderungen zu dokumentieren;
  - Einflüsse der beabsichtigten Modifikationen zu analysieren und die Anforderung(en) zu genehmigen oder zurückzuweisen;
  - die Einzelheiten und die Bevollmächtigung zu allen genehmigten Modifikationen zu dokumentieren;
  - die Softwarekonfiguration an angemessenen Punkten in der Softwareentwicklung zu dokumentieren;
- folgende Informationen dokumentieren, um ein nachfolgendes Audit zu ermöglichen: Ausgabestatus, die Begründung für und Genehmigung aller Modifikationen und die Einzelheiten der Modifikation;
- die Version der Anwendungssoftware formal dokumentieren. Masterkopien der Software und die gesamte zugehörige Dokumentation müssen aufbewahrt werden, um Pflege und Modifikation während der Betriebslebensdauer der Softwareversion zu ermöglichen.

6.11.3.3 Anforderungen zur Softwarearchitektur

ANMERKUNG 1 Die Softwarearchitektur legt die wesentlichen Komponenten und Teilsysteme der Systemsoftware und der Anwendungssoftware fest, wie sie miteinander verbunden sind und wie die erforderlichen Eigenschaften erreicht werden sollten. Beispiele für Module der Anwendungssoftware umfassen Anwendungsfunktionen, die überall in der Maschine nachgebildet sind, Maschinen-Eingaben/Ausgaben, Komponenten für Überschreitung und Hemmung, Überprüfung der Gültigkeit von Daten und Überprüfung von Bereichen usw.

ANMERKUNG 2 Die Softwarearchitektur wird auch von der zugrunde liegenden Architektur des vom Lieferanten gelieferten Teilsystems beeinflusst.

6.11.3.3.1 Der Entwurf der Softwarearchitektur muss auf der erforderlichen Spezifikation der SRECS-Sicherheit innerhalb des Rahmens der Einschränkungen der Systemarchitektur des SRECS und des Entwurfs des Teilsystems basieren.

6.11.3.3.2 Der Entwurf der Softwarearchitektur muss:

a) eine umfassende Beschreibung der internen Struktur, des Betriebs des SRECS und seiner Komponenten vorsehen (siehe Anmerkung);

b) die Spezifikation aller identifizierten Softwarekomponenten und die Beschreibung von Verbindungen und Wechselwirkungen zwischen identifizierten Komponenten (Software und Hardware) einschließen;

c) den internen Aufbau und die Architektur aller identifizierten Komponenten, die nicht als Black-Box betrachtet werden, einschließen;

d) die Softwaremodule identifizieren, die im SRECS enthalten sind, aber nicht in irgendeinem sicherheitsbezogenen Betrieb verwendet werden.

ANMERKUNG Es ist von besonderer Wichtigkeit, dass die Dokumentation der Architektur aktuell und komplett in Bezug auf das SRECS ist.

6.11.3.3.3 Es muss eine Auswahl von Verfahren und Maßnahmen beschrieben und begründet werden, die während des Entwurfs der Anwendungssoftware notwendig sind, um die Spezifikation zu erfüllen. Diese Verfahren und Maßnahmen müssen auf die Sicherstellung der Vorhersehbarkeit des Verhaltens des SRECS zielen und müssen mit allen in der SRECS-Dokumentation identifizierten Einschränkungen konsistent sein.

6.11.3.3.4 Maßnahmen, die zur Aufrechterhaltung der Integrität aller Daten verwendet werden, müssen beschrieben und begründet werden. Solche Daten können Eingangs-Ausgangsdaten der Maschine, Kommunikationsdaten, Daten der Betriebsschnittstelle, Instandhaltungsdaten und interne Datenbankdaten umfassen.

6.11.3.4 Anforderungen zu Unterstützungswerkzeugen, Benutzeranleitung und Anwendungsprogrammiersprachen

6.11.3.4.1 Es muss ein geeigneter Satz von Werkzeugen, einschließlich Werkzeugen für Konfigurationsmanagement, Simulation und Prüfeinrichtungen ausgewählt werden. Die Verfügbarkeit geeigneter Werkzeuge (nicht notwendigerweise die Werkzeuge, die während der einleitenden Systementwicklung verwendet werden) zur Unterstützung relevanter Arbeiten während der Lebensdauer des SRECS muss betrachtet werden. Die Angemessenheit der Werkzeuge muss erläutert und dokumentiert werden.

ANMERKUNG Die Auswahl von Entwicklungswerkzeugen hängt vom Charakter der Aktivitäten der Softwareentwicklung, der Embedded-Software und der Softwarearchitektur ab. Eventuell können Werkzeuge zur Verifikation und Validierung wie Codeanalysatoren und Simulatoren erforderlich sein.

6.11.3.4.2 Wo immer notwendig, muss eine Sprachenteilmenge der Anwendungsprogrammiersprache definiert werden.

6.11.3.4.3 Anwendungssoftware muss unter Berücksichtigung der Einschränkungen und bekannter Schwächen, die in den Anwenderhandbüchern des SRECS und des (der) Teilsystems (Teilsysteme) enthalten sind, entworfen werden.

6.11.3.4.4 Die gewählte Anwendungsprogrammiersprache muss entweder:

– unter Verwendung eines Übersetzers/Compilers verarbeitet werden, der beurteilt werden muss, um seine Eignung für den Einsatz zu begründen;

– vollständig und eindeutig definiert sein oder auf eindeutige festgelegte Eigenschaften eingeschränkt worden sein;

– den Eigenschaften der Anwendung entsprechen;

ANMERKUNG Eine Eigenschaft der Anwendung verweist zum Beispiel auf irgendwelche Einschränkungen der Leistungsfähigkeit.

– Eigenschaften enthalten, die die Erkennung von Programmierfehlern erleichtern und

– Eigenschaften unterstützen, die zum Entwurfsverfahren passen;

oder die Mängel der verwendeten Programmiersprache müssen in der Beschreibung des Entwurfs der Software-Architektur dokumentiert werden, und die Eignung der Sprache muss einschließlich der zusätzlich erforderlichen Maßnahmen dargelegt werden, um die festgestellten Unzulänglichkeiten der Sprache zu berücksichtigen.

6.11.3.4.5 Die Verfahren zur Verwendung der Anwendungsprogrammiersprache müssen zufrieden stellende Konfigurationspraxis festlegen, unsichere allgemeine Sprachmerkmale verbieten (z. B. undefinierte Sprachmerkmale, unstrukturierte Entwürfe usw.), Überprüfungen beschreiben, um Fehler in der Konfiguration zu erkennen, und die Verfahren für die Dokumentation des Anwendungsprogramms beschreiben. Folgende Informationen müssen mindestens in der Dokumentation des Anwendungsprogramms enthalten sein:

a) juristische Person (z. B. Firma, Autor(en) usw.);

b) Beschreibung;

c) Rückführbarkeit auf die funktionalen Anforderungen der Anwendung;

d) Rückführbarkeit auf Standardbibliotheksfunktionen;

e) Eingaben und Ausgaben und

f) Konfigurationsmanagement.

6.11.3.5 Anforderungen zum Entwurf der Anwendungssoftware

6.11.3.5.1 Die folgenden Informationen müssen vor dem Beginn des detaillierten Entwurfs der Anwendungssoftware zur Verfügung stehen:

– die Spezifikation der Software-Sicherheitsanforderungen;
– die Beschreibung des Entwurfs der Softwarearchitektur einschließlich der Identifizierung der Anwendungslogik und der Funktionalität der Fehlertoleranz, eine Liste von Eingangs- und Ausgangsdaten, die zu verwendenden allgemeinen Softwaremodule und Unterstützungswerkzeuge und die Verfahren zur Konfiguration der Anwendungssoftware mit den verfügbaren Materialien, um die Funktionalität der Anwendung für die definierten E/A zu ergeben und
– der Plan zur Validierung der Software bezüglich der Sicherheit.

6.11.3.5.2 Die Anwendungssoftware muss in einer strukturierten Art und Weise erstellt werden, um Folgendes zu erreichen:

– Modularität der Funktionalität der Anwendung und der E/A-Steuerungsdaten;
– Prüfbarkeit der Funktionalität (einschließlich Fehlertoleranzeigenschaften) und der internen Struktur;
– die Möglichkeit sicher ausgeführter Modifikation durch Bereitstellung einer angemessenen Rückführbarkeit und Erläuterung der Anwendungsfunktionen und verbundenen Einschränkungen.

6.11.3.5.3 Für jede Hauptkomponente/jedes Teilsystem in der Beschreibung des Entwurfs der Architektur der Anwendungssoftware (siehe 6.11.3.5.1) muss die weitere Verfeinerung des Entwurfs beruhen auf:

– Funktionen, die wiederholt im gesamten Entwurf verwendet werden;
– Abbildung der Eingangs-/Ausgangsinformationen von Modulen der Anwendungssoftware;
– Realisierung der Anwendungsfunktionen aus den allgemeinen Softwarefunktionen und der E/A-Abbildung.

6.11.3.5.4 Der Entwurf jedes Moduls der Anwendungssoftware und die auf jedes Modul der Anwendungssoftware anzuwendenden strukturellen Tests müssen spezifiziert werden.

6.11.3.5.5 Es müssen angemessene Software- und SRECS-Integrationstests spezifiziert werden, um sicherzustellen, dass das Anwendungsprogramm die spezifizierten Anforderungen für die Sicherheit der Anwendungssoftware erfüllt. Folgendes muss berücksichtigt werden:

– die Aufteilung der Anwendungssoftware in handhabbare Integrationseinheiten;
– Testfälle;
– Arten der auszuführenden Tests;
– Testumgebung, Werkzeuge, Konfiguration und Programme;
– Testkriterien, nach denen die Vollständigkeit der Tests beurteilt werden muss und
– Verfahren für Korrekturen bei Ausfall eines Tests.

6.11.3.6 Anforderungen zur Entwicklung des Anwendungscodes

6.11.3.6.1 Die Anwendungssoftware muss:

– lesbar, verständlich und prüfbar sein;
– die relevanten Entwurfsverfahren erfüllen;
– die relevanten Anforderungen, die während der Sicherheitsplanung spezifiziert worden sind, erfüllen.

6.11.3.6.2 Die Anwendungssoftware muss überprüft werden, um Übereinstimmung mit dem spezifizierten Entwurf, den Codierrichtlinien und den Anforderungen der Sicherheitsplanung sicherzustellen.

ANMERKUNG Die Überprüfung der Anwendungssoftware schließt Verfahren wie Inspektionen der Software oder Walkthroughs, Codeanalyse oder mathematischen Beweis ein. Diese Verfahren sollten in Verbindung mit Tests und/oder Simulation verwendet werden, um Sicherheit zu gewährleisten, dass die Anwendungssoftware ihre zugehörige Spezifikation erfüllt.

6.11.3.7 Anforderungen zum Test der Anwendungsmodule

ANMERKUNG Der Test, dass die Anwendungssoftware korrekt ihre Testspezifikation erfüllt, ist eine Verifikationsaktivität. Es ist die Kombination von Code-Überprüfung und strukturellem Testen, die die Sicherheit ergibt, dass ein Modul der Anwendungssoftware seine zugehörige Spezifikation erfüllt, d. h. dass es verifiziert ist.

6.11.3.7.1 Die Konfiguration jedes Eingangs- und Ausgangspunktes muss durch Überprüfung, Test oder Simulation überprüft werden, um zu bestätigen, dass die E/A-Daten auf die korrekte Anwendungslogik abgebildet werden.

6.11.3.7.2 Jedes Softwaremodul muss durch einen Prozess von Überprüfung, Simulation und Test überprüft werden, um zu bestimmen, dass die beabsichtigte Funktion korrekt ausgeführt wird und keine unbeabsichtigten Funktionen ausgeführt werden.

6.11.3.7.3 Die Tests müssen für das spezifische, dem Test unterworfenen Modul angemessen sein und müssen:

– sicherstellen, dass jede Verzweigung aller Module der Anwendungssoftware ausgeführt wird;

– sicherstellen, dass Grenzdaten angewendet werden;

– sicherstellen, dass Abläufe korrekt implementiert sind, einschließlich relevanter Synchronisationsbedingungen.

6.11.3.7.4 Die Ergebnisse des Tests der Module der Anwendungssoftware müssen dokumentiert werden.

6.11.3.7.5 Wenn Software bereits beurteilt wurde oder wenn eine umfangreiche Anzahl positiver Betriebserfahrungen vorhanden ist, kann der Umfang der Tests reduziert werden.

6.11.3.8 Anforderungen zum Integrationstest der Anwendungssoftware

ANMERKUNG Der Test, dass die Software korrekt integriert wurde, ist eine Verifikationsaktivität.

6.11.3.8.1 Die Tests der Anwendungssoftware müssen überprüfen, dass alle Module der Anwendungssoftware und Komponenten/Teilsysteme korrekt miteinander und mit der zugrunde liegenden Embedded-Software zusammenwirken, um ihre beabsichtigten Funktionen auszuführen und nicht unbeabsichtigte Funktionen ausführen, die irgendeine Sicherheitsfunktion gefährden könnten.

6.11.3.8.2 Die Ergebnisse des Integrationstests der Anwendungssoftware müssen dokumentiert werden, und es müssen Angaben gemacht werden:

– zu den Testergebnissen und

– ob die Ziele der Testkriterien erfüllt worden sind.

6.11.3.8.3 Wenn ein Ausfall vorliegt, müssen die Gründe für den Ausfall und die ergriffenen Korrekturen in der Dokumentation der Testergebnisse enthalten sein.

6.11.3.8.4 Während der Integration der Anwendungssoftware muss jede Modifikation oder Änderung der Software Gegenstand einer Sicherheitseinflussanalyse sein, die Folgendes festlegen muss:

– alle betroffenen Softwaremodule und

– alle notwendigen Aktivitäten in Bezug auf Reverifikation und Erneuerung des Entwurfs.

6.12 Integration und Test des sicherheitsbezogenen elektrischen Steuerungssystems

ANMERKUNG Die Integration des SRECS wird üblicherweise vor der Installation ausgeführt, jedoch kann die Integration des SRECS in einigen Fällen nicht vor Beendigung der Installation ausgeführt werden (zum Beispiel, wenn die Entwicklung der Anwendungssoftware nicht vor Beendigung der Installation beendet ist).

6.12.1 Allgemeine Anforderungen

6.12.1.1 Das SRECS muss gemäß dem festgelegten SRECS-Entwurf integriert werden. Als Teil der Integration aller Teilsysteme und Teilsystem-Elemente in das SRECS muss das SRECS gemäß den festgelegten Integrationstests getestet werden. Diese Tests müssen überprüfen, dass alle Module korrekt zusammenwirken, um ihre beabsichtigte Funktion auszuführen und nicht unbeabsichtigte Funktionen ausführen.

6.12.1.2 Die Integration der sicherheitsbezogenen Anwendungssoftware in das SRECS muss Tests einschließen, die während der Entwurfs- und Entwicklungsphase festgelegt worden sind, um die Kompatibilität der Anwendungssoftware mit der Hardware und der Embedded-Software-Plattform sicherzustellen, so dass die Anforderungen zur funktionalen und zur sicherheitsbezogenen Leistungsfähigkeit eingehalten werden.

ANMERKUNG 1 Dies bedeutet nicht das Testen aller Eingangskombinationen. Das Testen aller Äquivalenzklassen (siehe IEC 61508-7, B.5 und C.5.7) kann ausreichend sein. Statische Analyse, dynamische Analyse oder Ausfallanalyse können die Zahl der Testfälle auf ein akzeptables Maß reduzieren. Die Anwendung eines strukturierten Entwurfs oder semi-formaler Methoden kann Tests und Verifikation erleichtern.

ANMERKUNG 2 Die Anwendung eines strukturierten Entwurfs oder semi-formaler Methoden kann eine reduzierte Tiefe und Anzahl von Testfällen erlauben.

ANMERKUNG 3 Statistische Beweise können ebenso verwendet werden, um eine reduzierte Tiefe und Anzahl von Testfällen zu erlauben.

6.12.1.3 Es muss eine angemessene Dokumentation der Integrationstests des SRECS erstellt werden, die die Testergebnisse enthält und aussagt, ob die Ziele und Kriterien, die während der Entwurfs- und Entwicklungsphase festgelegt wurden, erreicht bzw. eingehalten worden sind. Falls es einen Ausfall gibt, müssen die Gründe für den Ausfall dokumentiert werden, Korrekturen ergriffen werden, und es muss ein erneuter Test durchgeführt werden.

6.12.1.4 Während der Integration und der Tests müssen alle Modifikationen oder Änderungen an dem SRECS Gegenstand einer Einflussanalyse sein, die alle betroffenen Komponenten und die zusätzliche Verifikation identifizieren muss.

6.12.1.5 Während der SRECS-Integrationstests muss Folgendes dokumentiert werden:

a) die Version der verwendeten Testspezifikation;

b) die Kriterien für Akzeptanz der Integrationstests;

c) die Version des getesteten SRECS;

d) die verwendeten Werkzeuge und Einrichtungen mit Kalibrierdaten;

e) die Ergebnisse aller Tests;

f) alle Widersprüche zwischen erwarteten und tatsächlichen Ergebnissen;

g) die ausgeführte Analyse und die getroffenen Entscheidungen, ob die Prüfung fortgesetzt oder eine Änderungsanforderung eingeleitet wird, im Falle, dass Widersprüche auftreten.

6.12.2 Tests zur Feststellung der systematischen Sicherheitsintegrität während der Integration des SRECS

6.12.2.1 Zur Aufdeckung von Fehlern, und zur Vermeidung von Ausfällen während der Integration der Anwendungssoftware und Hardware müssen Tests angewendet werden. Während der Tests müssen Überprüfungen ausgeführt werden, um zu klären, ob die festgelegten Eigenschaften des SRECS erreicht worden sind.

6.12.2.2 Die folgenden Tests müssen angewendet werden:

a) funktionale Tests, bei denen dem SRECS Daten, die den Betrieb angemessen charakterisieren, übergeben werden. Die Ausgaben müssen beobachtet werden, und ihre Reaktion wird mit der in der Spezifikation angegebenen Reaktion verglichen. Abweichungen von der Spezifikation und Anzeichen einer unvollständigen Spezifikation müssen dokumentiert werden und

b) dynamische Tests zur Verifikation des dynamischen Verhaltens unter realistischen funktionalen Bedingungen und zur Aufdeckung von Ausfällen bei der Erfüllung der funktionalen Spezifikation des SRECS sowie zur Beurteilung der Brauchbarkeit und Robustheit des SRECS.

ANMERKUNG Die Funktionen eines Systems oder Programms werden in einer festgelegten Umgebung mit festgelegten Testdaten ausgeführt, die systematisch aus der Spezifikation der SRECS-Sicherheitsanforderungen gemäß festgelegten Kriterien abgeleitet werden. Dies zeigt das Systemverhalten des SRECS auf und lässt einen Vergleich mit der Spezifikation zu. Es ist Ziel, zu bestimmen, ob das SRECS und/oder seine Teilsysteme alle in der Spezifikation geforderten Funktionen korrekt ausführen. Das Verfahren der Bildung von Äquivalenzklassen ist ein Beispiel eines Kriteriums für Black-Box-Testdaten. Der Eingabedatenraum wird anhand der Spezifikation in spezielle Eingangswertebereiche (Äquivalenzklassen) unterteilt. Testfälle werden dann wie folgt gebildet:

– Daten aus zulässigen Bereichen;

– Daten aus unzulässigen Bereichen;

– Daten aus den Bereichsgrenzen;

– Extremwerte;

– und Kombinationen dieser Klassen.

Andere Kriterien können wirksam sein, um Testfälle während der verschiedenen Testaktivitäten (Modultest, Integrationstest und Systemtest) auszuwählen.

6.13 Installation des SRECS

6.13.1 Ziel

Die Ziele der Anforderungen dieses Unterabschnitts sind für die Installation eines SRECS sicherzustellen, dass es für seine vorgesehene Verwendung geeignet ist und dass es für die Validierung bereit ist.

6.13.2 Anforderungen

6.13.2.1 Ein SRECS muss in Übereinstimmung mit dem Plan der funktionalen Sicherheit für die endgültige Systemvalidierung (siehe Punkt h) von 4.2.1) installiert werden.

6.13.2.2 Es müssen geeignete Aufzeichnungen der Installation des SRECS erstellt werden, die alle Testergebnisse enthalten. Falls ein Ausfall vorliegt, müssen die Gründe für den Ausfall festgehalten werden.

7 Benutzerinformationen des SRECS

7.1 Ziel

Es müssen Informationen zum SRECS geliefert werden, um es dem Anwender zu ermöglichen, Verfahren zu entwickeln, um sicherzustellen, dass die erforderliche funktionale Sicherheit des SRECS während des Gebrauchs und der Instandhaltung der Maschine erhalten bleibt.

7.2 Dokumentation für Installation, Gebrauch und Instandhaltung

ANMERKUNG 1 Siehe auch Abschnitt 6 von ISO 12100-2, in dem allgemeine Informationen enthalten sind, die bei der Erstellung der Begleitdokumente beachtet werden sollten.

ANMERKUNG 2 Ein oder mehrere Punkte der in diesem Unterabschnitt beschriebenen Dokumentation könnten aufgeführt worden sein, um anderen Aspekten dieser Norm zu genügen.

Die Dokumentation muss Informationen für Installation, Gebrauch und Instandhaltung des SRECS bereitstellen. Dies muss einschließen:

a) eine umfassende Beschreibung der Einrichtung, Installation und Montage;

b) eine Erklärung zur vorgesehenen Verwendung des SRECS und alle Maßnahmen, die notwendig sein können, um vernünftigerweise vorhersehbare Fehlanwendung zu verhindern;

c) Informationen zur physikalischen Umgebung (z. B. Beleuchtung, Vibration, Geräuschpegel, atmosphärische Verunreinigungen), wo angemessen;

d) Übersichts(block)diagramm(e), wo angemessen;

e) Stromlaufplan (Stromlaufpläne);

f) Intervall des Proof-Tests oder Gebrauchsdauer;

g) eine Beschreibung (einschließlich Diagramme gegenseitiger Verbindungen) des Zusammenwirkens (falls vorhanden) zwischen der (den) SRECS-Funktion(en) und der (den) Funktion(en) des elektrischen Maschinensteuerungssystems;

h) eine Beschreibung der notwendigen Maßnahmen zur Sicherstellung der Trennung der SRECS-Funktion(en) von der (den) Funktion(en) des elektrischen Maschinensteuerungssystems;

i) eine Beschreibung des Schutzes und der vorhandenen Mittel zur Aufrechterhaltung der Sicherheit, wo es notwendig ist, das (die) SRCF(s) auszusetzen (z. B. für manuelle Programmierung, Programmverifikation);

j) Informationen zur Programmierung, wo zutreffend;

k) Beschreibung der auf das SRECS anwendbaren Anforderungen zur Instandhaltung, einschließlich:

   1) einem Logbuch für die Aufzeichnung der Instandhaltungshistorie der Maschine;

   2) die Routineaktionen, die durchgeführt werden müssen, um die funktionale Sicherheit des SRECS zu erhalten, einschließlich des routinemäßigen Ersatzes von Bauteilen mit vordefinierter Gebrauchsdauer;

   3) der zu befolgenden Instandhaltungsverfahren bei Auftreten von Fehlern oder Ausfällen in dem SRECS, einschließlich:

      – Verfahren zur Fehlerdiagnose und Reparatur;

      – Verfahren zur Bestätigung des korrekten Betriebs nach Reparaturen;

      – Anforderungen zu Instandhaltungsaufzeichnungen;

   4) der für Instandhaltung und Wiederinbetriebnahme notwendigen Werkzeuge und der Verfahren zum Erhalt der Werkzeuge und Einrichtungen;

   5) einer Festlegung für regelmäßige Prüfungen, Instandhaltung zur Korrektur und korrigierende Instandhaltung.

ANMERKUNG 3 Regelmäßige Prüfungen sind diejenigen funktionalen Tests, die notwendig sind, um den korrekten Betrieb zu bestätigen und Fehler zu erkennen.

ANMERKUNG 4 Vorbeugende Instandhaltung sind die Maßnahmen, die ergriffen werden, um die erforderliche Leistungsfähigkeit des SRECS zu erhalten.

ANMERKUNG 5 Korrigierende Instandhaltung schließt die Maßnahmen ein, die ergriffen werden, um das SRECS nach dem Auftreten bestimmter Fehler wieder in den Zustand wie beim Entwurf zurückzubringen.

8 Validierung des sicherheitsbezogenen elektrischen Steuerungssystems

ANMERKUNG Validierung des SRECS kann einen Teil der Validierungsaktivitäten bilden, die auf den Gesamtentwurf der Maschine angewendet werden.

8.1 Ziel

Dieser Abschnitt legt die Anforderungen für den Validierungsprozess fest, der auf das SRECS anzuwenden ist. Dies schließt Inspektion und Prüfung des SRECS ein, um sicherzustellen, dass es die in der Spezifikation der Sicherheitsanforderungen festgelegten Anforderungen erreicht.

8.2 Allgemeine Anforderungen

8.2.1 Die Validierung des SRECS muss in Übereinstimmung mit einem vorbereiteten Plan ausgeführt werden (siehe 4.2).

ANMERKUNG 1 In einigen Fällen kann die Validierung bezüglich der Sicherheit nicht vor dem Ende der Installation abgeschlossen werden (zum Beispiel, wenn die Entwicklung der Anwendungssoftware nicht vor der Installation abgeschlossen wurde).

ANMERKUNG 2 Die Validierung eines programmierbaren SRECS beinhaltet die Validierung sowohl der Hardware als auch der Software. Die Anforderungen für die Validierung von Software sind in 6.11.3 enthalten.

8.2.2 Jede SRCF, die in der SRECS-Anforderungsspezifikation (siehe 5.2) spezifiziert ist, und alle SRECS-Betriebs- und Instandhaltungsverfahren müssen durch Test und/oder Analyse validiert werden.

8.2.3 Es muss eine angemessene Dokumentation der Tests zur Validierung des SRECS bezüglich der Sicherheit erstellt werden, die für jede SRCF Folgendes darlegen muss:

a) die Version des verwendeten Plans zur Validierung des SRECS bezüglich der Sicherheit und die Version des getesteten SRECS;

b) die geprüfte (oder analysierte) SRCF zusammen mit dem spezifischen Bezug zu der während der Planung der Validierung des SRECS bezüglich der Sicherheit festgelegten Anforderung;

c) die verwendeten Werkzeuge und Einrichtungen zusammen mit Kalibrierdaten;

d) die Ergebnisse jedes Tests;

e) Widersprüche zwischen erwarteten und tatsächlichen Ergebnissen.

8.2.4 Wenn Widersprüche auftreten, müssen Korrekturen und Nachprüfungen, soweit erforderlich, durchgeführt und dokumentiert werden.

8.3 Validierung der systematischen Sicherheitsintegrität des SRECS

8.3.1 Folgendes muss angewendet werden:

a) zur Aufdeckung von Ausfällen während der Phasen der Spezifikation, des Entwurfs und der Integration und zur Vermeidung von Ausfällen während der Validierung der Software und Hardware des SRECS müssen Funktionstests angewendet werden. Dieses muss Verifikation (z. B. durch Inspektion oder Test) zur Beurteilung einschließen, ob das SRECS gegen widrige umweltbedingte Einflüsse geschützt ist und muss auf der Spezifikation der Sicherheitsanforderungen basieren;

ANMERKUNG 1 Siehe auch 6.12.2.1.

b) Prüfung der Störfestigkeit, um sicherzustellen, dass das SRECS imstande ist, 5.2.3 zu erfüllen. Die Prüfung der Störfestigkeit in Bezug auf elektromagnetische Beeinflussung von SRECS-Teilsystemen oder Teilsystem-Elementen muss nicht durchgeführt werden, wenn eine ausreichende Störfestigkeit des SRECS für seine vorgesehene Anwendung durch Analyse demonstriert werden kann;

ANMERKUNG 2 Das SRECS sollte, wann immer möglich, mit einem typischen Anwendungsprogramm geladen werden und alle peripheren Leitungen (alle digitalen, analogen und seriellen Schnittstellen, wie auch die Busverbindungen und Energieversorgung usw.) werden genormten Störsignalen ausgesetzt. Um eine quantitative Aussage zu erhalten, ist es vernünftig, sich allen Grenzen vorsichtig anzunähern.

c) wenn der erforderliche Anteil sicherer Ausfälle ≥ 90 % beträgt, müssen Tests durch Fehlereinbau ausgeführt werden. Diese Tests müssen Fehler in die SRECS-Hardware einbringen oder simulieren und die Reaktion muss dokumentiert werden.

8.3.2 Zusätzlich müssen eine oder mehrere der folgenden Gruppen analytischer Verfahren unter Berücksichtigung der Komplexität des SRECS und des zugewiesenen SIL angewendet werden:

a) statische Analyse und Ausfallanalyse;

ANMERKUNG 1 Diese Kombination von analytischen Verfahren wird nur für SRECS als angemessen betrachtet, die SRCFs mit einem zugewiesenen SIL ausführen, der SIL 2 nicht übersteigt.

ANMERKUNG 2 Weitere Informationen sind in IEC 61508-7, B.6.4 und B.6.6 vorhanden.

b) statische Analyse, dynamische Analyse und Ausfallanalyse;

ANMERKUNG 3 Diese Kombination von analytischen Verfahren wird nicht empfohlen für SRECS, die SRCFs mit einem zugewiesenen SIL unterhalb von SIL 2 ausführen.

ANMERKUNG 4 Weitere Informationen sind in IEC 61508-7, B.6.4, B.6.5 und B.6.6. vorhanden.

c) Simulation und Ausfallanalyse.

ANMERKUNG 5 Diese Kombination von analytischen Verfahren wird nur für SRECS als angemessen betrachtet, die SRCFs mit einem zugewiesenen SIL ausführen, der SIL 2 nicht übersteigt.

ANMERKUNG 6 Weitere Informationen sind in IEC 61508-7, B.3.6 und B.6.6. vorhanden.

8.3.3 Zusätzlich müssen eine oder mehrere der folgenden Gruppen testender Verfahren unter Berücksichtigung der Komplexität des SRECS und dem zugewiesenen SIL angewendet werden:

a) Black-Box-Test: ein Test bzw. Tests des dynamischen Verhaltens unter realen funktionalen Bedingungen zur Aufdeckung von Ausfällen bei der Erfüllung der funktionalen Spezifikation des SRECS und zur Beurteilung der Brauchbarkeit und Robustheit des SRECS;

ANMERKUNG 1 Siehe auch 6.12.2.1.

b) wenn der erforderliche Anteil sicherer Ausfälle < 90 % beträgt, müssen Tests durch Fehlereinbau ausgeführt werden. Diese Tests müssen Fehler in die SRECS-Hardware einbringen oder simulieren, und die Ergebnisse müssen dokumentiert werden;

c) Der Test unter „Grenzbedingungen“ muss ausgeführt werden, um die durch Anwendung analytischer Verfahren (siehe 8.3.2) festgelegten Extremfälle (d. h. Grenzfälle) zu beurteilen;

ANMERKUNG 2 Die betriebliche Leistungsfähigkeit des SRECS und die Bauteildimensionierung wird unter Grenzbedingungen getestet. Die Umgebungsbedingungen werden auf ihre höchsten zulässigen Grenzwerte hin verändert. Die wesentlichsten Reaktionen des SRECS werden überprüft und mit der Spezifikation der Sicherheitsanforderungen verglichen.

d) Felderfahrung: die Verwendung von Felderfahrung aus verschiedenen Anwendungen als eine der Maßnahmen zur Vermeidung von Fehlern während der Validierung des SRECS.

ANMERKUNG 3 Siehe auch 6.12.2.

9 Modifikation

9.1 Ziel

Dieser Abschnitt legt das (die) Modifikationsverfahren fest, das (die) anzuwenden ist (sind), wenn das SRECS während Entwurf, Integration und Validierung (z. B. während der Installation und Inbetriebnahme) geändert wird.

9.2 Modifikationsverfahren

9.2.1 Die Anforderung für eine Modifikation des SRECS kann zum Beispiel herrühren von:

– geänderter Spezifikation der Sicherheitsanforderungen;
– Bedingungen der tatsächlichen Verwendung;
– Erfahrungen aus Zwischenfällen/Unfällen;
– Wechsel des bearbeiteten Materials;
– Modifikationen der Maschine oder ihrer Betriebsarten.

ANMERKUNG Eingriffe (z. B. Justage, Einrichten, Reparatur) an dem SRECS, die in Übereinstimmung mit den Benutzerinformationen oder der Gebrauchsanweisung des SRECS erfolgen, werden im Rahmen dieses Abschnitts nicht als Modifikation betrachtet.

9.2.2 Der Grund (Die Gründe) für eine Modifikation des SRECS muss (müssen) dokumentiert werden.

9.2.3 Die Auswirkung der vorgesehenen Modifikation muss analysiert werden, um die Auswirkung auf die funktionale Sicherheit des SRECS festzustellen.

9.2.4 Die Analyse der Einflüsse der Modifikation und die Auswirkung auf die funktionale Sicherheit des SRECS müssen dokumentiert werden.

9.2.5 Alle akzeptierten Modifikationen, die eine Auswirkung auf das SRECS haben, müssen eine Rückkehr zu einer angemessenen Entwurfsphase seiner Hardware und/oder seiner Software (z. B. Spezifikation, Entwurf, Integration, Installation, Inbetriebnahme und Validierung) einleiten. Alle nachfolgenden Phasen müssen dann in Übereinstimmung mit den für die spezifischen Phasen festgelegten Verfahren dieser Norm durchgeführt werden. Alle betroffenen Dokumente müssen überarbeitet, geändert und neu herausgegeben werden.

9.2.6 Bevor irgendeine Modifikation umgesetzt wird, muss ein auf den überarbeiteten Dokumenten basierender vollständiger Aktionsplan erstellt und dokumentiert werden.

9.3 Konfigurationsmanagementverfahren

9.3.1 Die Konfigurationsmanagementverfahren müssen in Übereinstimmung mit dem Plan der funktionalen Sicherheit (siehe 4.2.1) unter Berücksichtigung von Folgendem ausgeführt werden:

a) einem Plan jedes Modifikationsprozesses;
b) einer Dokumentation des Entscheidungsprozesses und jeder SRECS-relevanten Entscheidung;
c) einer chronologischen Dokumentation (z. B. ein Logbuch) der Verfahren zur Änderungsanforderung einschließlich:
   – identifizierter Gefährdungen, die beeinflusst werden können;
   – Beschreibung der Änderungsanforderung (Hardware und/oder Software);
   – Grund (Gründe) für die Änderungsanforderung (siehe auch 9.2.1);
   – erfolgte Entscheidung (und Autorisierung für jede Entscheidung);
   – der Einflussanalyse;
   – Reverifikation (jeder Phase) und Revalidierung;
   – aller Dokumente, die durch die Aktivitäten der Änderungsanforderung betroffen sind;
   – aller Aktivitäten, die während des Änderungsprozesses ausgeführt wurden und der Personen/Einheiten, die für sie verantwortlich waren;

d) Dokumentation der folgenden Informationen, um ein nachfolgendes Audit zu erlauben:
   - Konfigurationsstatus;
   - Freigabestatus;
   - die Begründung für und Genehmigung von allen Modifikationen;
   - die Einzelheiten der Modifikation.

9.3.2 Die Verfahren für einen angemessenen Änderungskontrollprozess sollten die Anforderungen betrachten zu:

a) Verfahren zur Definition eines unverwechselbaren Standes jeder Version des SRECS;

b) Definition aller Konfigurationsbestandteile eines Standes. Dies muss zumindest einschließen:
   1) Analyse und Spezifikation der Sicherheitsanforderungen;
   2) relevante Entwurfsdokumente;
   3) Hardware- und/oder Softwaremodule;
   4) Testpläne und Ergebnisse;
   5) Verifikations- und Validierungsberichte;
   6) bereits vorhandene Softwarekomponenten, die in das SRECS einzugliedern sind;
   7) Werkzeuge und Entwicklungsumgebungen, die für Erstellung und Test zu verwenden sind;
   8) genaue Pflege mit unverwechselbarer Identifikation aller Konfigurationsbestandteile, die notwendig sind, um die Integrität des SRECS aufrechtzuerhalten;
   9) Änderungskontrollverfahren, um:
      - nicht autorisierte Modifikationen zu verhindern,
      - Änderungsanforderungen zu dokumentieren,
      - den Einfluss der beabsichtigten Änderungsanforderung zu analysieren und die Anforderung zu genehmigen oder zurückzuweisen,
      - die Einzelheiten und die Autorisierung für alle genehmigten Modifikationen zu dokumentieren,
      - einen Konstruktionsstand an angemessenen Punkten der Hardware- oder Softwareentwicklung zu errichten und die (teilweisen) Integrationsprüfungen, die den Stand rechtfertigen, zu dokumentieren,
      - die Zusammensetzung und die Erstellung aller Konstruktionsstände der Hardware oder Software (einschließlich der erneuten Zusammenstellung früherer Stände) zu garantieren;
   10) eine Analyse der Auswirkungen, die den Einfluss jeder Änderungsanforderung beurteilt. Diese Analyse muss auch eine angemessene Gefährdungsanalyse einschließen und muss alle anderen Modifikationsaktivitäten eines SRECS berücksichtigen;
   11) Rückkehr zu einer angemessenen Entwurfsphase der Hardware und/oder Software (z. B. Spezifikation, Entwurf, Integration, Installation, Inbetriebnahme und Validierung) des SRECS für alle akzeptierten Modifikationen, die einen Einfluss auf das SRECS haben. Alle nachfolgenden Phasen müssen dann in Übereinstimmung mit dieser Norm ausgeführt werden;
   12) Ausführung aller notwendigen Verfahren, um aufzuzeigen, dass die erforderliche Sicherheitsintegrität erreicht worden ist;
   13) die Autorisierung zur Ausführung der erforderlichen Aktivität zur Änderungsanforderung muss von den Ergebnissen der Einflussanalyse abhängen.

9.3.3 Die Dokumentation des Änderungskontrollprozesses muss mindestens enthalten:

a) einen Plan jedes Modifikationsprozesses;

b) eine Dokumentation zu jeder der oben aufgeführten organisatorischen Anforderungen und jedem Verfahren;

c) eine Dokumentation des Entscheidungsprozesses und jeder erfolgten SRECS-relevanten Entscheidung;

d) eine chronologische Dokumentation (Logbuch) der Verfahren zur Änderungsanforderung einschließlich:
   - identifizierter Gefährdungen, die beeinflusst werden können;
   - Beschreibung der Änderungsanforderung (Hardware und/oder Software);
   - Grund (Gründe) für die Änderungsanforderung (siehe auch 9.2.1);
   - erfolgter Entscheidung (und Autorisierung für jede Entscheidung);
   - der Einflussanalyse;
   - Reverifikation (jeder Phase) und Revalidierung;
   - aller Dokumente, die durch die Aktivitäten der Änderungsanforderung betroffen sind;
   - aller Aktivitäten, die während des Änderungsprozesses ausgeführt wurden und der Personen/Einheiten, die für sie verantwortlich waren;

e) Dokumentation der folgenden Informationen, um ein nachfolgendes Audit zu erlauben:
   - Konfigurationsstatus;
   - Freigabestatus;
   - die Begründung für und Genehmigung von allen Modifikationen;
   - die Einzelheiten der Modifikation.

10 Dokumentation

10.1 Die Dokumentation muss:

- genau und knapp sein;
- von denjenigen Personen, die sie verwenden müssen, einfach zu verstehen sein;
- den Zweck erfüllen, wofür sie erstellt worden ist;
- verfügbar und pflegbar sein.

10.2 Der Konstrukteur des SRECS sollte zwischen der Dokumentation, die für den Anwender wichtig ist, und derjenigen, die für seinen Entwurf und Konstruktion wichtig ist, unterscheiden.

10.3 Die Dokumente müssen Titel oder Namen tragen, die auf den Anwendungsbereich des Inhalts hinweisen.

10.4 Die Dokumente müssen einen Revisionsindex (Versionsnummern) tragen, um verschiedene Versionen des Dokuments identifizieren zu können.

ANMERKUNG Siehe auch IEC 82045-1:2001 für weitere Informationen zu Verfahren, die für das Management der Dokumentation verwendet werden können.

10.5 Tabelle 8 fasst die Informationen und die Dokumentation zusammen, die, wo angemessen, zur Verfügung stehen müssen.

Tabelle 8 – Informationen und Dokumentation eines SRECS

Erforderliche Informationen	Abschnitt
Plan der funktionalen Sicherheit	4.2.1
Spezifikation der Anforderungen für SRCFs	5.2
Spezifikation der funktionalen Sicherheitsanforderungen für SRCFs	5.2.3
Spezifikation der Anforderungen zur Sicherheitsintegrität für SRCFs	5.2.4
SRECS-Entwurf	6.2.5
Strukturierter Entwurfsprozess	6.6.1.2
Dokumentation des SRECS-Entwurfs	6.6.1.8
Struktur von Funktionsblöcken	6.6.2.1.1
SRECS-Architektur	6.6.2.1.5
Spezifikation der Sicherheitsanforderungen des Teilsystems	6.6.2.1.7
Realisierung des Teilsystems	6.7.2.2
Teilsystem-Architektur (Elemente und ihre Wechselbeziehungen)	6.7.4.3.1.2
In Anspruch genommene Fehlerausschlüsse bei der Abschätzung der Fehlertoleranz/SFF	6.7.6.1 c)/6.7.7.3
Teilsystemmontage	6.7.10
Spezifikation der Software-Sicherheitsanforderungen	6.10.1
Software basierende Parametrisierung	6.11.2.4
Einzelheiten zum Software-Konfigurationsmanagement	6.11.3.2.2
Angemessenheit der Softwareentwicklungswerkzeuge	6.11.3.4.1
Dokumentation des Anwendungsprogramms	6.11.3.4.5
Ergebnisse des Tests der Module der Anwendungssoftware	6.11.3.7.4
Ergebnisse der Integrationstests der Anwendungssoftware	6.11.3.8.2
Dokumentation der SRECS-Integrationstests	6.12.1.3
Dokumentation der Installation des SRECS	6.13.2.2
Dokumentation für Installation, Gebrauch und Instandhaltung	7.2
Dokumentation der Tests zur Validierung des SRECS	8.2.4
Dokumentation für SRECS-Konfigurationsmanagement	9.3.1

Anhang A
(informativ)

Festsetzung des SIL

A.1 Allgemeines

Dieser informative Anhang stellt ein Beispiel eines qualitativen Ansatzes zur Risikoabschätzung und Festsetzung des SIL bereit, der auf SRCFs für Maschinen angewendet werden kann. Beispiele anderer Verfahren, die für die Festsetzung des SIL verwendet werden können, sind in IEC 61508-5 angegeben und werden in einer vorgeschlagenen zukünftigen Technischen Spezifikation des IEC TC 44 skizziert.

ANMERKUNG 1 Die in diesem Anhang beschriebene Methodologie verwendet eine qualitative Abschätzung des Risikos und ist dazu vorgesehen, allgemein für die Festlegung eines (der) SIL(s) für SRCF(s) von Maschinen eingesetzt zu werden. Die bei der Anwendung dieser Methodologie verwendeten Risikoparameter (siehe Bild A.2) für einzelne Maschinen und ihre speziellen Gefährdungen sollten Gegenstand der Übereinstimmung unter den Beteiligten sein, um sicherzustellen, dass das SRECS eine angemessene Risikominderung bereitstellen kann.

ANMERKUNG 2 In einer großen Anzahl maschinenspezifischer Normen („C"-Normen in CEN) ist eine Risikoabschätzung durchgeführt worden, um eine erforderliche Kategorie in Übereinstimmung mit ISO 13849-1:1999 für sicherheitsbezogene Teile von Maschinensteuerungen auszuwählen. Es ist bekannt, dass zur Vereinfachung allgemein die folgenden Beziehungen verwendet werden: erforderliche Kategorie 1 zu erforderlichem SIL 1, erforderliche Kategorie 2 zu erforderlichem SIL 1, erforderliche Kategorie 3 zu erforderlichem SIL 2 und erforderliche Kategorie 4 zu erforderlichem SIL 3. Umfassendere Verfahren der Abbildung zwischen erforderlichen Kategorien aus ISO 13849-1:1999 und erforderlichen in dieser internationalen Norm verwendeten SILs sind in Beratung.

Für jede spezielle Gefährdung sollten die Anforderungen zur Sicherheitsintegrität separat für die durch das SRECS auszuführende(n) sicherheitsbezogene(n) Steuerungsfunktion(en) bestimmt werden (siehe 5.2.4.2).

Bild A.1 zeigt ein Beispiel einer praktischen Art und Weise der Durchführung einer Risikobeurteilung zu einer speziellen Gefährdung, die zur Abschätzung einer SIL-Anforderung für eine SRECS-Funktion führt. Diese Methodologie sollte für jedes Risiko durchgeführt werden, das durch eine sicherheitsbezogene Steuerungsfunktion zu reduzieren ist, die durch ein SRECS auszuführen ist. Bild A.1 sollte in Verbindung mit den erläuternden Informationen in diesem Anhang verwendet werden.

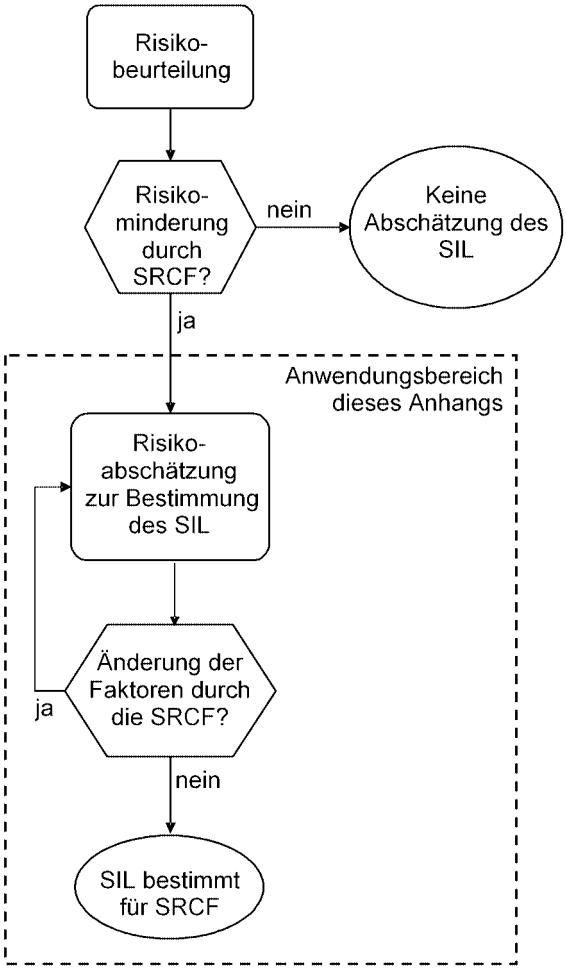


Bild A.1 – Ablauf des Prozesses der Festsetzung des SIL

Die Risikoabschätzung ist ein iterativer Prozess. Dies bedeutet, dass es notwendig ist, den Prozess mehr als einmal durchzuführen.

Bild A.1 zeigt einen rückgekoppelten Pfeil auf die Risikoabschätzung. Dies ist erforderlich, weil die Bereitstellung einer speziellen Schutzmaßnahme zur Implementierung einer SRCF einen Einfluss auf die Risikoparameter haben kann (z. B. die Verwendung eines Schutz-Lichtvorhangs kann zu einer größeren Zugriffshäufigkeit führen). Ein Ausfall des Lichtvorhangs setzt dann den Bediener einem größeren Risiko aus, als ursprünglich gedacht. Dies erfordert, dass der Prozess wiederholt werden sollte unter Anwendung des gleichen Verfahrens, jedoch unter Verwendung des (der) berichtigten Risikoparameter(s).

Am Ende des in Bild A.1 gezeigten Prozesses ist der abgeschätzte SIL die SIL-Anforderung für die sicherheitsbezogene Steuerungsfunktion.

A.2 Risikoabschätzung und Festsetzung des SIL

A.2.1 Identifizierung/Angabe der Gefährdung

Es werden die Gefährdungen angegeben, einschließlich derjenigen durch vernünftigerweise vorhersehbare Fehlanwendung, deren Risiken durch die Ausführung einer SRCF zu reduzieren sind. Diese Gefährdungen werden in der Spalte „Gefährdung“ in Tabelle A.5 aufgelistet.

A.2.2 Risikoabschätzung

Die Risikoabschätzung sollte für jede Gefährdung durch Bestimmung der Risikoparameter durchgeführt werden, die, wie in Bild A.2 gezeigt, aus Folgendem abgeleitet werden sollten:

– Schwere des Schadens, S, und
– Wahrscheinlichkeit des Auftretens dieses Schadens. Diese ist eine Funktion der:
  – Häufigkeit und Dauer der Exposition von Personen zur Gefährdung, F;
  – Wahrscheinlichkeit des Auftretens eines gefahrbringenden Ereignisses, W, und
  – Möglichkeiten zur Vermeidung oder Begrenzung des Schadens, P.

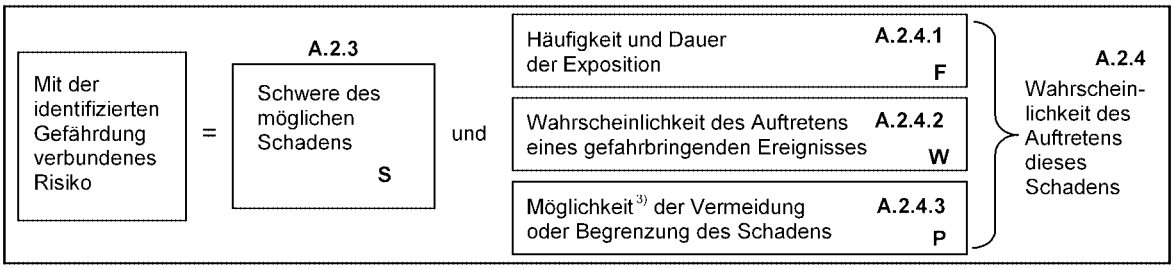


Bild A.2 – Parameter der Risikoabschätzung

Die in Tabelle A.5 eingetragenen Abschätzungen sollten üblicherweise auf worst-case-Betrachtungen für die SRCF beruhen. In einer Situation, in der jedoch zum Beispiel eine irreversible Verletzung möglich ist, aber mit einer bedeutend niedrigeren Wahrscheinlichkeit als eine reversible Verletzung, sollte jede Verletzungsstufe einen separaten Eintrag in der Tabelle haben. Es ist möglich, dass eine unterschiedliche SRCF für jeden Eintrag implementiert wird. Wenn eine SRCF implementiert wird, um beide Einträge abzudecken, sollte die höchste SIL-Zielanforderung verwendet werden.

A.2.3 Schwere (S)

Die Schwere von Verletzungen oder gesundheitlichen Schäden kann abgeschätzt werden, indem reversible Verletzungen, irreversible Verletzungen und Tod in Betracht gezogen werden. Es wird die passende Stufe der Schwere aus Tabelle A.1, basierend auf den Folgen einer Verletzung, ausgewählt, wobei:

4 eine tödliche oder bedeutende irreversible Verletzung bedeutet, dass es sehr schwierig sein wird, die gleiche Arbeit nach Heilung beizubehalten, wenn Heilung überhaupt möglich ist;

3 eine größere oder irreversible Verletzung bedeutet, die derart ausfällt, dass es möglich ist, die gleiche Arbeit nach Heilung beizubehalten. Dies kann auch eine schwere größere, jedoch reversible Verletzung, wie zum Beispiel gebrochene Gliedmaßen, einschließen;

2 eine reversible Verletzung, einschließlich schwerer Fleischwunden, Stichwunden und schwerer Quetschungen bedeutet, dass es der Behandlung durch einen Mediziner bedarf;

1 eine kleinere Verletzung, einschließlich Schrammen und kleiner Quetschungen bedeutet, dass es der Behandlung im Rahmen Erster Hilfe bedarf.

Die zutreffende Zeile für Auswirkungen (S) wird aus Tabelle A.1 ausgewählt. Die entsprechende Nummer wird in der Spalte „S" in Tabelle A.5. eingefügt.

Tabelle A.1 – Klassifikation der Schwere (S)

Auswirkungen	Schwere (S)
irreversibel: Tod, Verlust eines Auges oder Arms	4
irreversibel: gebrochene Gliedmaßen, Verlust (eines) mehrerer Finger(s)	3
reversibel: Behandlung durch einen Mediziner erforderlich	2
reversibel: Erste Hilfe erforderlich	1

3) Im englischen Text wurde der Begriff „probality", d. h. „Wahrscheinlichkeit" verwendet. Der Begriff „possibility", d. h. „Möglichkeit" ist aber zutreffend.

A.2.4 Wahrscheinlichkeit des Auftretens des Schadens

Jeder der drei Parameter der Wahrscheinlichkeit des Auftretens des Schadens (d. h. F, W und P) sollte unabhängig von den anderen abgeschätzt werden. Es ist eine worst-case-Annahme für jeden Parameter anzuwenden, um sicherzustellen, dass SRCF(s) nicht fälschlicherweise ein geringerer SIL als notwendig zugewiesen wird (werden). Im Allgemeinen ist die Verwendung eines Schemata einer aufgabenorientierten Analyse besonders empfehlenswert, um sicherzustellen, dass eine geeignete Betrachtung der Abschätzung der Wahrscheinlichkeit des Auftretens eines Schadens erfolgt.

A.2.4.1 Häufigkeit und Dauer der Exposition

Folgende Aspekte werden betrachtet, um den Grad der Exposition zu bestimmen:

– Notwendigkeit des Zugangs zum Gefahrenbereich basierend auf allen Betriebsarten, zum Beispiel Normalbetrieb, Instandhaltung und

– Art des Zugangs, zum Beispiel manuelles Einlegen von Material, Durchführung von Einstellungen.

Es sollte dann möglich sein, den mittleren Zeitabstand zwischen Expositionen und folglich die mittlere Häufigkeit des Zugangs abzuschätzen.

Es sollte ebenso möglich sein, die Dauer vorherzusehen, zum Beispiel ob sie größer als 10 min sein wird. Wenn die Dauer kleiner als 10 min ist, kann der Wert auf die nächste Stufe herabgestuft werden. Dies trifft nicht zu, wenn die Häufigkeit der Exposition ≤ 1 h ist, dieser Wert sollte nie abgestuft werden.

ANMERKUNG Die Dauer steht in Bezug zur Verrichtung von Tätigkeiten, die unter dem Schutz der SRCF ausgeführt werden. Die Anforderungen von IEC 60204-1 und ISO 14118 im Hinblick auf Energietrennung und Energieableitung sollten für wesentliche Eingriffe angewendet werden.

Dieser Faktor schließt keine Betrachtung zum Ausfall der SRCF ein.

Die zutreffende Zeile für Häufigkeit und Dauer der Exposition (F) wird aus Tabelle A.2 ausgewählt. Die entsprechende Nummer wird in der Spalte „F" in Tabelle A.5. eingefügt.

Tabelle A.2 – Klassifikation der Häufigkeit und der Dauer der Exposition (F)

Häufigkeit und Dauer der Exposition (F)	
Häufigkeit der Exposition	**Dauer > 10 min**
≤ 1 h	5
> 1 h bis ≤ 1 Tag	5
> 1 Tag bis ≤ 2 Wochen	4
> 2 Wochen bis ≤ 1 Jahr	3
> 1 Jahr	2

A.2.4.2 Wahrscheinlichkeit des Auftretens des gefahrbringenden Ereignisses

Die Wahrscheinlichkeit des Auftretens eines Schadens sollte unabhängig von den anderen verbundenen Parametern F und P abgeschätzt werden. Es sollte eine worst-case-Annahme für jeden Parameter angewendet werden, um sicherzustellen, dass SRCF(s) nicht fälschlicherweise ein geringerer SIL als notwendig zugewiesen werden. Um zu verhindern, dass dies auftritt, ist die Verwendung eines Schemata einer aufgabenorientierten Analyse besonders empfehlenswert, um sicherzustellen, dass eine geeignete Betrachtung der Abschätzung der Wahrscheinlichkeit des Auftretens eines Schadens erfolgt.

Dieser Parameter kann abgeschätzt werden unter Berücksichtigung:

a) der Vorhersagbarkeit des Verhaltens von Bauteilen der Maschine mit Relevanz in Bezug auf die Gefährdung in unterschiedlichen Arten der Verwendung (z. B. Normalbetrieb, Instandhaltung, Fehlersuche).

Dies erfordert eine sorgfältige Berücksichtigung des Steuerungssystems, besonders im Hinblick auf das Risiko eines unerwarteten Anlaufs. Die Schutzwirkung irgendeines SRECS sollte nicht berücksichtigt werden. Dies ist notwendig, um die Höhe des Risikos abzuschätzen, das entsteht, wenn das SRECS ausfällt. Allgemein ausgedrückt muss betrachtet werden, ob die Maschine oder das verarbeitete Material die Neigung hat, sich in unerwarteter Art und Weise zu verhalten.

Das Verhalten der Maschine wird von sehr vorhersehbar bis nicht vorhersehbar variieren, jedoch können unerwartete Ereignisse nicht vernachlässigt werden.

ANMERKUNG 1 Vorhersagbarkeit ist oft mit der Komplexität der Funktion der Maschine verbunden.

b) der festgelegten oder vorhersehbaren Merkmale menschlichen Verhaltens im Hinblick auf die Wechselwirkung mit Bauteilen der Maschine mit Relevanz in Bezug auf die Gefährdung. Dies kann charakterisiert werden durch:

- Stress (z. B. wegen Zeitdrucks, Arbeitsaufgaben, erkannter Schadensbegrenzung) und/oder
- fehlendes Bewusstsein für Informationen in Bezug auf die Gefährdung. Dies wird durch Faktoren wie Geschicklichkeit, Ausbildung, Erfahrung und Komplexität der Maschine/des Prozesses beeinflusst.

Diese Merkmale unterstehen normalerweise nicht dem direkten Einfluss des SRECS-Entwicklers, jedoch wird eine Analyse der Aufgaben Tätigkeiten aufdecken, bei denen ein vollständiges Bewusstsein für alle Probleme einschließlich unerwarteter Folgen vernünftigerweise nicht vorausgesetzt werden kann.

Eine „sehr hohe" Wahrscheinlichkeit des Auftretens eines gefährdenden Ereignisses sollte gewählt werden, um normale Produktionszwänge und worst-case-Betrachtungen widerzuspiegeln. Für die Verwendung eines niedrigeren Wertes sind eindeutige Gründe erforderlich (z. B. genau beschriebene Anwendung und Kenntnisse über Anwenderfähigkeiten auf hohem Niveau).

ANMERKUNG 2 Alle erforderlichen oder angenommenen Fertigkeiten, Kenntnisse usw. sollten in den Benutzerinformationen angegeben werden.

Die zutreffende Zeile für Wahrscheinlichkeit des Auftretens des gefährdenden Ereignisses (W) wird aus Tabelle A.3 ausgewählt. Die entsprechende Nummer wird in der Spalte „W" in Tabelle A.5. eingefügt.

Tabelle A.3 – Klassifikation der Wahrscheinlichkeit (W)

Wahrscheinlichkeit des Auftretens	Wahrscheinlichkeit (W)
sehr hoch	5
wahrscheinlich	4
möglich	3
selten	2
vernachlässigbar	1

A.2.4.3 Möglichkeit[3)] der Vermeidung oder Begrenzung des Schadens (P)

Dieser Parameter kann durch Berücksichtigung von Aspekten der Maschinenkonstruktion und der beabsichtigten Anwendung der Maschine, die helfen können den Schaden durch eine Gefährdung zu vermeiden oder zu begrenzen, abgeschätzt werden. Diese Aspekte schließen zum Beispiel ein:

- plötzliches, schnelles oder langsames Auftreten des gefährdenden Ereignisses;
- räumliche Möglichkeit sich von der Gefährdung zurückzuziehen;
- die Beschaffenheit des Bauteils oder des Systems, zum Beispiel ist ein Messer gewöhnlich scharf, ein Rohr in einer Molkerei ist gewöhnlich heiß, Elektrizität ist gewöhnlich von Natur aus gefährlich, jedoch unsichtbar und

3) Im englischen Text wurde der Begriff „probality", d. h. „Wahrscheinlichkeit" verwendet. Der Begriff „possibility", d. h. „Möglichkeit" ist aber zutreffend.

– Möglichkeit des Erkennens einer Gefährdung, zum Beispiel elektrische Gefährdung: eine Kupferschiene ändert nicht ihr Aussehen, ob sie unter Spannung steht oder nicht; zu erkennen, ob jemand ein Instrument benötigt, um festzustellen, ob elektrische Einrichtungen unter Spannung stehen oder nicht; Umgebungsbedingungen, zum Beispiel können hohe Geräuschpegel verhindern, dass eine Person den Start einer Maschine hört.

Die zutreffende Zeile für Möglichkeit[3)] der Vermeidung oder Begrenzung des Schadens (P) wird aus Tabelle A.4 ausgewählt. Die entsprechende Nummer wird in der Spalte „P" in Tabelle A.5. eingefügt.

Tabelle A.4 – Klassifikation der Möglichkeit[3)] der Vermeidung oder Begrenzung des Schadens (P)

Möglichkeit[3)] der Vermeidung oder Begrenzung des Schadens (P)	
unmöglich	5
selten	3
wahrscheinlich	1

A.2.5 Klasse der Wahrscheinlichkeit des Schadens (K)

Die Punkte aus den Spalten F, W und P werden für jede Gefährdung und, soweit zutreffend, für jede Verletzungsstufe addiert und die Summe in die Spalte K in Tabelle A.5 eingetragen.

Tabelle A.5 – Parameter zur Festlegung der Klasse der Wahrscheinlichkeit des Schadens (K)

Lfd. Nr.	Gefährdung	S	F	W	P	K
1						
2						
3						
4						

A.2.6 Festlegung des SIL

Tabelle A.6 zeigt an dem Schnittpunkt der Zeile Schwere (S) mit der zutreffenden Spalte (K), ob Handlungsbedarf besteht. Der schwarz gefärbte Bereich zeigt den festgelegten SIL als Soll für die SRCF. Die heller schattierten Bereiche sollten als Empfehlung betrachtet werden, dass andere Maßnahmen (AM) angewendet werden.

Tabelle A.6 – Matrix der Festlegung des SIL

Schwere (S)	Klasse (K)				
	3 bis 4	5 bis 7	8 bis 10	11 bis 13	14 bis 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(AM)	SIL 1	SIL 2	SIL 3
2			(AM)	SIL 1	SIL 2
1				(AM)	SIL 1

[3)] Im englischen Text wurde der Begriff „probality", d. h. „Wahrscheinlichkeit" verwendet. Der Begriff „possibility", d. h. „Möglichkeit" ist aber zutreffend.

BEISPIEL: Für eine spezifische Gefährdung, für die S als 3, F als 4, W als 5 und P als 5 bestimmt worden sind, ergibt sich:

$$K = F + W + P = 4 + 5 + 5 = 14$$

Bei Anwendung der Tabelle A.6 ergibt dies eine Zuweisung eines SIL 3 für die SRCF, die dazu vorgesehen ist, die spezielle Gefährdung abzuschwächen.

Bild A.3 zeigt ein Beispiel einer Dokumentation, die verwendet werden kann, um die Ergebnisse einer Aufgabe zur Festlegung des SIL bei Verwendung dieses informativen Anhangs festzuhalten.

Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:

Teil von:

Produkt:

Hersteller:

Datum:

schwarzer Bereich = Sicherheitsmaßnahmen erforderlich

grauer Bereich = Sicherheitsmaßnahmen empfohlen

☐ vorläufige Risikobeurteilung

☐ zwischenzeitliche Risikobeurteilung

☐ nachfolgende Risikobeurteilung

Auswirkungen	Schwere	Klasse K					Häufigkeit und		Wahrscheinlichkeit		Vermeidung	
	S	3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Dauer, F		gef. Ereigniss, W		P	
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 Stunde	5	häufig	5		
Permanent, Verlust von Fingern	3		AM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ Tag	5	wahrscheinlich	4		
Reversibel, medizinische Behandlung	2			AM	SIL 1	SIL 2	> 1 Tag – ≤ 2 Wo.	4	möglich	3	unmöglich	5
Reversibel, Erste Hilfe	1				AM	SIL 1	> 2 Wo. – ≤ 1 Jahr	3	selten	2	möglich	3
							> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Lfd. Nr.	Gef. Nr.	Gefährdung	S	F	W	P	K	Sicherheitsmaßnahme	sicher

Kommentare

Bild A.3 – Beispiel-Formblatt für den Prozess der Bestimmung des SIL

Anhang B
(informativ)

Beispiel eines Entwurfs eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) unter Anwendung der Konzepte und Anforderungen aus den Abschnitten 5 und 6

B.1 Allgemeines

Der von dieser Norm verwendete strukturierte Ansatz zum Entwurf eines SRECS definiert eine Methodologie, wonach funktionale Anforderungen und Anforderungen zur Sicherheitsintegrität für sicherheitsbezogene Steuerungsfunktionen in eine Anzahl von Teilfunktionen aufgeteilt werden. Dieser Prozess wird eingesetzt, um im Maschinensektor einen technischen Rahmen für funktionale Sicherheit zu implementieren. Bild B.1 beschreibt die verwendete Terminologie auf jeder dieser Stufen, die wichtig sind, wenn ein SRECS-Entwurf in eine Maschine integriert wird.

Diese Entwurfsmethodologie kann durch Verifikations- und Validierungsprozesse verwendet werden, um aufzuzeigen, dass ein SRECS die in Abschnitt 5 beschriebene Spezifikation der Sicherheitsanforderungen erfüllt.

Das nachfolgende Beispiel eines SRECS-Entwurfs ist dazu bestimmt, die Prinzipien der funktionalen Aufteilung und die Realisierung einer spezifizierten sicherheitsbezogenen Steuerungsfunktion in Übereinstimmung mit den Anforderungen von Abschnitt 6 zu erläutern. Folglich ist dieses Beispiel vereinfacht und berücksichtigt keine zusätzlichen Maßnahmen, die in Praxis erforderlich sein könnten, zum Beispiel Steuereinrichtungen mit selbsttätiger Rückstellung.

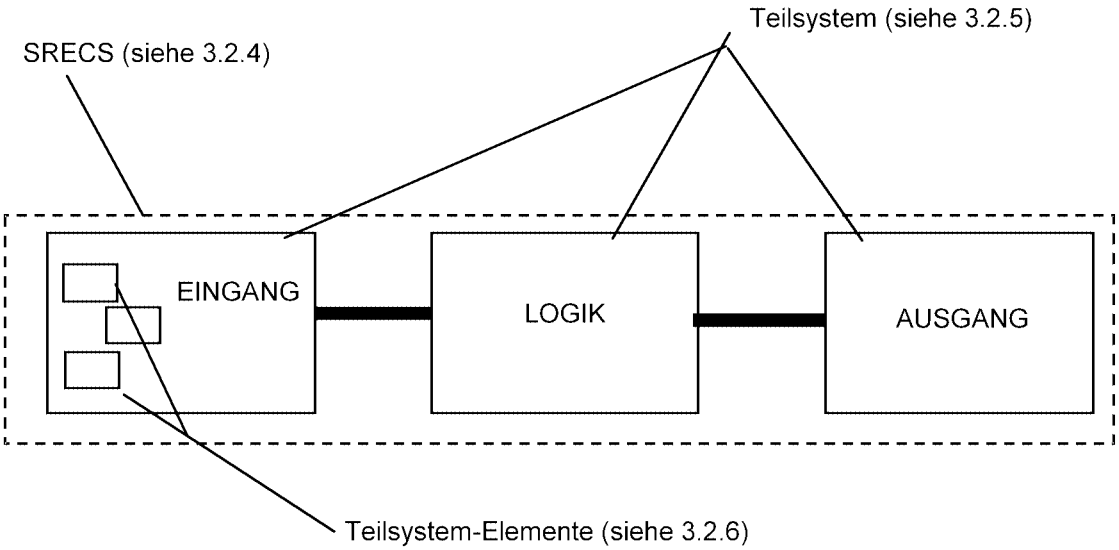


Bild B.1 – Terminologie im Zusammenhang funktionaler Aufteilung

Im Allgemeinen sind die in Bild B.1 gezeigten Begriffe dafür bestimmt, den Entwurfsprozess in zwei Schlüsselphasen zu beschreiben, dies sind:

– SRECS-Entwurf, der von einem Maschinenkonstrukteur oder einem Steuerungssystemintegrator durchgeführt werden könnte und

– Teilsystem-(und Teilsystem-Element)Entwurf, was für die Verkäufer elektrischer Einrichtungen und Steuergeräte (z. B. Schütze, Verriegelungsschalter, speicherprogrammierbare Steuerungen) und die Maschinenkonstrukteure oder Steuerungssystemintegratoren zutreffend ist.

B.2 Beispiel

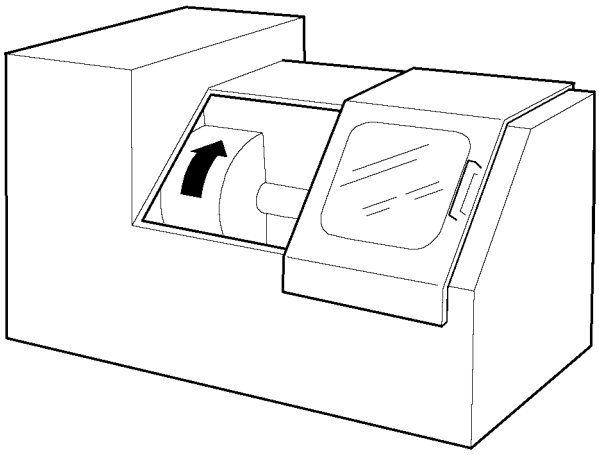


Bild B.2 – Beispiel einer Maschine

Die in dieser Norm verwendete Methodologie basiert auf einem strukturierten top-down-Ansatz zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen und dem Entwurf des SRECS, das diese Funktionen ausführt.

Schritt 1: Spezifikation der SRCF-Sicherheitsanforderungen (Abschnitt 5)

Aus einer Spezifikation der SRCF-Sicherheitsanforderungen können die folgenden Informationen abgeleitet werden:

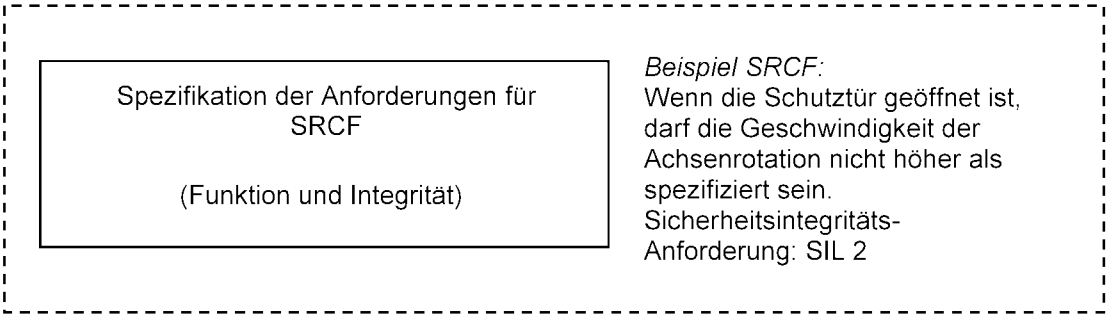


Bild B.3 – Spezifikation der Anforderungen für eine SRCF

Schritt 2: SRECS-Entwurfs- und Entwicklungsprozess (siehe 6.6.2)

Schritt 2.1: Die in der Spezifikation der Sicherheitsanforderungen spezifizierte sicherheitsbezogene Steuerungsfunktion wird in eine Struktur von Funktionsblöcken aufgeteilt.

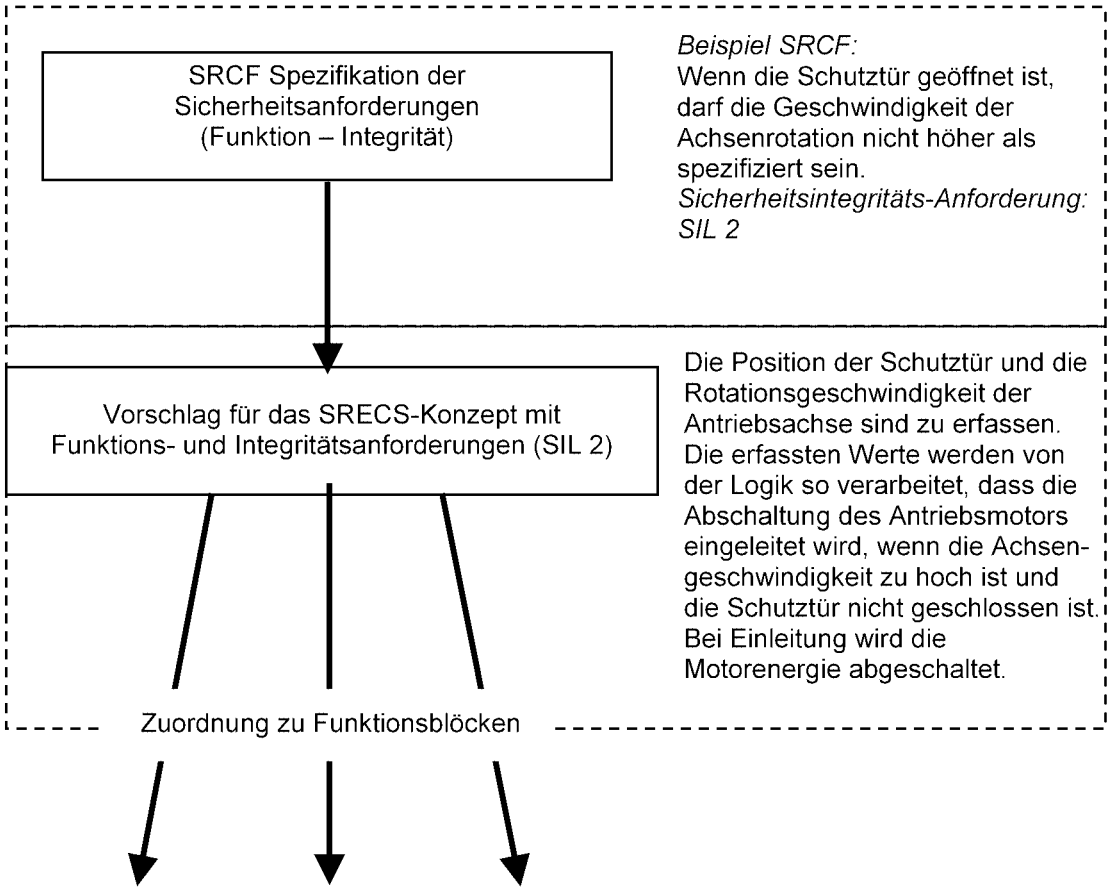


Bild B.4 – Aufteilung in eine Struktur von Funktionsblöcken

Schritt 2.2: Die Struktur der Funktionsblöcke ergibt ein erstes Konzept für eine Architektur des SRECS. Die Sicherheitsanforderungen für jeden Funktionsblock werden aus der Spezifikation der Sicherheitsanforderungen der entsprechenden sicherheitsbezogenen Steuerungsfunktion abgeleitet.

Das (Die) Element(e), das (die) jeden Funktionsblock ausführt (ausführen), muss (müssen) zumindest die gleiche SIL-Fähigkeit erreichen, wie die für die SRCF bestimmte. Dies ist in Bild B.5 als eine SIL 2-Fähigkeit gezeigt (d. h. FB1 SILCL 2 usw.).

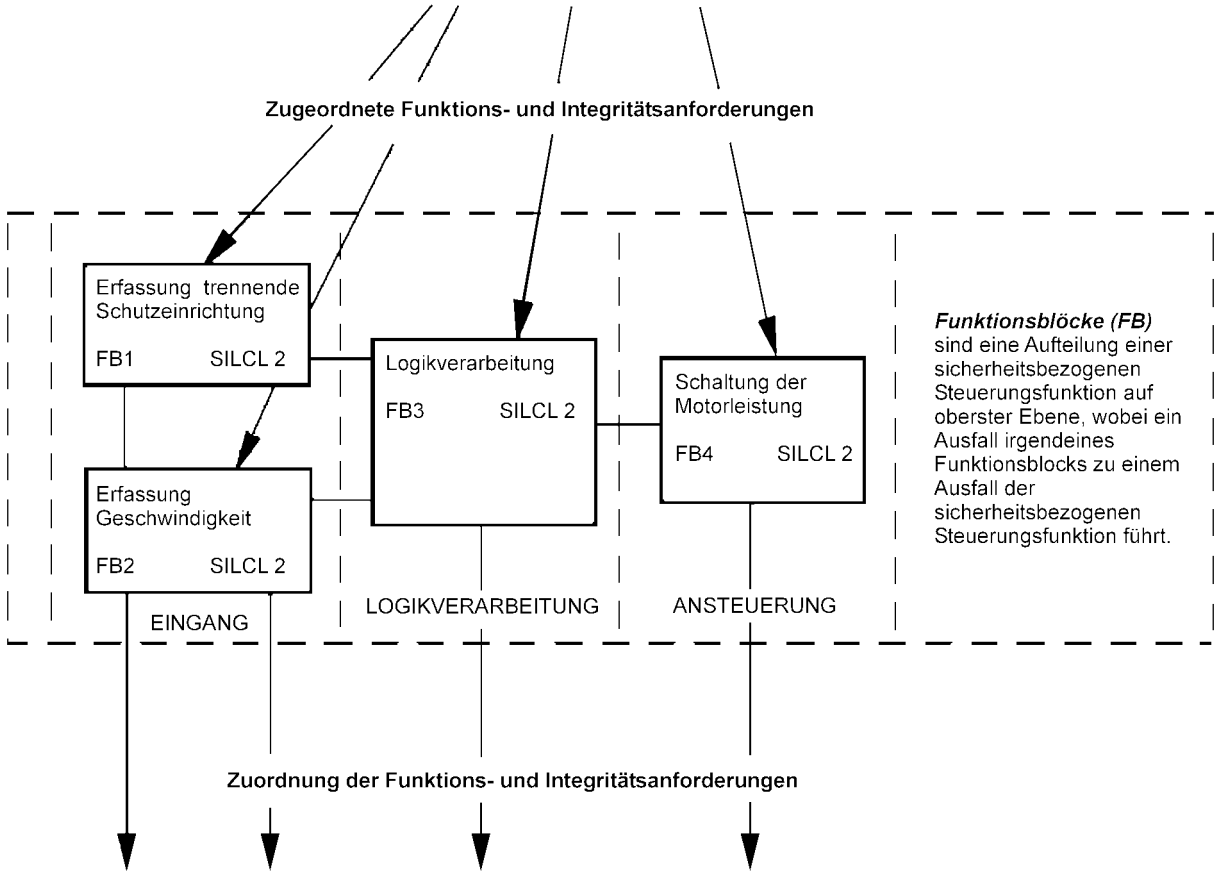


Bild B.5 – Erstes Konzept für eine Architektur eines SRECS

Schritt 3: Jeder Funktionsblock ist zu einem Teilsystem innerhalb der Architektur des SRECS zugeordnet. Jedes Teilsystem kann aus Teilsystem-Elementen bestehen und soweit notwendig Diagnosefunktionen enthalten, um sicherzustellen, dass Fehler erkannt werden können und angemessene Schritte unternommen werden (siehe 6.2).

Die Architektur sollte das SRECS in Form seiner Teilsysteme und ihrer Wechselbeziehungen beschreiben. Für dieses Beispiel gibt es eine Anzahl von Auswahlmöglichkeiten, die für die Realisierung des SRECS und die Architektur seiner Teilsysteme verwendet werden können.

Beispiel 1: In diesem Beispiel (siehe Bild B.6) sind die Diagnosefunktionen innerhalb jedes Teilsystems eingebettet.

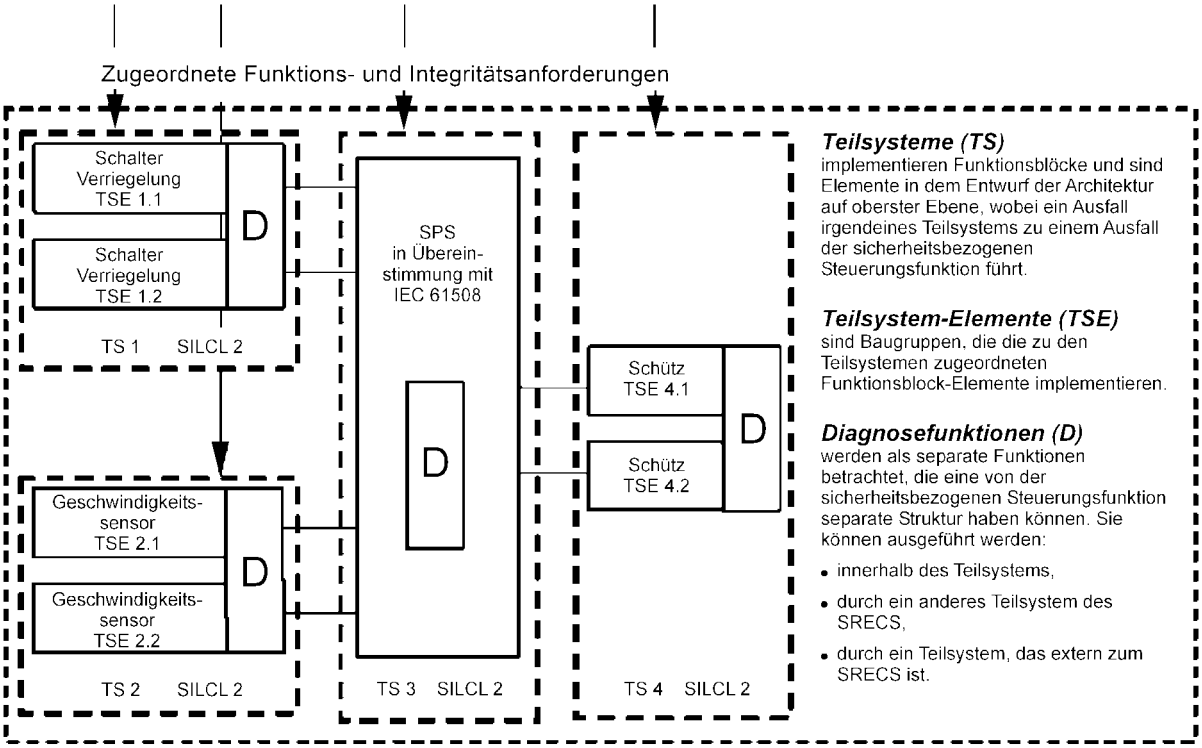


Bild B.6 – SRECS-Architektur mit innerhalb jedes Teilsystems eingebetteten Diagnosefunktionen (TS1 bis TS4)

Beispiel 2: In diesem Beispiel (siehe Bild B.7) sind die Diagnosefunktionen innerhalb einer speicherprogrammierbaren Steuerung (SPS), die die relevanten Aspekte der IEC 61508 erfüllt, in TS3 eingebettet.

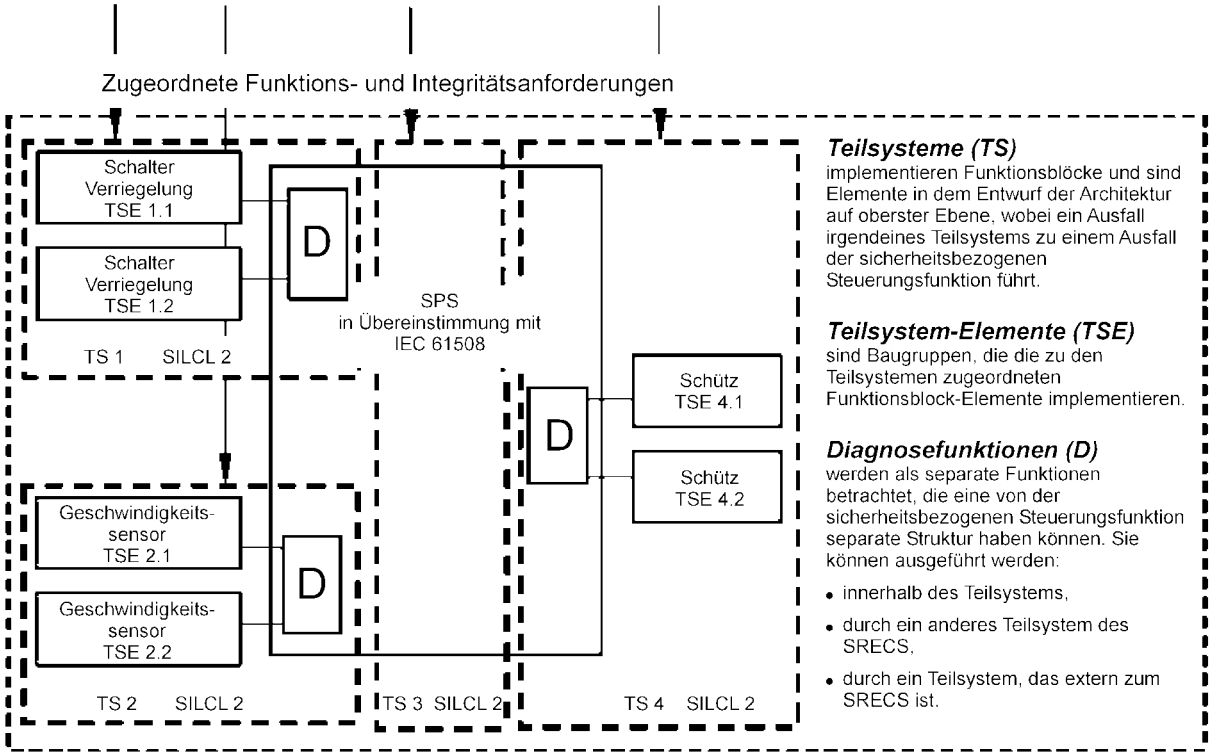


Bild B.7 – SRECS-Architektur mit innerhalb des Teilsystems TS3 eingebetteten Diagnosefunktionen

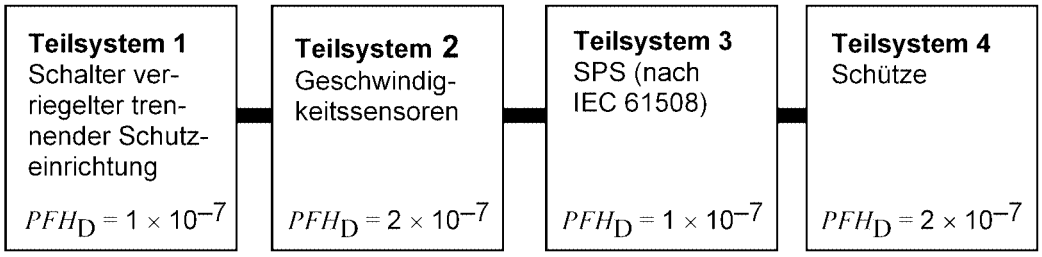
Schritt 4: Abschätzung des durch das SRECS erreichten SIL (siehe 6.6.3)

Der SIL, der für das SRECS in Anspruch genommen werden kann, muss geringer als oder gleich dem geringsten Wert der SILCLs irgendeines der Teilsysteme sein. Die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls des SRECS (PFH_{DSRECS}) ist die Summe der Wahrscheinlichkeiten gefahrbringender zufälliger Hardwareausfälle aller Teilsysteme pro Stunde (PFH_{D1} bis PFH_{DN}), die an der Ausführung der sicherheitsbezogenen Steuerungsfunktion beteiligt sind und muss, wo zutreffend, die Wahrscheinlichkeit gefahrbringender Übertragungsfehler für digitale Datenkommunikationsprozesse (P_{TE}) wie folgt einschließen:

$$PFH_{\mathrm{DSRECS}} = PFH_{\mathrm{D1}} + \ldots + PFH_{\mathrm{DN}} + P_{\mathrm{TE}}$$

Für dieses Beispiel ist der Ausfallgrenzwert für die sicherheitsbezogene Steuerungsfunktion SIL 2 und nach Tabelle 3 (siehe 5.2.4.2) ist dies äquivalent zu einer Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (PFH_{D}) im Bereich von $\geq 10^{-7}$ bis $< 10^{-6}$. Folglich kann unter der Annahme, dass die Wahrscheinlichkeiten eines gefahrbringenden Ausfalls pro Stunde jedes der Teilsysteme, so wie unten gezeigt sind, die Summe der Wahrscheinlichkeiten eines gefahrbringenden Ausfalls pro Stunde aller Teilsysteme, wie in Bild B.8 gezeigt, abgeschätzt werden.

Daher lässt sich für dieses Beispiel zeigen, dass der Entwurf des SRECS alle die Anforderungen erfüllt, um die bestimmte sicherheitsbezogene Steuerungsfunktion mit SIL 2 auszuführen.



$$PFH_{DSRECS} = (1 \times 10^{-7}) + (2 \times 10^{-7}) + (1 \times 10^{-7}) + (2 \times 10^{-7}) = 6 \times 10^{-7}$$

Bild B.8 – Abschätzung der PFH_D für ein SRECS

Anhang C
(informativ)

Hinweise zu Entwurf und Entwicklung von Embedded-Software

ANMERKUNG Dieser informative Anhang ist dazu vorgesehen, die grundlegenden Verfahren zu veranschaulichen, die erforderlich sind, um die Anforderungen von IEC 61508-3 zu erfüllen. Ohne die Anwendung weiterer Maßnahmen ergibt sich aus ihm selbst keine Übereinstimmung mit IEC 61508-3.

C.1 Allgemeines

Dieser Anhang ist dazu vorgesehen, Personen beim Entwurf und der Entwicklung von Embedded-Software zur Implementierung von sicherheitsbezogenen Steuerungsfunktionen innerhalb eines SRECS behilflich zu sein.

Das hier behandelte Hauptziel sind allgemeine Hinweise zur Verhinderung von Ausfällen der Embedded-Software und zu jedem anderen unerwarteten Verhalten der Embedded-Software, das zum Entstehen von gefährlichen Fehlern in dem System führen könnte.

Um diese Ziele zu erreichen, werden folgende Punkte betrachtet:

– eine Beschreibung der Haupteigenschaften, die Softwareelemente eines SRECS besitzen sollten, um seine Qualität und Sicherheit zu garantieren (Richtlinien zu Softwareelementen);

– die Aufstellung aller relevanten mit Softwareentwicklung verbundenen technischen Aktivitäten und Vorkehrungen für die am Softwareentwurf Beteiligten. Diese können dann verwendet werden, um den Entwickler während der Produktion dieser Art von Software zu leiten (Software-Entwicklungsprozess-richtlinien);

– einen Referenzrahmen zur Softwarebewertung. Dies erlaubt dem Softwareentwickler und/oder dem Analysierenden zu entscheiden, dass Softwareelemente die Sicherheitsanforderungen des zu analysierenden SRECS oder SRECS-Teilsystems erfüllen (Software-Verifikationsrichtlinien).

Dieser Anhang liefert eine Zusammenstellung grundlegender Richtlinien im Zusammenhang mit IEC 61508-3, die auf Embedded-Software für Mikrokontroller angepasst sind.

C.2 Richtlinien zu Softwareelementen

Dieser Abschnitt stellt die Richtlinien dar, die ein Embedded-Softwareelement eines SRECS oder SRECS-Teilsystems erfüllen sollte, um im Betrieb sicher und von zufrieden stellend hoher Qualität zu sein. Um ein solches Softwareelement zu erhalten, sollte eine Anzahl von Aktivitäten, eine bestimmte Organisation und eine Anzahl von Grundsätzen eingerichtet werden. Dies sollte so früh wie möglich im Entwicklungszyklus erfolgen.

C.2.1 Schnittstelle mit der Systemarchitektur

Die Liste der Einschränkungen, die sich aus der Hardwarearchitektur für die Software ergibt, sollte definiert und dokumentiert werden. Auswirkungen jeder Hardware/Software-Wechselwirkung auf die Sicherheit der überwachten Maschine oder des Systems sollten vom Konstrukteur identifiziert und ausgewertet werden und im Softwareentwurf berücksichtigt werden.

ANMERKUNG Einschränkungen schließen ein: Protokolle und Formate, Eingangs-/Ausgangsfrequenzen, durch steigende oder fallende Flanke oder durch Zustand, Eingangsdaten, die inverse Logik verwenden usw. Die Auflistung dieser Einschränkungen ermöglicht sie zu Beginn der Entwicklungsaktivität zu berücksichtigen und reduziert das Risiko von Inkompatibilitäten zwischen Software und Hardware, wenn die Software auf der Zielhardware installiert wird.

C.2.2 Softwarespezifikationen

Softwarespezifikationen sollten die folgenden Punkte berücksichtigen:

– sicherheitsbezogene Steuerungsfunktionen mit quantitativer Beschreibung der Kriterien der Leistungsfähigkeit (Präzision, Genauigkeit) und zeitlichen Einschränkungen (Reaktionszeit), wenn möglich alle mit Toleranzen oder Grenzen;

– Systemkonfiguration oder Architektur;

– Instruktionen, die für die Sicherheitsintegrität der Hardware relevant sind (Logikeinheiten, Sensoren, Aktoren usw.);

– Instruktionen, die für die Softwareintegrität relevant sind;

– Einschränkungen in Bezug auf Speicherkapazität und Systemreaktionszeit;

– Benutzer- und Geräteschnittstellen;

– Instruktionen für die Eigenüberwachung der Software und für die durch Software durchgeführte Überwachung der Hardware;

– Instruktionen, die es erlauben, alle sicherheitsbezogenen Steuerungsfunktionen während des Betriebs der Systeme zu verifizieren (z. B. Test während des Betriebs, Erfassungszeit flüchtiger Signale, Gleichzeitigkeit mit Abtastrate).

ANMERKUNG 1 Die Instruktionen für die Überwachung, die unter Berücksichtigung der Sicherheitsziele und betrieblicher Einschränkungen (Dauer des kontinuierlichen Betriebs usw.) entwickelt worden sind, können Vorrichtungen wie Watchdogs, Überwachung der Auslastung der Prozessorzentraleinheit (CPU), Rückkopplung von Ausgängen auf Eingänge für die Eigenüberwachung der Software einschließen. Für die Überwachung der Hardware, die Überwachung der CPU und des Speichers usw. Instruktionen für die Verifikation der sicherheitsbezogenen Steuerungsfunktion: Die Möglichkeit regelmäßiger Verifikation des korrekten Betriebs der Sicherheitsvorrichtungen sollte zum Beispiel in die Spezifikationen einbezogen werden.

Funktionale Anforderungen sollten für jede funktionale Betriebsart spezifiziert werden. Der Übergang von einer Betriebsart auf die andere sollte spezifiziert werden.

ANMERKUNG 2 Funktionale Betriebsarten können einschließen: nominelle Betriebsarten und eine oder mehrere herabgestufte Betriebsart(en). Das Ziel ist es, das Verhalten in allen Situationen zu spezifizieren, um unerwartete Verhaltensweisen in nichtnominellen Zusammenhängen zu vermeiden.

C.2.3 Vorhandene Software

Der Begriff „vorhandene“ Software bezieht sich auf Quellmodule, die nicht besonders für das vorgesehene System entwickelt worden sind und in den Rest der Software integriert werden. Dies schließt Softwareelemente, die vom Entwickler für vorherige Projekte entwickelt worden sind oder kommerziell erwerbbare Software ein (z. B. Module für Berechnungen, Algorithmen zur Sortierung von Daten).

Wenn diese Art von Software behandelt wird und besonders im Fall von kommerziellen Softwareelementen, haben die Entwickler nicht immer Zugriff auf alle benötigten Elemente, um die vorherigen Anforderungen zu erfüllen (z. B. welche Tests durchgeführt worden sind; die Verfügbarkeit der Entwurfsdokumentation). Daher kann eine besondere Koordination mit dem die Analyse Ausführenden zum frühest möglichen Zeitpunkt notwendig sein.

Der Entwickler sollte den die Analyse Ausführenden auf die Verwendung bereits vorhandener Software hinweisen und der Entwickler sollte aufzeigen, dass vorhandene Software das gleiche Niveau wie die anderen Sotwareelemente hat. Ein solcher Nachweis sollte wie folgt ausgeführt werden:

a) entweder durch Anwendung der gleichen Verifikationsaktivitäten für die bereits vorhandene Software wie für die übrige Software und/oder

b) durch praktische Erfahrungen, bei denen die vorhandene Software auf einem ähnlichen System in einer vergleichbaren Anwendungsumgebung in Funktion war (z. B. kann es notwendig sein, die Auswirkungen eines Wechsels des Compilers oder eines anderen Softwarearchitekturformats zu bewerten).

ANMERKUNG 1 Das Ziel des Hinweises auf Verwendung von vorhandener Software ist es, die Beratung mit dem die Analyse Ausführenden über eventuelle Schwierigkeiten, die diese Art von Software bedingen könnte, so früh wie möglich zu beginnen. Die Integration vorhandener Quellcodemodule kann der Grund für bestimmte Besonderheiten oder unsicheres Verhalten sein, wenn sie nicht nach den gleichen Maßstäben wie die übrige Software entwickelt wurden.

Bereits vorhandene Software sollte unter Verwendung der gleichen Prinzipien zu Konfigurationsmanagement und Versionskontrolle, die für die übrige Software angewendet werden, identifiziert werden.

ANMERKUNG 2 Konfigurationsmanagement und Versionskontrolle sollten für alle Softwarekomponenten unabhängig von ihrem Ursprung verwendet werden.

C.2.4 Softwareentwurf

Die Beschreibung des Softwareentwurfs sollte eine Beschreibung folgender Punkte beinhalten:

– der Softwarearchitektur, die die Struktur definiert, die dazu bestimmt ist, Spezifikationen zu erfüllen;
– der Eingaben und Ausgaben (z. B. in Form eines internen und externen Datenverzeichnisses) für alle Module, die die Softwarearchitektur bilden;
– der Interrupts;
– der globalen Daten;
– jeden Softwaremoduls (Eingaben/Ausgaben, Algorithmen, Einzelheiten des Entwurfs usw.);
– der verwendeten Modul- oder Datenbibliotheken;
– der verwendeten bereits vorhandenen Software.

Software sollte modular sein und in logischer Art und Weise geschrieben sein, um ihre Verifikation oder Pflege zu erleichtern:

– jedes Modul oder jede Gruppe von Modulen sollte(n) soweit möglich zu einer Funktion aus der (den) Spezifikation(en) korrespondieren,
– Schnittstellen zwischen Modulen sollten so einfach wie möglich sein.

ANMERKUNG Die allgemeinen Eigenschaften einer korrekten Softwarearchitektur können in folgender Weise zusammengefasst werden: ein Modul sollte über einen hohen Grad an funktionalem Zusammenhalt verfügen und eine einfache Schnittstelle zu seiner Umgebung haben.

Software sollte:

– die Anzahl oder den Umfang globaler Variablen beschränken;
– die Anordnung von Feldern in Speichern kontrollieren (um das Risiko von Überläufen zu vermeiden).

C.2.5 Codierung

Der Quellcode sollte:

– lesbar, verständlich und Gegenstand von Tests sein;
– die Entwurfspezifikationen des Softwaremoduls erfüllen;
– die Anweisungen des Codierhandbuchs befolgen.

C.3 Richtlinien für den Software-Entwicklungsprozess

C.3.1 Entwicklungsprozess: Software-Lebenszyklus

Das Ziel der nachfolgenden auf den Software-Lebenszyklus anwendbaren Hinweise ist es, eine formalisierte Beschreibung der Organisation der Softwareentwicklung und insbesondere der verschiedenen technischen Aufgaben, die diese Entwicklung darstellen, zu erreichen.

Der Software-Entwicklungslebenszyklus sollte spezifiziert und dokumentiert werden (z. B. in einem Softwarequalitätsplan). Der Lebenszyklus sollte alle technischen Aktivitäten und Phasen einschließen, die notwendig und ausreichend für die Softwareentwicklung sind.

Jede Phase des Lebenszyklus sollte in grundlegende Aufgaben unterteilt werden und sollte eine Beschreibung folgender Punkte beinhalten:

– Eingaben (Dokumente, Normen usw.);
– Ausgaben (erzeugte Dokumente, Analyseberichte usw.);
– durchzuführende Aktivitäten;
– durchzuführende Verifikationen (Analysen, Tests usw.).

C.3.2 Dokumentation: Dokumentationsmanagement

Die Dokumentation sollte die Anforderungen von Abschnitt 10 dieser Norm erfüllen.

C.3.3 Konfigurationsmanagement und Management der Softwaremodifikationen

Das Konfigurationsmanagement und das dementsprechende Versionsmanagement ist ein unentbehrlicher Teil jeder Entwicklung, für die eine Genehmigung erforderlich sein kann. Tatsächlich ist eine Genehmigung nur gültig, wo eine gegebene Konfiguration identifiziert werden kann. Das Konfigurationsmanagement umfasst Konfigurationsidentifikationsaktivitäten, Modifikationsmanagement, die Festsetzung von Referenzpunkten und die Archivierung von Softwareelementen einschließlich der zugehörigen Daten (Dokumente, Testaufzeichnungen usw.). Über den gesamten Lebenszyklus des Projektes sind die wichtigsten Ziele bereitzustellen:

– eine definierte und kontrollierte Softwarekonfiguration, die eine physikalische Archivierung garantiert und dazu verwendet werden kann, einen ausführbaren Code zusammenhängend zu reproduzieren (mit Berücksichtigung zukünftiger Softwareproduktion oder Modifikation);
– eine Referenzbasis für das Modifikationsmanagement;
– ein Mittel zur Kontrolle, so dass alle Probleme geeignet analysiert werden und dass die genehmigten Modifikationen richtig durchgeführt werden.

Gründe für Modifikationen können zum Beispiel bedingt sein durch:

– funktionale Sicherheit unterhalb der spezifizierten;
– Erfahrungen mit systematischen Fehlern;
– neue oder geänderte Gesetzgebung zur Sicherheit;
– Modifikationen der Maschine oder ihrer Verwendung;
– Modifikation der gesamten Sicherheitsanforderungen;
– Analyse der Leistungsfähigkeit in Bezug auf Betrieb und Instandhaltung, die darauf hinweist, dass die Leistungsfähigkeit unterhalb des Solls liegt.

C.3.4 Konfigurations- und Archivierungsmanagement

Es sollte ein Verfahren für das Konfigurationsmanagement und das Management der Modifikationen definiert und dokumentiert werden. Dieses Verfahren sollte mindestens die folgenden Punkte einschließen:

– Gegenstände, die durch die Konfiguration gemanagt werden, zumindest: Softwarespezifikation, vorläufiger und detaillierter Softwareentwurf, Quellcodemodule, Pläne, Verfahren und Ergebnisse der Tests zur Validierung;
– Identifikationsregeln (für ein Quellmodul, für eine Softwareversion usw.);
– Behandlung von Modifikationen (Aufzeichnung von Anforderungen usw.).

Für jeden Gegenstand der Konfiguration sollte es möglich sein, alle Änderungen, die aufgetreten sein könnten und die Versionen aller zugehörigen Elemente zu identifizieren.

ANMERKUNG 1 Der Zweck besteht darin, die historische Entwicklung jeden Gegenstands verfolgen zu können: welche Modifikationen sind durchgeführt worden, warum und wann?

Das Software-Konfigurationsmanagement sollte es erlauben, eine genaue und präzise Identifikation einer Softwareversion zu erreichen. Das Konfigurationsmanagement sollte alle Gegenstände in Verbindung bringen (und ihre Versionen), die zur Demonstration der funktionalen Sicherheit benötigt werden.

Alle Gegenstände der Softwarekonfiguration sollten durch das Konfigurationsmanagementverfahren berücksichtigt werden, bevor sie getestet werden oder von dem die Analyse Ausführenden für die Bewertung der abschließenden Softwareversion angefordert werden.

ANMERKUNG 2 Das Ziel an dieser Stelle ist es, sicherzustellen, dass das Bewertungsverfahren an Software, bei der alle Elemente einen präzisen Zustand haben, ausgeführt wird. Jede nachträgliche Änderung mag eine Revision der Software erfordern, so dass sie von dem die Analyse Ausführenden erkennbar ist.

Es sollten Verfahren für die Archivierung der Software und ihrer zugehörigen Daten aufgestellt werden (Verfahren zur Speicherung von Backups und Archiven).

ANMERKUNG 3 Diese Backups und Archive können dazu verwendet werden, die Software während ihrer funktionalen Gebrauchsdauer zu pflegen und zu modifizieren.

C.3.5 Management der Softwaremodifikationen

Jede Softwaremodifikation, die einen Einfluss auf die funktionale Sicherheit des SRECS hat, sollte den Regeln, die für das Management der Modifikationen und das Konfigurationsmanagement aufgestellt sind, unterworfen werden, so dass der Entwicklungsprozess an dem höchsten erforderlichen Punkt „stromaufwärts“ wieder aufgenommen wird, um die Modifikation ohne Verringerung der funktionalen Sicherheit zu berücksichtigen.

ANMERKUNG Insbesondere sollte auch die Dokumentation aktualisiert und alle notwendigen Verifikationsaktivitäten durchgeführt werden. Dies garantiert, dass die Software nach jeder Modifikation ihre gesamten ursprünglichen Eigenschaften behält.

C.4 Entwicklungswerkzeuge

Werkzeuge, die während der Entwicklungsverfahren verwendet werden (Compiler, Linker, Tests usw.), sollten in der Dokumentation aufgeführt sein (Name, Referenz, Version usw.), die mit der Softwareversion verbunden ist (z. B. in dem Versionskontrolldokument).

ANMERKUNG Verschiedene Versionen von Werkzeugen müssen nicht notwendigerweise die gleichen Ergebnisse erzeugen. Eine genaue Identifikation der Werkzeuge zeigt deshalb direkt den Zusammenhang des Prozesses der Erzeugung einer ausführbaren Version, wenn eine Version modifiziert wird.

C.5 Reproduktion, Lieferung

C.5.1 Erzeugung des ausführbaren Codes

Jede Option oder Änderung in der Erzeugung während der Softwareproduktion sollte festgehalten werden (z. B. in der Versionsliste), so dass es möglich ist festzustellen, wie und wann die Software erzeugt wurde.

C.5.2 Softwareinstallation und Nutzung

Alle Ausfälle, die mit sicherheitsbezogenen Steuerungsfunktionen verbunden sind und dem Konstrukteur des Systems bekannt geworden sind, sollten aufgezeichnet und analysiert werden.

ANMERKUNG Dies bedeutet, dass sich der Konstrukteur aller sicherheitsbezogenen Ausfälle, die ihm mitgeteilt wurden, bewusst ist und dass er die angemessene Reaktion erfolgen lässt (z. B. Warnung anderer Anwender, Softwaremodifikation usw.).

C.6 Verifikation und Validierung der Software

Der Sinn von Verifikationsaktivitäten ist es aufzuzeigen, dass Softwareelemente, die aus einer gegebenen Phase des Entwicklungszyklus stammen, mit den Spezifikationen, die während der vorherigen Phasen erstellt worden sind und mit jeder anwendbaren Norm oder Regel übereinstimmen. Sie dienen auch als Maßnahme zur Erkennung und Darlegung für jeden Fehler, der eventuell während der Softwareentwicklung gemacht worden ist.

Softwareverifikation ist nicht einfach eine Reihe von Tests, obwohl Verifikation die vorherrschende Aktivität für das in diesem Anhang betrachtete relativ kleine Softwareelement ist. Andere Aktivitäten wie zum Beispiel Überprüfungen und Analysen, ob in Verbindung mit diesen Tests oder nicht, werden auch als Verifikationsaktivitäten betrachtet. In bestimmten Fällen können sie einige Tests ersetzen (z. B. im Falle, dass ein Test nicht durchgeführt werden kann, weil er die Zerstörung eines Hardwarebauteils zur Folge hätte).

C.7 Allgemeine Richtlinien zur Verifikation und Validierung

Der die Analyse Ausführende sollte fähig sein, die Bewertung der Softwarekonformität durch die Ausführung von allen während der verschiedenen Software-Entwicklungsphasen als hilfreich betrachteten Überprüfungen oder Begutachtungen durchzuführen.

Alle technischen Aspekte von Software-Lebenszyklusprozessen sind Gegenstand der Bewertung durch den die Analyse Ausführenden. Es sollte ihm erlaubt sein, alle Verifikationsberichte (Tests, Analysen usw.) und alle technischen Dokumente, die während der Softwareentwicklung verwendet werden, zu Rate zu ziehen.

ANMERKUNG 1 Die Beteiligung des die Analyse Ausführenden in der Spezifikationsphase ist gegenüber einer späteren Beteiligung zu bevorzugen, weil dies den Einfluss auf jede gemachte Entscheidung begrenzen sollte. Auf der anderen Seite sind finanzielle und menschliche Aspekte des Projekts nicht Gegenstand der Bewertung.

ANMERKUNG 2 Es liegt im Interesse des Antragstellers, dass ein befriedigender Nachweis zu allen während der Softwareentwicklung durchgeführten Aktivitäten geführt wird.

ANMERKUNG 3 Der die Analyse Ausführende sollte alle notwendigen Elemente zu seiner Verfügung haben, um eine Meinung zu formulieren.

Die Bewertung der Softwarekonformität wird für eine spezifische, referenzierte Softwareversion ausgeführt. Jede Modifikation von früher bewerteter Software, die von dem die Analyse Ausführenden abschließend bewertet wurde, sollte auf die letzte Version ausgerichtet sein, so dass alle zusätzlichen Bewertungsaktivitäten zur Aktualisierung dieser Bewertung durchgeführt werden können.

ANMERKUNG 4 Jede Modifikation kann das Verhalten der Software verändern; die durchgeführte Bewertung des die Analyse Ausführenden kann daher nur für eine bestimmte Softwareversion zutreffen.

C.8 Überprüfung der Verifikation und Validierung

Analyseaktivitäten und die Verifikation des Softwareentwurfs sollten die Konformität zu Spezifikationen verifizieren.

ANMERKUNG 1 Der Zweck besteht darin sicherzustellen, dass die Softwarespezifikation und der Softwareentwurf (sowohl vorläufiger als auch detaillierter) in Übereinstimmung miteinander stehen.

Eine externe Überprüfung zur Validierung (mit dem die Analyse Ausführenden) sollte am Ende der Validierungsphase abgehalten werden.

ANMERKUNG 2 Diese kann dazu verwendet werden festzustellen, ob das Element die Spezifikationen erfüllt oder nicht.

Das Ergebnis jeder Überprüfung sollte dokumentiert und archiviert werden. Das Ergebnis sollte eine Liste aller im Überprüfungsprozess entschiedenen Aktionen und die Schlussfolgerungen aus der Überprüfung einschließen (Entscheidung, ob zur nächsten Aktivität übergegangen wird oder nicht). Die im Rahmen der Überprüfungen definierten Aktivitäten sollten kontrolliert und ausgeführt werden.

C.9 Softwaretest

C.9.1 Allgemeine Validierung

Bevor die ersten Testberichte erstellt werden, ist es wichtig, in einem Testplan eine Teststrategie aufzustellen. Diese Strategie zeigt den gewählten Lösungsweg, die Ziele, die im Hinblick auf die Testabdeckung formuliert sind, die verwendeten Umgebungen und die spezifischen Verfahren, die anzuwendenden Erfolgskriterien usw.

Die Testziele sollten dem Typ der Software und den spezifischen Faktoren angepasst werden. Diese Kriterien bestimmen die Art der auszuführenden Tests – Funktionstests, Test unter Grenzbedingungen, Test außerhalb von Grenzbedingungen, Tests der Leistungsfähigkeit, Test der Auslastung, Test zum Ausfall externer Einrichtungen, Konfigurationstests – ebenso wie den Bereich der Objekte, die vom Test abzudecken sind (Tests der Funktionsart, Tests der sicherheitsbezogenen Steuerungsfunktion, Tests jedes Elements der Spezifikation usw.).

Die Verifikation einer neuen Softwareversion sollte Nicht-Regressions-Tests einschließen.

ANMERKUNG Nicht-Regressions-Tests werden verwendet, um sicherzustellen, dass die Modifikationen der Software das Verhalten der Software nicht in irgendeiner unerwarteten Weise geändert haben.

C.9.2 Verifikation der Softwarespezifikation: Tests zur Validierung

Der Sinn dieser Verifikationen ist es, Fehler zu erkennen, die mit der Software in der Zielsystemumgebung in Verbindung stehen. Fehler, die durch diese Art der Verifikation erkannt werden, sind zum Beispiel folgende: jeder falsche Mechanismus zur Behandlung von Unterbrechungen, ungenügende Rücksichtnahme auf Laufzeitanforderungen, falsche Reaktion der Software, die in einer vorübergehenden Betriebsart läuft (Einschalten, Eingangsfluss, Umschaltung in eine abgestufte Betriebsart usw.), Konflikte im Zugriff auf verschiedene Ressourcen oder Organisationsprobleme im Speicher, Unfähigkeit der integrierten Tests Fehler zu erkennen, Software/Hardware-Schnittstellenfehler, Stacküberläufe. Die Tests zur Validierung sind die wichtigsten Bestandteile zur Verifikation der Softwarespezifikation.

Die Testabdeckung sollte in einer Nachweis-Matrix deutlich gemacht werden und sicherstellen, dass:

– jedes Element der Spezifikation einschließlich Sicherheitsmechanismen von einem Test zur Validierung abgedeckt wird und
– das Realzeitverhalten der Software in jeder Betriebsart verifiziert werden kann.

Darüber hinaus sollte die Validierung unter repräsentativen Betriebsbedingungen des SRECS oder des SRECS-Teilsystems durchgeführt werden.

ANMERKUNG 1 Dies garantiert, dass die Software wie im Betrieb erwartet reagiert. Es trifft nur für Fälle zu, in denen die Testbedingungen zur Zerstörung der Hardware führen können (z. B. physikalischer Fehler eines Bauteils, der nicht simuliert werden kann). Damit die Validierung aussagekräftig ist, sollte sie unter den Betriebsbedingungen des SRECS oder des SRECS-Teilsystems ausgeführt werden (d. h. mit den endgültigen Versionen von Software und Hardware mit auf dem Zielsystem installierter Software). Jede andere Kombination kann die Wirksamkeit des Tests vermindern und eine Analyse erfordern, ob sie repräsentativ ist.

Die Ergebnisse der Validierung sollten in einem Bericht zur Validierung aufgezeichnet werden, der zumindest die folgenden Punkte umfassen sollte:

– die Versionen der Software und des Systems, die validiert wurden;
– eine Beschreibung der ausgeführten Tests zur Validierung (Eingänge, Ausgänge, Testverfahren);
– die zur Validierung oder Auswertung der Ergebnisse verwendeten Werkzeuge und Einrichtungen;
– die Ergebnisse, die aussagen, ob jeder Test zur Validierung erfolgreich war oder ein Ausfall vorliegt;
– eine Beurteilung der Validierung: aufgedeckte Nichtkonformitäten, Einfluss auf die Sicherheit, Entscheidung, ob die Validierung akzeptiert wird oder nicht.

Für jede ausgelieferte Softwareversion sollte ein Bericht zur Validierung vorliegen, und er sollte sich auf die endgültige Version jedes ausgelieferten Softwareelements beziehen.

ANMERKUNG 2 Dieser Bericht kann als Nachweis vorgesehen werden, dass Tests tatsächlich durchgeführt wurden und dass die Ergebnisse korrekt waren (oder erklärbare Abweichungen enthalten sind). Er kann auch dazu verwendet werden, Tests zu einem späteren Zeitpunkt nochmals auszuführen oder lässt sich für eine zukünftige Softwareversion oder ein anderes Projekt nutzen. Er liefert eine Garantie, dass jede ausgelieferte Version in ihrer endgültigen Ausführung validiert worden ist. Auf der anderen Seite zwingt er nicht zu einer kompletten Validierung jeder Modifikation eines vorhandenen Codes – eine Einflussanalyse kann in bestimmten Fällen eine teilweise Validierung rechtfertigen.

C.9.3 Verifikation des Softwareentwurfs: Software-Integrationstests

Diese Verifikation konzentriert sich auf die korrekte Zusammenstellung der Softwaremodule und auf die gegenseitigen Beziehungen zwischen Softwarekomponenten. Sie kann verwendet werden, um Fehler folgender Art aufzudecken: fehlerhafte Initialisierung von Variablen und Konstanten, Fehler im Transfer von Parametern, jegliche Datenveränderung besonders globaler Daten, falscher Ablauf von Ereignissen und Operationen.

Software-Integrationstests sollten fähig sein, Folgendes zu verifizieren:

– korrekter Ablauf der Ausführung der Software;
– Datenaustausch zwischen Modulen;
– Betrachtung der Kriterien zur Leistungsfähigkeit;
– Nichtänderung von globalen Daten.

Die Testabdeckung sollte in einer Nachweis-Matrix deutlich gemacht werden, die den Zusammenhang zwischen den auszuführenden Tests und den Zielen der definierten Tests veranschaulicht.

Die Ergebnisse der Integrationstests sollten in einem Bericht zum Software-Integrationstest aufgezeichnet werden, der zumindest folgende Punkte enthält:

– die Version der integrierten Software;
– eine Beschreibung der ausgeführten Tests (Eingaben, Ausgaben, Verfahren);
– die Ergebnisse der Integrationstests und ihre Bewertung.

C.9.4 Verifikation des Detailentwurfs: Modultests

Modultests konzentrieren sich auf Softwaremodule und ihre Konformität mit dem detaillierten Entwurf. Diese Aktivität kann für umfassende und komplexe Softwareelemente unabdingbar sein, wird aber nur für die hier betrachteten kleinen Softwareelemente empfohlen. Diese Phase des Verifikationsverfahrens erlaubt die Erkennung von folgenden Arten von Fehlern:

– Unfähigkeit eines Algorithmus, die Softwarespezifikationen zu erfüllen;
– fehlerhafte Schleifenoperationen;
– falsche logische Entscheidungen;
– Unfähigkeit, gültige Kombinationen von Eingangsdaten korrekt zu berechnen;
– falsche Antworten auf fehlende oder geänderte Eingangsdaten;
– Verletzung von Feldgrenzen;
– fehlerhafte Berechnung von Abläufen;
– ungenügende Genauigkeit;
– Genauigkeit oder Leistungsfähigkeit eines Algorithmus.

Jedes Softwaremodul sollte einer Reihe von Tests unter Verwendung von Eingangsdaten unterworfen werden, um zu verifizieren, dass das Modul die auf der Stufe des Detailentwurfs spezifizierten Funktionen erfüllt.

Die Testabdeckung sollte in einer Nachweis-Matrix angegeben werden, die den Zusammenhang zwischen den Testergebnissen und den Zielen der definierten Tests veranschaulicht.

Anhang D
(informativ)

Ausfallarten elektrischer/elektronischer Bauteile

Die Betriebsumgebung für ein SRECS und seine Teilsysteme sollte als Minimum der in IEC 60204-1 beschriebenen Betriebsumgebung entsprechen. In Praxis genügen jedoch viele Teilsysteme einer Produktnorm (z. B. AOPD), in der eine Betriebsumgebung mit erhöhten Anforderungen festgelegt sein kann.

Die in Tabelle D.1 angegebenen Informationen sind Beispiele von Anteilen an Ausfallarten für elektrische/ elektronische Bauteile, die aus den angegebenen Referenzquellen abgeleitet sind. Diese Werte können sich von den in anderen Quellen angegebenen Werten unterscheiden. Im Allgemeinen sollten die verwendeten Daten zu Ausfallarten die praktische Anwendung der Bauteile widerspiegeln.

ANMERKUNG 1 Die folgende Tabelle stellt keine vollständige Liste von Bauteilausfallarten dar.

ANMERKUNG 2 Daten zu Ausfallarten sollten vom Hersteller eines Teilsystems zur Verfügung gestellt werden.

Tabelle D.1 – Beispiele für Anteile von Ausfallarten für elektrische/elektronische Bauteile

Bauteil	Ausfallart	Typischer Anteil an der Ausfallart %
Schalter mit zwangläufiger Öffnung bei Anforderung, zum Beispiel Drucktaster, Not-Aus-Taster, Positionsschalter, Nockenschalter, Betriebsartenwahlschalter	Nichtöffnen von Kontakten	20
	Nichtschließen von Kontakten	80
Elektromechanische Positionsschalter, Grenzschalter, handbetätigte Schalter usw. (keine zwangläufige Öffnung bei Anforderung)	Nichtöffnen von Kontakten	50
	Nichtschließen von Kontakten	50
Relais	alle Kontakte verbleiben im angezogenen Zustand, wenn die Spule entregt ist	25
	alle Kontakte verbleiben im nicht angezogenen Zustand, wenn die Spule erregt ist	25
	Nichtöffnen von Kontakten	10
	Nichtschließen von Kontakten	10
	gleichzeitiger Kurzschluss zwischen drei Kontakten eines Wechselkontaktes	10
	gleichzeitiges Geschlossensein von Schließer- und Öffnerkontakten	10
	Kurzschluss zwischen zwei Kontaktpaaren und/oder zwischen Kontakten und Spulenklemme	10

Bauteil	Ausfallart	Typischer Anteil an der Ausfallart %
Leistungsschalter, differenzieller Leistungs-schalter, Fehlerstromschutzschalter	alle Kontakte verbleiben im angezogenen Zustand, wenn die Spule entregt ist	25
	alle Kontakte verbleiben im nicht angezogenen Zustand, wenn die Spule erregt ist	25
	Nichtöffnen von Kontakten	10
	Nichtschließen von Kontakten	10
	gleichzeitiger Kurzschluss zwischen drei Kontakten eines Wechselkontaktes	10
	gleichzeitiges Geschlossensein von Schließer- und Öffnerkontakten	10
	Kurzschluss zwischen zwei Kontaktpaaren und/oder zwischen Kontakten und Spulenklemme	10
Schütz	alle Kontakte verbleiben im angezogenen Zustand, wenn die Spule entregt ist	25
	alle Kontakte verbleiben im nicht angezogenen Zustand, wenn die Spule erregt ist	25
	Nichtöffnen von Kontakten	10
	Nichtschließen von Kontakten	10
	gleichzeitiger Kurzschluss zwischen drei Kontakten eines Wechselkontaktes	10
	gleichzeitiges Geschlossensein von Schließer- und Öffnerkontakten	10
	Kurzschluss zwischen zwei Kontaktpaaren und/oder zwischen Kontakten und einer Spulenklemme	10
Sicherung	kein Durchbrennen (Kurzschluss)	10
	Unterbrechung	90
Näherungsschalter	Ausgang dauernd niederohmig	25
	Ausgang dauernd hochohmig	25
	Unterbrechung der Energieversorgung	30
	Nichtbetätigen des Schalters infolge eines mechanischen Ausfalls	10
	gleichzeitiger Kurzschluss zwischen drei Anschlüssen eines Wechselkontaktes	10

Bauteil	Ausfallart	Typischer Anteil an der Ausfallart %
Temperaturschalter	Nichtschließen von Kontakten	30
	Nichtöffnen von Kontakten	10
	Kurzschlüsse zwischen benachbarten Kontakten	10
	gleichzeitiger Kurzschluss zwischen drei Anschlüssen von Wechselkontakten	10
	fehlerhafter Sensor	20
	Änderung des Schaltpunktes oder der Ausgangscharakteristik	20
Druckschalter	Nichtschließen von Kontakten	30
	Nichtöffnen von Kontakten	10
	Kurzschlüsse zwischen benachbarten Kontakten	10
	gleichzeitiger Kurzschluss zwischen drei Anschlüssen von Wechselkontakten	10
	fehlerhafter Sensor	20
	Änderung des Schaltpunktes oder der Ausgangscharakteristik	20
Magnetventil	Nicht-Anzug	5
	Nicht-Abfall	15
	Veränderung der Schaltzeiten	5
	Leckage	65
	andere Ausfallarten (siehe Anmerkung 4)	10
Transformator	Unterbrechung einzelner Wicklungen	70
	Kurzschluss zwischen verschiedenen Wicklungen	10
	Kurzschluss in einer Wicklung	10
	Veränderung des wirksamen Windungsverhältnisses	10
Induktivitäten	Unterbrechung	80
	Kurzschluss	10
	zufällige Änderung des Wertes	10
Widerstände	Unterbrechung	80
	Kurzschluss	10
	zufällige Änderung des Wertes	10
Widerstandsnetzwerke	Unterbrechung	70
	Kurzschluss	10
	Kurzschluss zwischen beliebigen Anschlüssen	10
	zufällige Änderung des Wertes	10

Bauteil	Ausfallart	Typischer Anteil an der Ausfallart %
Potentiometer	Unterbrechung einzelner Anschlüsse	70
	Kurzschluss zwischen allen Anschlüssen	10
	Kurzschluss zwischen zwei beliebigen Anschlüssen	10
	zufällige Änderung des Wertes	10
Kondensatoren	Unterbrechung	40
	Kurzschluss	40
	zufällige Änderung des Wertes	10
	Veränderung des Wertes tan α	10
Diskrete Halbleiter	Unterbrechung eines einzelnen Anschlusses	25
	Kurzschluss zwischen zwei beliebigen Anschlüssen	25
	Kurzschluss zwischen allen Anschlüssen	25
	Änderung der Charakteristika	25
Nicht programmierbare integrierte Schaltkreise (nicht komplex, d. h. weniger als 1 000 Gatter und/oder weniger als 24 Anschlüsse, Operationsverstärker, Schieberegister und Hybridmodule)	Unterbrechung eines einzelnen Anschlusses	20
	Kurzschluss zwischen zwei beliebigen Anschlüssen	20
	„Stuck at"-Fehler	20
	parasitäre Oszillation der Ausgänge	20
	Änderung von Kennwerten (z. B. Eingangs-/ Ausgangsspannung analoger Einrichtungen)	20
Optokoppler	Unterbrechung eines einzelnen Anschlusses	30
	Kurzschluss zwischen zwei beliebigen eingangsseitigen Anschlüssen	30
	Kurzschluss zwischen zwei beliebigen ausgangsseitigen Anschlüssen	30
	Kurzschluss zwischen zwei beliebigen Anschlüssen des Ein- und Ausgangs	10
Stecker und Buchse, mehrpolige Steckverbindungen	Kurzschluss zwischen zwei beliebigen benachbarten Steckerstiften	10
	Kurzschluss eines beliebigen Leiters zu einem ungeschützten leitfähigen Teil	10
	Unterbrechung einzelner Steckerstifte	80
Klemmstellen	Kurzschluss zwischen benachbarten Klemmen	10
	Unterbrechung einzelner Klemmen	90

ANMERKUNG 1 Diese Daten wurden aus mehreren industriellen Quellen einschließlich der folgenden hergeleitet:

MIL-HDBK 217F(Notice 2) Reliability Prediction of Electronic Equipment (28-02-95), Parts Stress Analysis

MIL-HDBK 217F(Notice 2) Reliability Prediction of Electronic Equipment (28-02-95), Appendix A, Parts Count Reliability Prediction

SN 29500 Part 7, Failure Rates of Components, Expected Values for Relays, April 1992

SN 29500 Part 11, Failure Rates of Components, Expected Values for Contactors, August 1990

Die Dokumente der Reihe SN 29500 sind öffentlich verfügbar und können bezogen werden von:

Siemens AG, CT SR SI

Otto-Hahn-Ring 6

D-81739 München

ANMERKUNG 2 Elektrische Ausfallarten sind der Tabelle D.5 von ISO 13849-2 entnommen. Mechanische Ausfallarten (soweit zutreffend) stammen aus den Anhängen A, B und C von ISO 13849-2.

ANMERKUNG 3 Einige elektrische/elektronische Bauteile, zum Beispiel Widerstände und Kondensatoren, können für verschiedene Ausführungen andere Verteilungen von Ausfallarten im Unterschied zu den in der Tabelle angegebenen haben.

ANMERKUNG 4 Andere Ausfallarten, die für ein Magnetventil zutreffen, schließen ein:

– Nichtschalten (Hängen bleiben in der End- oder Nulllage) oder nicht vollständiges Schalten (Hängen bleiben in einer beliebigen Zwischenstellung);
– selbsttätige Veränderung der Ausgangsschaltstellung (ohne ein Eingangssignal);
– Änderung der Leckageflussrate über eine lange Zeitdauer;
– Bersten des Ventilgehäuses oder Bruch des/der bewegten Bauteils/Baugruppen sowie Bruch der Befestigungs- oder Gehäuseschrauben;
– pneumatische/hydraulische Fehler, die unkontrolliertes Verhalten von Servo- und Proportionalventilen bewirken.

ANMERKUNG 5 Andere Informationsquellen zu Daten von Ausfallraten und Anteilen an der Ausfallart sind zum Beispiel:

– UTE C 80-810 RDF 2000: Reliability data handbook – A universal model for reliability prediction of electronic components, PCBs und equipments

Failure mode/mechanism distributions FMD-91, RAC 1991

Anhang E
(informativ)

Elektromagnetische (EM) Phänomene und erhöhte Störfestigkeitsgrade für SRECS, die für den Gebrauch im Industriebereich nach IEC 61000-6-2 vorgesehen sind

Tabelle E.1 – EM-Phänomene und erhöhte Störfestigkeitsgrade für SRECS

Anschluss (siehe Anmerkung 1)	**Phänomen**	**Basisnorm**	**Erhöhte Werte für zusätzliche Prüfungen der Leistungsfähigkeit des SRECS (siehe 6.4.3)**
Gehäuse	Entladung statischer Elektrizität (ESD)	IEC 61000-4-2	6 kV/8 kV Kontakt-/Luftentladung (siehe Anmerkung 2)
	hochfrequente elektromagnetische (EM) Felder	IEC 61000-4-3	20 V/m (80 MHz bis 1 GHz) 6 V/m (1,4 GHz bis 2 GHz) 3 V/m (2 GHz bis 2,7 GHz) (siehe Tabelle E.2 und Anmerkung 3)
	Magnetfeld mit energietechnischer Frequenz	IEC 61000-4-8	30 A/m (siehe Anmerkungen 4 und 5)
Wechselspannungs-versorgung (AC)	Spannungseinbrüche/Kurzzeit-unterbrechungen	IEC 61000-4-11	0,5 Perioden, 30 % Reduzierung (siehe Anmerkung 5)
	Spannungsschwankungen/Unter-brechungen	IEC 61000-4-11	250 Perioden, > 95 % Reduzierung (siehe Anmerkung 5)
	schnelle transiente elektrische Störgrößen (Burst)	IEC 61000-4-4	4 kV
	Stoßspannungen (Surge)	IEC 61000-4-5	2 kV Leitung zu Leitung / 4 kV Leitung nach Masse (siehe Anmerkung 6)
	leitungsgeführte Störgrößen, induziert durch hochfrequente Felder	IEC 61000-4-6	10 V bei den angegebenen Frequenzen (siehe Tabelle E.3 und Anmerkung 3)
Gleichspannungs-versorgung (DC) (siehe Anmerkung 7)	schnelle transiente elektrische Störgrößen (Burst)	IEC 61000-4-4	4 kV
	Stoßspannungen (Surge)	IEC 61000-4-5	1 kV Leitung zu Leitung / 2 kV Leitung nach Masse (siehe Anmerkung 6)
	leitungsgeführte Störgrößen, induziert durch hochfrequente Felder	IEC 61000-4-6	10 V bei den angegebenen Frequenzen (siehe Tabelle E.3 und Anmerkung 3)
E/A-Signal-/ Steuerleitungen	schnelle transiente elektrische Störgrößen (Burst)	IEC 61000-4-4	2 kV für Leitungen > 3 m
	Stoßspannungen (Surge)	IEC 61000-4-5	2 kV Leitung nach Masse (siehe Anmerkung 8)
	leitungsgeführte Störgrößen, induziert durch hochfrequente Felder	IEC 61000-4-6	10 V bei den angegebenen Frequenzen (siehe Tabelle E.3 und Anmerkung 3)
Funktionserde	schnelle transiente elektrische Störgrößen (Burst)	IEC 61000-4-4	2 kV

ANMERKUNG 1 Ein Anschluss ist eine spezielle Schnittstelle des SRECS und seiner Teilsysteme zur externen elektromagnetischen Umgebung.

ANMERKUNG 2 Schärfegrade müssen in Übereinstimmung mit den in IEC 61000-4-2 beschriebenen Umgebungsbedingungen für Teile angewendet werden, die von anderen Personen als dem Betriebspersonal in Übereinstimmung mit festgelegten Verfahren zur Beherrschung von ESD berührt werden können. Dies gilt jedoch nicht für Einrichtungen, für die der Zugang nur auf angemessen geschultes Personal beschränkt ist.

ANMERKUNG 3 Die erhöhten Werte müssen in Frequenzbereichen angewendet werden, die im Allgemeinen für digitale Mobilfunksender verwendet werden, mit Ausnahme dort, wo zuverlässige Maßnahmen verwendet werden, um elektromagnetische Beeinflussung solcher Einrichtungen zu verhindern. ISM-Frequenzen müssen individuell in Betracht gezogen werden.

ANMERKUNG 4 Nur für magnetisch empfindliche Einrichtungen.

ANMERKUNG 5 Ein erhöhter Wert wird nicht auf Phänomene angewendet, wo dies nicht als notwendig für die funktionale Sicherheit betrachtet wird.

ANMERKUNG 6 Externe Schutzvorrichtungen sind erlaubt, um Immunität zu erreichen.

ANMERKUNG 7 DC-Anschlüsse zwischen Teilen von Einrichtungen/Systemen, die nicht mit einem DC-Verteilungsnetzwerk verbunden sind, werden als E/A-Signal-/Steueranschlüsse behandelt.

ANMERKUNG 8 Nur im Fall von langen Leitungen.

ANMERKUNG 9 Referenz IEC 61326-3 (in Vorbereitung).

ANMERKUNG 10 Wo eine Produktnorm (z. B. IEC 61496-1) andere Prüfschärfegrade für spezielle EMV-Phänomene im Zusammenhang mit funktionaler Sicherheit festlegt, gelten diese anderen Prüfschärfegrade für diese SRECS-Teilsysteme.

Tabelle E.2 – Ausgewählte Frequenzen für HF-Feld-Prüfungen

System	Frequenz
GSM	890 bis 915 MHz
GSM	1 710 bis 1 785 MHz
GSM	1 890 MHz
UMTS	noch festzulegen
Sprechfunk	noch festzulegen
ISM	433,05 bis 434,79 MHz
ISM ???	83,996 bis 84,004 MHz
ISM ???	167,992 bis 168,008 MHz
ISM ???	886,000 bis 906,000 MHz

Tabelle E.3 – Ausgewählte Frequenzen für Prüfungen leitungsgeführter HF

System	Frequenz
ISM	6,765 bis 6,795 MHz
ISM	13,553 bis 13,567 MHz
ISM	26,957 bis 27,283 MHz
ISM	40,66 bis 40,70 MHz

Anhang F
(informativ)

Methodologie zur Abschätzung der Anfälligkeit gegenüber Ausfällen in Folge gemeinsamer Ursache (CCF)

F.1 Allgemeines

Dieser informative Anhang stellt einen einfachen qualitativen Ansatz für die Abschätzung von CCF bereit, der auf den Entwurf von Teilsystemen angewendet werden kann.

F.2 Methodologie

Der vorgesehene Entwurf eines Teilsystems sollte beurteilt werden, um die Wirksamkeit der verwendeten Maßnahmen zum Schutz gegenüber CCF festzustellen. Die anwendbaren Punkte in der Tabelle F.1 sollten identifiziert, und es sollte eine Gesamtpunktzahl festgestellt werden. Diese wird verwendet, um den Faktor der Ausfälle in Folge gemeinsamer Ursache aus Tabelle F.2 als Prozentwert zu bestimmen.

Tabelle F.1 – Kriterien zur Bestimmung von CCF

Merkmal	Referenz	Punkte
Trennung/Isolierung		
Sind SRECS-Signalkabel für die einzelnen Kanäle an allen Stellen getrennt von anderen Kanälen geführt oder ausreichend geschützt?	1a	5
Ist die Erkennung von Signalübertragungsfehlern bei Verwendung von Informationscodierung/ -decodierung ausreichend?	1b	10
Sind SRECS-Signalkabel und elektrische Energieversorgungskabel an allen Stellen getrennt oder ausreichend geschützt?	2	5
Werden Teilsystem-Elemente als physikalisch getrennte Einheiten in eigenen lokalen Gehäusen vorgesehen, wenn sie zu einem CCF beitragen können?	3	5
Diversität/Redundanz		
Werden in dem Teilsystem verschiedene elektronische Technologien verwendet, zum Beispiel einmal Elektronik oder programmierbare Elektronik und andererseits ein elektromechanisches Relais?	4	8
Werden in dem Teilsystem Elemente verwendet, die verschiedene physikalische Prinzipien nutzen (z. B. Erfassungselemente an einer Schutztür, die mechanische und magnetische Erfassungsverfahren verwenden)?	5	10
Werden in dem Teilsystem Elemente mit unterschiedlichem Zeitverhalten in Bezug auf funktionalen Betrieb und/oder Ausfallarten verwendet?	6	10
Haben die Teilsystem-Elemente ein Diagnose-Testintervall von ≤ 1 min?	7	10
Komplexität/Entwurf/Anwendung		
Ist die Querverbindung zwischen Kanälen des Teilsystems verhindert mit Ausnahme der Querverbindungen, die für Diagnosezwecke verwendet werden?	8	2
Beurteilung/Analyse		
Sind die Ergebnisse der Ausfallarten- und Auswirkungsanalyse ausgewertet worden, um Quellen von Ausfällen in Folge gemeinsamer Ursache festzustellen und sind zuvor bestimmte derartige Quellen durch den Entwurf beseitigt worden?	9	9
Werden Feldausfälle analysiert und in den Entwurfsprozess zurückgemeldet?	10	9
Kompetenz/Training		
Verstehen die Entwickler der Teilsysteme die Gründe für und Auswirkungen von Ausfällen in Folge gemeinsamer Ursache?	11	4
Überwachung der Umgebungsbedingungen		
Arbeiten die Teilsystem-Elemente wahrscheinlich immer auch ohne äußere Überwachung der Umgebungsbedingungen innerhalb des Temperatur-, Feuchte-, Korrosions-, Staub- und Vibrationsbereiches usw. in dem es geprüft worden ist?	12	9
Ist das Teilsystem gegen die nachteiligen Einflüsse durch elektromagnetische Beeinflussung immun bis zu und einschließlich der in Anhang E festgelegten Grenzen?	13	9
ANMERKUNG In Tabelle F.1 ist ein alternatives Merkmal (z. B. Referenzen 1a und 1b) dort aufgeführt, wo es vorgesehen ist, dass eine Berücksichtigung des Beitrags zur Vermeidung von CCF nur für das am meisten relevante Merkmal erfolgt.		

Bei der Anwendung der Tabelle F.1 sollten diejenigen Punkte, die als den Entwurf des Teilsystems beeinflussend betrachtet werden, zusammengezählt werden, um eine Gesamtpunktzahl für den auszuführenden Entwurf zu erhalten. Wo gezeigt werden kann, dass gleichwertige Mittel zur Vermeidung von CCF durch die Verwendung von speziellen Entwurfsmaßnahmen (z. B. die Verwendung von opto-entkoppelten Geräten im Gegensatz zu geschirmten Kabeln) erreicht werden können, kann die zutreffende Punktzahl beansprucht werden, da dies so betrachtet werden kann, als dass sich der gleiche Beitrag zur Vermeidung von CCF ergibt.

Diese Gesamtpunktzahl kann unter Anwendung der Tabelle F.2 dazu verwendet werden, einen Faktor der Ausfälle in Folge gemeinsamer Ursache (β) zu bestimmen.

Tabelle F.2 – Abschätzung des CCF-Faktors (β)

Gesamtpunktzahl	Faktor der Ausfälle in Folge gemeinsamer Ursache (β)
< 35	10 % (0,1)
35 bis 65	5 % (0,05)
65 bis 85	2 % (0,02)
85 bis 100	1 % (0,01)

Der hergeleitete Wert von β sollte, wie in 6.7.8.1 gefordert, bei der Abschätzung der Wahrscheinlichkeit gefahrbringender Ausfälle verwendet werden.

Anhang ZA
(normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod), dann gilt die entsprechende EN oder das HD.

Publikation	Jahr	Titel	EN/HD	Jahr
IEC 60204-1	–[4)]	Safety of machinery – Electrical equipment of machines Part 1: General requirements	EN 60204-1 + Corr. September	1997[5)] 1998
IEC 61000-6-2, mod.	–[4)]	Electromagnetic compatibility (EMC) Part 6-2: Generic standards – Immunity for industrial environments	EN 61000-6-2	2001[5)]
IEC 61310	Reihe	Safety of machinery – Indication, marking and actuation	EN 61310	Reihe
IEC 61508-2	–[4)]	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2001[5)]
IEC 61508-3	–[4)]	Part 3: Software requirements	EN 61508-3	2001[5)]
ISO 12100-1	2003	Safety of machinery Basic concepts, general principles for design Part 1: Basic terminology, methodology	EN ISO 12100-1	2003
ISO 12100-2	2003	Basic concepts, general principles for design Part 2: Technical principles	EN ISO 12100-2	2003
ISO 13849-1	1999	Safety of machinery – Safety-related parts of control systems Part 1: General principles for design	–	–
ISO 13849-2	2003	Part 2: Validation	EN ISO 13849-2	2003
ISO 14121	–[4)]	Safety of machinery Principles of risk assessment	–	–

[4)] Undatierte Verweisung.

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

Anhang ZZ
(informativ)

Zusammenhang mit grundlegenden Anforderungen von EG-Richtlinien

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

– 1.2.1;

– 1.2.7.

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

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