

	Sicherheit von Maschinen Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren Steuerungen von Maschinen (IEC 44/380/CD:2002)	DIN IEC 62061
VDE	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Vorstand beschlossenen Genehmigungsverfahrens unter nebenstehenden Nummern in das VDE-Vorschriftenwerk aufgenommen und in der etz Elektrotechnische Zeitschrift bekannt gegeben worden.	Klassifikation VDE 0113 Teil 50
ICS 13.110; 25.040.40; 35.240.50 Einsprüche bis 2003-07-31 Entwurf Safety of machinery – Functional safety of electrical, electronic and programmable control systems for machinery; (IEC 44/380/CD:2002) Anwendungswarnvermerk Dieser Norm-Entwurf wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt. Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren. Stellungnahmen werden erbeten – vorzugsweise als Datei per E-Mail an dke@vde.com in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden – oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main. Das internationale Schriftstück IEC 44/380/CD:2002-05 „62061: Safety of machinery – Functional safety of electrical, electronic and programmable control systems for machinery“ ist unverändert in diesen deutschen Norm-Entwurf übernommen worden. Beginn der Gültigkeit Diese Norm gilt ab ... Fortsetzung Seite 2 bis 98 und 89 Seiten IEC-Original DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Nationales Vorwort

Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung des Internationalen Norm-Entwurfs [Committee Draft (CD)] IEC 44/380/CD:2002 „62061: Safety of machinery - Functional safety of electrical, electronic and programmable control systems for machinery“.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den mit aufgenommenen englischen IEC-Text.

Der Internationale Entwurf wurde vom TC 44 „Safety of machinery - Electrotechnical aspects“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als CD herausgegeben. Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene entstandener Internationaler Norm-Entwurf im Schlusstadium [Final Draft International Standard (FDIS)] zeitgleich (parallel) bei IEC und CENELEC zur Abstimmung gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen.

Da der Abstimmungszeitraum für einen FDIS nur 2 Monate beträgt, und zum FDIS keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit noch vor der Abstimmung berücksichtigen zu können.

Für den vorliegenden Norm-Entwurf 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.

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf eine Norm oder andere Unterlage 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 oder anderen Unterlage.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe der Norm oder anderen Unterlage.

Eine Information über den Zusammenhang der zitierten Normen und anderen Unterlagen mit den entsprechenden Deutschen Normen und anderen Unterlagen ist nachstehend wiedergegeben. oder anderen Unterlage

IEC hat 1997 die Benummerung der IEC-Publikationen geändert. Zu den bisher verwendeten Normnummern wird jeweils 60000 addiert. So ist zum Beispiel aus IEC 68 nun IEC 60068 geworden.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
prEN ISO/FDIS 12100-1:200X	–	–	–
prEN ISO/FDIS 12100-2:200X	–	–	–
–	ISO 13121:200X	–	–
–	IEC 60204-1:200X	–	–
EN 61508-1:2001	IEC 61508-1:1998	DIN EN 61508-1 (VDE 0803 Teil 1):2002-11	VDE 0803 Teil 1
EN 61508-4:2001	IEC 61508-4:1998	DIN EN 61508-4 (VDE 0803 Teil 4):2002-11	VDE 0803 Teil 4

Nationaler Anhang NB (informativ)

Literaturhinweise

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

DIN EN 61508-4 (VDE 0803 Teil 4):2002-11, *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.*

Deutsche Übersetzung

Sicherheit von Maschinen
Funktionale Sicherheit von elektrischen, elektronischen
und programmierbaren Steuerungen von Maschinen

	Seite
Einleitung	7
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe und Abkürzungen	12
3.1 Begriffe	12
3.2 Abkürzungen	18
4 Management der funktionalen Sicherheit	18
4.1 Zweck	18
4.2 Anforderungen	18
5 Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen	19
5.1 Zweck	19
5.2 Spezifikation der Anforderungen für sicherheitsbezogene Steuerungsfunktionen	20
6 Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems	22
6.1 Zweck	22
6.2 Allgemeine Anforderungen	22
6.3 Anforderungen zum Verhalten (des SRECS) bei Erkennung eines Fehlers im SRECS	23
6.4 Anforderungen zur systematischen Sicherheitsintegrität	24
6.5 Auswahl eines sicherheitsbezogenen elektrischen Steuerungssystems	25
6.6 Entwurf und Entwicklung eines sicherheitsbezogenen elektrischen Steuerungssystems (SRECS)	25
6.7 Realisierung von Teilsystemen	31
6.8 Realisierung von Diagnosefunktionen	47
6.9 Hardware-Implementierung	47
6.10 Spezifikation der Software-Sicherheitsanforderungen	48
6.11 Software-Entwurf und Entwicklung	49
6.12 Integration und Test des sicherheitsbezogenen elektrischen Steuerungssystems	55
7 Benutzerinformationen des SRECS	58
7.1 Allgemeines	58
7.2 Technische Dokumentation	58
7.3 Dokumentation für die Instandhaltung	58
8 Validierung des sicherheitsbezogenen elektrischen Steuerungssystems	59
8.1 Allgemeine Anforderungen	59
8.2 Anforderungen zur systematischen Sicherheitsintegrität während der Validierung des SRECS	59
9 Modifikation	61

	Seite
9.1 Zweck	61
9.2 Modifikationsverfahren	61
10 Dokumentation	61
10.1 Die Dokumentation muss:	61
Anhang A (informativ) Bestimmung des SILs Methodologie zur Bestimmung erforderlicher Sicherheits-Integritätslevels (SILs)	63
A.1 Einleitung	63
A.2 Geplante Verwendung der Methodologie	63
A.3 Integration in den Rahmen von prEN ISO/FDIS 12100	63
A.4 Grenzen dieser Methodologie	64
A.5 Verwendung der Methodologie zur Bestimmung des SILs	64
A.5.1 Einleitung	64
A.5.2 Überblick	64
A.5.3 Schritt 1: Vorbereitung	64
A.5.4 Schritt 2: Analyse und Abbildung von Sicherheitsfunktionen (Formblatt A.1)	65
A.5.5 Schritt 3: Typ der durch ein SRECS auszuführenden sicherheitsbezogenen Steuerungsfunktion (Formblatt A.2 oder Formblatt A.5)	66
A.5.6 Schritt 4: Begriffe möglicher Unfallszenarien (Typ M1)	66
A.5.7 Schritt 5: Häufigkeiten möglicher Unfälle und Folgen (Formblatt A.3)	66
A.5.8 Schritt 6: Formblatt A.4	70
A.5.9 Schritt 7: Betrachtung aller Umstände der Verwendung und Personentypen	70
A.5.10 Schritt 8: Begriffe möglicher Unfallszenarien (Typ M2) (siehe Formblatt A.5)	70
A.5.11 Schritt 9: Häufigkeit des möglichen Unfallszenarios (siehe Formblatt A.6)	70
A.5.12 Schritt 10: Zugewiesener SIL	71
A.5.13 Schritt 11	71
A.5.14 Schritt 12: Plausibilitätskontrolle ("Sind die Ergebnisse vernünftig?")	71
Anhang B (informativ)	84
Anhang C (informativ) Entwurf und Entwicklung von Embedded-Software	85
C.1 Einleitung	85
C.2 Software-Produktanforderungen	85
C.2.1 Schnittstelle mit der Systemarchitektur	85
C.2.2 Softwarespezifikationen	86
C.2.3 Vorhandene Software	86
C.2.4 Softwareentwurf	87
C.2.5 Codierung	87
C.3 Software-Entwicklungsprozessanforderungen	87
C.3.1 Entwicklungsprozess: Software-Lebenszyklusanforderungen	87
C.3.2 Dokumentation: Anforderungen zum Dokumentationsmanagement	88
C.3.3 Konfiguration und Management der Softwaremodifikationen	88
C.3.4 Anforderungen zum Konfigurations- und Archivierungsmanagement	88

	Seite
C.3.5 Management der Softwaremodifikationen.....	89
C.4 Werkzeuge: Anforderungen zu Entwicklungswerkzeugen.....	89
C.5 Anforderungen zur externen Auftragsvergabe	89
C.6 Reproduktion, Lieferung.....	90
C.6.1 Anforderungen zum Schutz des ausführbaren Codes	90
C.6.2 Anforderungen zur Softwareinstallation und Inbetriebnahme	90
C.7 Anforderungen zur Verifikation und Validierung der Software	90
C.8 Allgemeine Anforderungen zur Verifikation und Validierung.....	90
C.9 Verifikationsanforderungen: Anforderungen zur Überprüfung	91
C.10 Anforderungen zum Softwaretest.....	91
C.10.1 Allgemeine Validierungsanforderungen	91
C.10.2 Verifikationsanforderungen zur Softwarespezifikation: Tests zur Validierung	91
C.10.3 Verifikationsanforderungen zum Softwareentwurf: Software-Integrationstests	92
C.10.4 Verifikationsanforderungen zum Detailentwurf: Modultests.....	93
Anhang D (informativ).....	94
Anhang E (informativ) Ausfallarten elektrischer/elektronischer Bauteile	95

Einleitung

Als ein Ergebnis der Automatisierung, der Forderung nach gesteigerter Produktion und reduziertem körperlichen Aufwand des Benutzers, spielen elektrische Steuerungssysteme von Maschinen eine zunehmende Rolle in der Maschinengesamtsicherheit. Weiterhin verwenden die Steuerungssysteme 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 keine Akzeptanz Elektronik und besonders programmierbare Elektronik in sicherheitsbezogenen Funktionen für signifikante Maschinengefährdungen einzusetzen.

Diese Internationale Norm beschreibt einen Lösungsweg für sicherheitsbezogene Betrachtungen von elektrischen, elektronischen und programmierbar elektronischen Steuerungssystemen von Maschinen und beschreibt Anforderungen zum Erreichen der notwendigen Leistungsfähigkeit. Diese Internationale Norm ist maschinensektorspezifisch innerhalb des Rahmens der Veröffentlichung der 61508 der Internationalen Elektrotechnischen Kommission (IEC) und führt in diesen Sektor eine Methodologie für elektrische Steuerungssysteme ein. Sie ist dazu vorgesehen, die Spezifikation der Leistungsfähigkeit des elektrischen Steuerungssystems in Bezug auf die signifikanten Gefährdungen (siehe 3.8 von prEN ISO/FDIS 12100-1) von einzelnen Maschinen in maschinenspezifischen Normen zu erleichtern.

Es gibt viele Situationen an einer Maschine, wo elektrische Steuerungssysteme benutzt werden, zum Beispiel als Teil der vorgesehenen Sicherheitsmaßnahmen, 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 hat in der Automatisierung das elektrische Steuerungssystem, das verwendet wird, um den korrekten Betrieb des Maschinenprozesses zu erreichen, auf Grund der Erzeugung von Gefährdungen, die direkt von Ausfällen des Steuerungssystems herrühren, oft einen Sicherheitsaspekt. Diese Norm stellt eine Methodologie und Anforderungen bereit zur:

- Bestimmung des erforderlichen Sicherheits-Integritätslevels für jede Sicherheitsfunktion;
- Ermöglichung eines angemessenen Entwurfs des elektrischen Steuerungssystems;
- Integration von in Übereinstimmung mit ISO 13849 (EN 954) entworfenen sicherheitsbezogenen Teilsystemen;
- Verifikation, dass das elektrische Steuerungssystem seine Spezifikationen erfüllt.

Diese Internationale Norm ist zur Verwendung innerhalb des Gesamtrahmens der in prEN ISO/FDIS 12100 beschriebenen systematischen Risikominderung und in Verbindung mit einer Risikobeurteilung gemäß den in ISO 14121 (EN 1050) beschriebenen Prinzipien vorgesehen. Eine zur Bestimmung des Sicherheits-Integritätslevels (SIL) vorgeschlagene Methodologie ist im informativen Anhang A enthalten.

Es werden Maßnahmen angegeben, um die Leistungsfähigkeit des elektrischen Steuerungssystems 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 zwischen dieser Norm und anderen relevanten Normen. Bild 2 zeigt die Struktur dieser Norm.

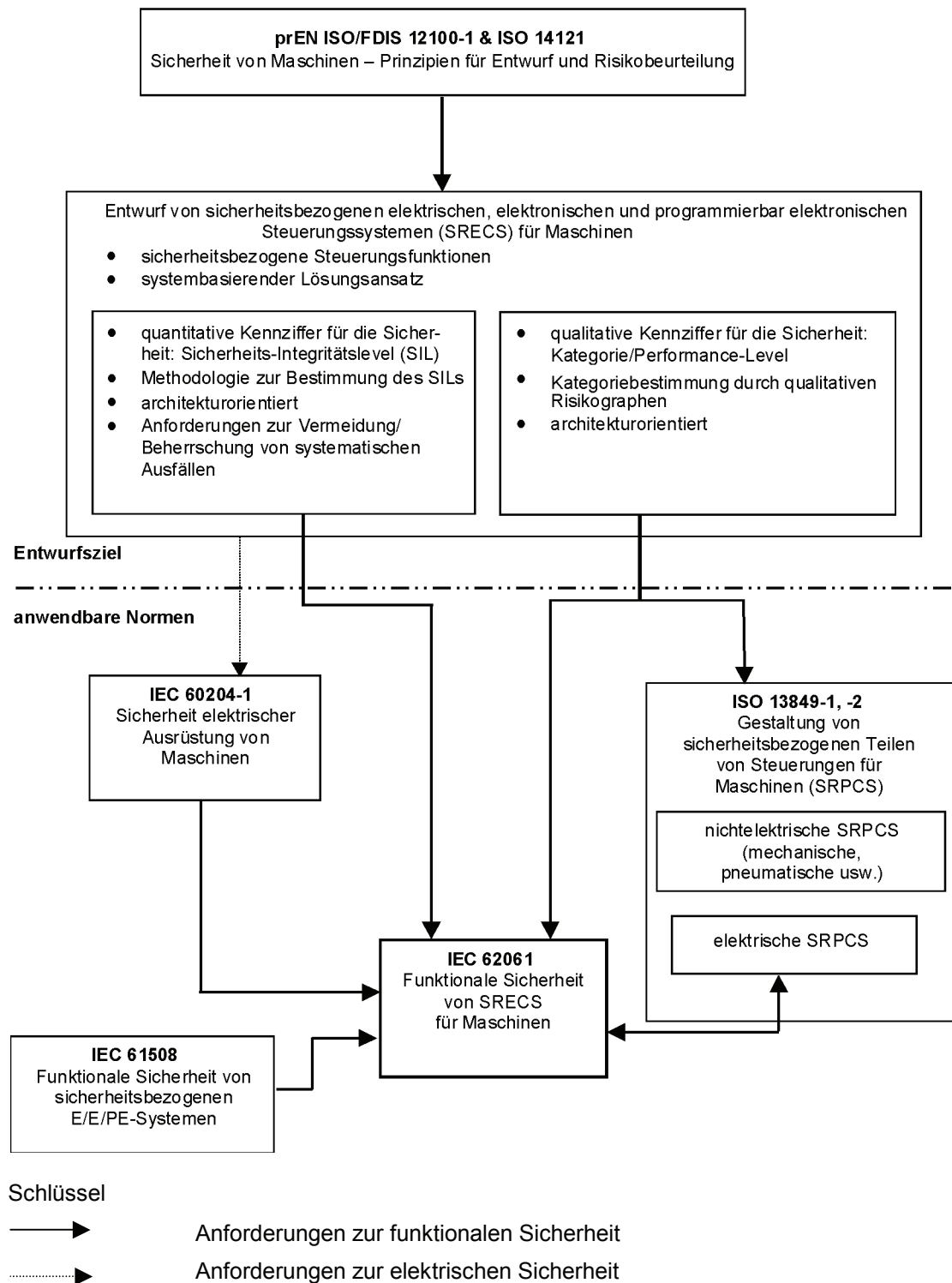


Bild 1 – Verhältnis zwischen der IEC 62061 und anderen relevanten Normen

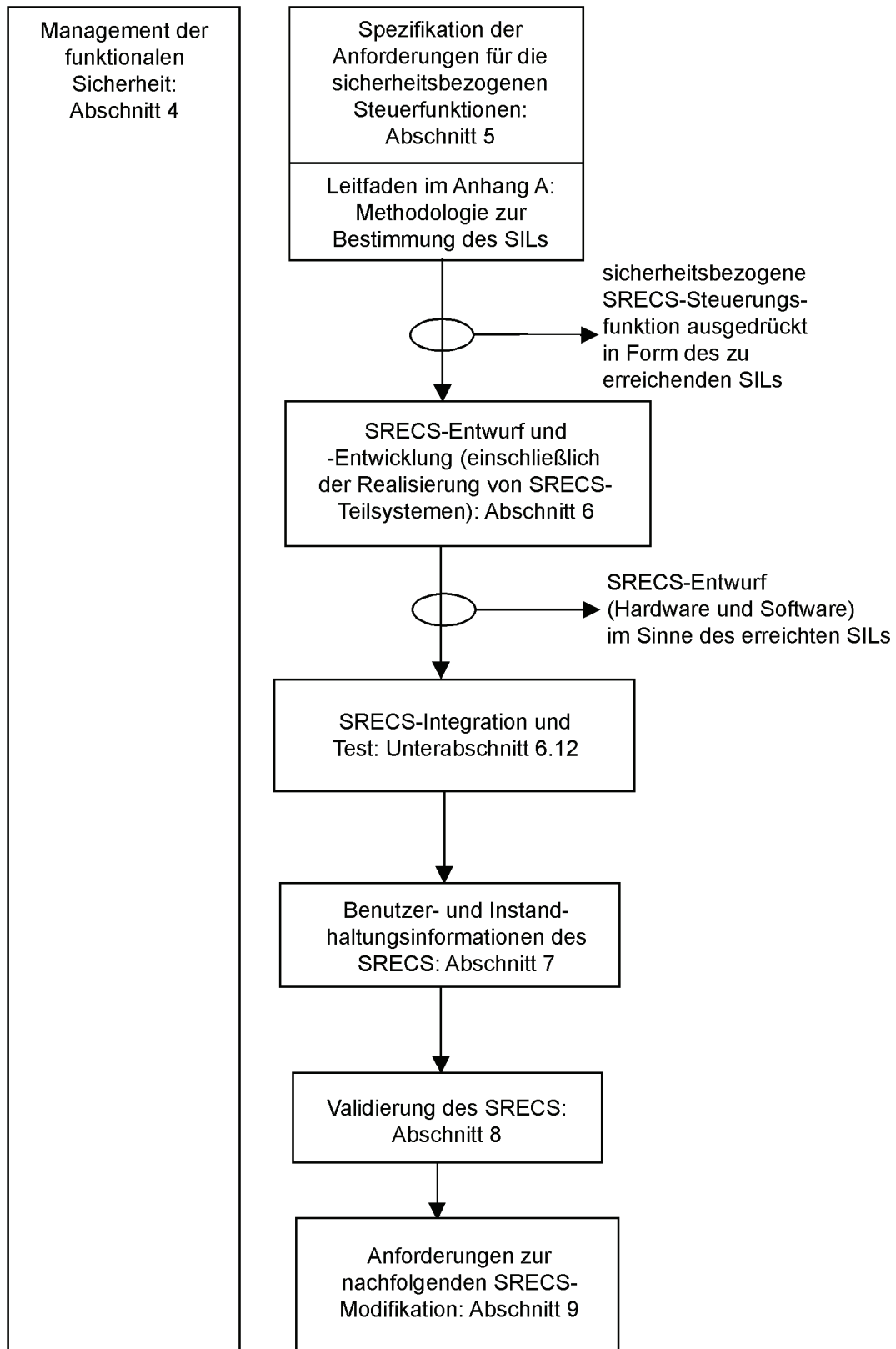


Bild 2 – Übersicht und allgemeine Struktur der IEC 62061

1 Anwendungsbereich

Diese Internationale Norm legt Anforderungen fest und macht Empfehlungen für den Entwurf, die Integration und die Validierung von sicherheitsbezogenen elektrischen, elektronischen und programmierbar elektronischen Steuerungssystemen (SRECS) für Maschinen (siehe Anmerkung 1). Sie ist auf Steuerungssysteme anwendbar, die entweder einzeln oder in Kombination verwendet werden, um Sicherheitsfunktionen an Maschinen auszuführen, die während der Arbeit nicht von Hand tragbar sind, einschließlich einer Gruppe von Maschinen, die in koordinierter Art und Weise zusammenarbeiten.

ANMERKUNG 1 In dieser Norm wird der Begriff "elektrische Steuerungssysteme" für "elektrische, elektronische und programmierbar elektronische Steuerungssysteme" und der Begriff "SRECS" für "sicherheitsbezogene elektrische, elektronische und programmierbar elektronische Steuerungssysteme" verwendet.

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 nötig 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 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;

ANMERKUNG 2 Es ist anerkannt, dass die Auswirkungen eines Ausfalls eines Steuerungssystems beträchtliche wirtschaftliche Verluste, Umweltschäden und Risiken für andere Personen einschließen können (zum Beispiel durch Mängel im oder durch Kontamination des im Prozess verarbeiteten Materials).

- ist beschränkt auf Risiken, die direkt aus den Gefährdungen der Maschine selbst oder einer Gruppe von Maschinen, die in koordinierter Art und Weise zusammenarbeiten;

ANMERKUNG 3 Oft werden Maschinen ein Element in dem Prozess eines anderen Sektors. Eine Palettierereinrichtung kann in einer Transportlinie oder Produktionslinie eingebunden sein. Am Ende einer zusammenhängenden Polymerproduktionslinie mit Extruder, Rahmen, Zugrollen usw. kann sich eine Aufwickleinrichtung befinden. In diesem Fall befinden sich die Maschinen im Anwendungsbereich dieser Norm und innerhalb des Anwendungsbereichs der Sektor-norm, von dem die Maschinen ein Teil sind. Ein typisches Beispiel ist der Fall, in dem eine Maschine(n) Teil einer Prozessaktivität ist und die Anforderungen zur funktionalen Sicherheit des elektrischen Steuerungssystems der Maschine zusätzlich die Anforderungen der IEC 61511 erfüllen müssen, insofern die Sicherheit des Prozesses betroffen ist.

- legt keine Anforderungen für die Leistungsfähigkeit von nicht-elektrischen Steuerungselementen 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 angewendet werden, die andere Technologien verwenden.

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

Die Zwecke der einzelnen Abschnitte in der IEC 62061 sind wie folgt:

Abschnitt	Zweck
4: Management der funktionalen Sicherheit	Der Zweck dieses Abschnitts ist es, folgendes festzulegen: Managementaktivitäten und die technischen Aktivitäten, die für das Erreichen der erforderlichen funktionalen Sicherheit der SRECS notwendig sind; und Verantwortlichkeiten, die für Personen, Abteilungen und Organisationen zutreffend sind, die für Aktivitäten in Bezug auf die Entwicklung eines SRECS verantwortlich sind.
5: Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen	Der Zweck dieses Abschnitts ist die 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	Der Zweck dieses Abschnitts ist es, die Auswahlkriterien und/oder die Methoden für Entwurf und Implementierung des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) festzulegen, um die Anforderungen zur funktionalen Sicherheit zu erfüllen. Dieses umfasst: 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 erfüllt.
7: Benutzerinformationen für die Maschine	Der Zweck dieses Abschnitts ist es, Anforderungen für die Benutzerinformationen des sicherheitsbezogenen elektrischen Steuerungssystems (SRECS), die mit der Maschine geliefert werden müssen, festzulegen. Dieses umfasst: Bereitstellung der Benutzeranleitung und der Verfahren, Bereitstellung der Instandhaltungsanleitung und der Verfahren.
8: Validierung des sicherheitsbezogenen elektrischen Steuerungssystems	Der Zweck dieses Abschnitts ist es, die Anforderungen für den Validierungsprozess, der auf das sicherheitsbezogene elektrische Steuerungssystem (SRECS) anzuwenden ist, festzulegen. Dieses umfasst: Inspektion und Test des in Betrieb genommenen SRECS um sicherzustellen, dass es die in der Spezifikation der Sicherheitsanforderungen festgelegten Anforderungen erreicht.
9: Modifikation des sicherheitsbezogenen elektrischen Steuerungssystems	Der Zweck dieses Abschnitts ist es, die Anforderungen für das Modifikationsverfahren, das bei Modifikation des sicherheitsbezogenen Steuerungssystems (SRECS) angewendet werden muss, festzulegen. Dieses umfasst: Modifikationen jedes sicherheitsbezogenen elektrischen Steuerungssystems (SRECS) werden geeignet geplant, überprüft und genehmigt, bevor die Änderung ausgeführt wird; die Spezifikation der SRECS-Sicherheitsanforderungen wird nach Ausführung der Modifikation eingehalten.

2 Normative Verweisungen

Die folgenden in Bezug genommenen Dokumente sind für die Anwendung dieses Dokuments unentbehrlich. Bei datierten Verweisungen gilt nur die angegebene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Ergänzungen).

prEN ISO/FDIS 12100-1: 200; Safety of machinery – Basic concepts, general principles for design – Part 1: Basic terminology, methodology

prEN ISO/FDIS 12100-2: 200x, Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles

ISO 14121:200x, Safety of machinery - Principles for risk assessment

IEC 60204–1: 200x, Safety of machinery – Electrical equipment of machines — Part 1: General requirements

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieser Norm gelten die folgenden Begriffe.

3.1.1

elektrisches Steuerungssystem

alle elektrischen, elektronischen und programmierbar elektronischen Teile eines Systems, die für die betriebliche Steuerung, Überwachung, Verriegelung, Kommunikation, Schutz und damit verbundene Funktionen verwendet werden

3.1.2

gefährbringender Ausfall

jede Fehlfunktion in der Maschine, in ihrer Energieversorgung oder in ihrem Steuerungssystem, die eine Gefährdung erzeugt (abgeleitet aus prEN ISO/FDIS 12100-1, 3.22)

3.1.3

Sicherheit

Freiheit von unvertretbarem Risiko (ISO/IEC Guide 51, 3.1)

3.1.4

funktionale Sicherheit

Teil der Gesamtsicherheit, bezogen auf die Maschine und das Maschinen-Steuerungssystem, die von der korrekten Funktion des SRECS, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt (abgeleitet aus IEC 61508-4)

ANMERKUNG Funktionale Sicherheit umfasst alle Aspekte, bei denen die Sicherheit von der korrekten Funktion des SRECS, sicherheitsbezogenen Systemen anderer Technologie und externen Einrichtungen zur Risikominderung abhängt. Diese Norm betrachtet in dem Begriff der funktionalen Sicherheit nur diejenigen Aspekte, die von der korrekten Funktion des SRECS abhängen.

3.1.5

Gefährdung (durch Maschinen)

potentielle Quelle einer Verletzung oder eines gesundheitlichen Schadens (abgeleitet aus prEN ISO/FDIS 12100-1: 200x, 3.5)

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).

3.1.6

Gefährdungssituation

Sachlage, bei der eine Person einer oder mehreren Gefährdungen ausgesetzt ist (abgeleitet aus prEN ISO/FDIS 12100-1, 3.9)

3.1.7

Maschine

Gesamtheit von miteinander verbundenen Teilen oder Vorrichtungen, von denen mindestens eins beweglich ist, sowie gegebenenfalls von Maschinen-Antriebsselementen, Steuer- und Energiekreisen usw., die zusammen für eine bestimmte Anwendung, wie die Verarbeitung, die Behandlung, die Fortbewegung oder die Aufbereitung eines Werkstoffes zusammengefügt sind

Als Maschine wird auch eine Gesamtheit von Maschinen betrachtet, die so angeordnet und gesteuert werden, dass sie als einheitliches Ganzes zur Erreichung ein und desselben Ziels zusammenarbeiten.

Ferner gelten als Maschine auswechselbare Ausrüstungen zur Änderung der Funktion einer Maschine, die nach dem Inverkehrbringen (der Lieferung) vom Bedienungspersonal selbst an der Maschine oder einer Reihe verschiedener Maschinen bzw. an einer Zugmaschine anzubringen sind, sofern diese Ausrüstungen keine Ersatzteile oder Werkzeuge sind. (IEC 60204-1, 3.33)

3.1.8

Maschinen-Steuerungssystem

System, dass auf Eingangssignale z. B. vom Prozess, anderen Maschinenelementen, einem Benutzer, externen Steuereinrichtungen reagiert und Ausgangssignale erzeugt, die dazu führen, dass die Maschine sich in der beabsichtigten Weise verhält

3.1.9

Schutzmaßnahme

Maßnahme, die zum Erreichen einer Risikominderung vorgesehen ist (abgeleitet aus prEN ISO/FDIS 12100-1:200x, 3.27)

3.1.10

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und der Schwere von Verletzungen oder gesundheitlichen Schäden (abgeleitet aus prEN ISO/FDIS 12100-1, 3.10)

3.1.11

Sicherheitsfunktion

Funktion einer Maschine, deren Ausfall unmittelbar zu einem Anstieg des(der) Risikos(en) führen kann (prEN ISO/FDIS 12100-1, 3.20)

ANMERKUNG Dieser Begriff weicht von den Begriffen in IEC 61508-4 und ISO 13849 ab.

3.1.12

Sicherheitsbezogenes elektrisches Steuerungssystem (SRECS)

elektrischer Teil eines Steuerungssystems dessen Ausfall zu einer Gefährdung führen kann

3.1.13

Sicherheitsintegrität

Wahrscheinlichkeit, dass ein sicherheitsbezogenes elektrisches Steuerungssystem die erforderlichen Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes zufriedenstellend ausführt (abgeleitet aus IEC 61508-4, 3.5.2)

ANMERKUNG Je höher der Sicherheits-Integritätslevel des sicherheitsbezogenen elektrischen Steuerungssystems ist, desto geringer ist die Wahrscheinlichkeit, dass das sicherheitsbezogene elektrische Steuerungssystem(e) die erforderliche Sicherheitsfunktion nicht ausführt.

3.1.14

Sicherheits-Integritätslevel (SIL)

diskrete Stufe (eine von drei möglichen) zur Festlegung der Anforderungen zur Sicherheitsintegrität der Sicherheitsfunktionen, die SRECS zugeordnet werden, wobei der Sicherheits-Integritätslevel 3 den höchsten und der Sicherheits-Integritätslevel 1 den niedrigsten Sicherheits-Integritätslevel darstellt (abgeleitet aus IEC 61508-4, 3.5.6)

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.

3.1.15

Betriebsart

Art, in der ein sicherheitsbezogenes System im Hinblick auf die Häufigkeit von Anforderungen an das System bestimmungsgemäß vorgesehen ist

3.1.15.1

Betriebsart mit niedriger Anforderungsrate

wenn die Häufigkeit von Anforderungen an ein sicherheitsbezogenes System nicht mehr als einmal pro Jahr beträgt und wenn die Häufigkeit der Anforderungen nicht größer als die doppelte Häufigkeit der Wiederholungsprüfung ist

3.1.15.2

Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung

wenn die Häufigkeit von Anforderungen an ein sicherheitsbezogenes System mehr als einmal pro Jahr beträgt oder wenn die Häufigkeit der Anforderungen größer als die doppelte Häufigkeit der Wiederholungsprüfung ist (IEC 61508-4, 3.5.12)

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

ANMERKUNG 2 Anforderungs-Betriebsart bedeutet, dass eine Sicherheitsfunktion nur auf Anfrage (Anforderung) ausgeführt wird, um die Maschine in einen festgelegten Zustand zu überführen. Das für die Ausführung der Sicherheitsfunktion vorgesehene SRECS hat keinen Einfluss auf die Maschine, bis es angefordert wird.

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

3.1.16

Ausfallgrenzwert

vorgesehene Wahrscheinlichkeit gefahrbringender Ausfälle, die in Bezug auf die Anforderungen zur Sicherheitsintegrität zu erreichen ist; festgelegt als die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (abgeleitet aus IEC 61508-4, 3.5.13)

3.1.17

Sicherheitsintegrität der Hardware

Teil der Sicherheitsintegrität eines SRECS, der sich auf zufällige Hardwareausfälle bezieht, die zu gefahrbringenden Ausfällen führen (abgeleitet aus IEC 61508-4, 3.5.5)

3.1.18

Sicherheitsintegrität der Software

Maß für die Wahrscheinlichkeit, dass die Software in einem programmierbaren elektronischen System ihre Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb eines festgelegten Zeitraumes erfüllt (IEC 61508-4, 3.5.3)

3.1.19

systematische Sicherheitsintegrität

Teil der Sicherheitsintegrität eines SRECS, der sich auf zufällige systematische Ausfälle (siehe Anmerkung zu 3.13) bezieht, die zu gefahrbringenden Ausfällen führen (IEC 61508-4, 3.5.4)

ANMERKUNG Die systematische Sicherheitsintegrität kann üblicherweise nicht quantifiziert werden.

3.1.20

Steuerungsfunktion

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

3.1.21

sicherheitsbezogene Steuerungsfunktion

Steuerungsfunktion mit einem festgelegten Integritätslevel, die von einem SRECS mit dem Ziel, den sicheren Zustand der Maschine aufrechtzuerhalten oder gefährliche Situationen an der Maschine zu verhindern, ausgeführt wird

ANMERKUNG Dieser Begriff weicht von den Begriffen der "Sicherheitsfunktion von Steuerungssystemen" in ISO 13849-1 ab. Die "Sicherheitsfunktion von Steuerungssystemen" nach dem Begriff in ISO 13849-1 umfasst die in dieser Norm definierte "sicherheitsbezogene Steuerungsfunktion" und "Fehlerreaktionsfunktion".

3.1.22

SRECS-Diagnosefunktion

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

ANMERKUNG Diese Funktion ist zur Erkennung von Fehlern, die zu einem gefahrbringenden Ausfall einer sicherheitsbezogenen Steuerungsfunktion führen können und zur Einleitung einer festgelegten Fehlerreaktionsfunktion zur Verhinderung des gefahrbringenden Ausfalls vorgesehen. Die Diagnosefunktion ist eine sicherheitsbezogene Funktion.

3.1.23

SRECS-Überwachungsfunktion

Funktion, die den Betrieb des sicherheitsbezogenen elektrischen Steuerungssystems überwacht und Ausgangsinformationen entsprechend dem Zustand des Steuerungssystems erzeugt

3.1.24

Fehlerreaktionsfunktion

Funktion, die eingeleitet wird, falls durch die SRECS-Diagnosefunktion ein Fehler oder Ausfall des sicherheitsbezogenen elektrischen Steuerungssystems erkannt wird und die das Ziel hat, den sicheren Zustand der Maschine aufrechtzuerhalten oder gefährliche Situationen an der Maschine zu verhindern

ANMERKUNG Eine Fehlerreaktionsfunktion ist mit der Implementierung einer sicherheitsbezogenen Steuerungsfunktion verbunden.

3.1.25

Funktionsblock

(en: function block)

konzeptionelle Einheit, die aus einer Aufteilung einer sicherheitsbezogenen Steuerungsfunktion auf oberster Ebene hervorgeht, wobei ein Ausfall irgendeines Funktionsblocks zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt

ANMERKUNG In dieser Norm kann eine sicherheitsbezogene Steuerungsfunktion (F) als die logische Summe der Funktionsblöcke (FB) betrachtet werden, d. h. $F = FB_1 \& FB_2 \& \dots \& FB_n$

3.1.26

Funktionsblock-Element

Teil eines Funktionsblocks

3.1.27

Teilsystem

Element in dem Entwurf der Architektur des SRECS auf oberster Ebene, wobei ein Ausfall irgendeines Teilsystems zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt

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

ANMERKUNG 2 Dieser Begriff ist eine Einschränkung der allgemeinen Begriffe in IEC 61508: "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 Im Unterschied zum allgemeinen Sprachgebrauch in dem "Teilsystem" irgendeine unterteilte Einheit bedeuten kann, wird der Begriff "Teilsystem" 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.

3.1.28

Teilsystem-Element

Teil eines Teilsystems. Ein Teilsystem kann eine einzelne Komponente oder irgendeine Gruppe von Komponenten umfassen

3.1.29

Architektur

spezifische Konfiguration von Hardware- und Softwareelementen in einem SRECS (abgeleitet aus IEC 61508-4, 3.3.5.)

3.1.30

Strukturelle Einschränkung

Anzahl von Anforderungen, die den Sicherheits-Integritätslevel einschränkt, der für ein Teilsystem geltend gemacht werden kann

ANMERKUNG Anforderungen zu strukturellen Einschränkungen sind in 6.7.6 enthalten.

3.1.31

Anteil sicherer Ausfälle

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:

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

wobei λ_S die Wahrscheinlichkeit ungefährlicher Ausfälle ist, λ_{DD} die Wahrscheinlichkeit gefahrbringender Ausfälle ist, die durch die Diagnosefunktionen erkannt werden, und λ_D die Wahrscheinlichkeit 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 6.7.6.4).

3.1.32

Diagnosedeckungsgrad

Verminderung der Wahrscheinlichkeit gefahrbringender Hardwareausfälle, die aus der Ausführung der automatischen Diagnosetests resultiert (abgeleitet aus IEC 61508-4, 3.8.6)

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

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

wobei λ_{DD} die Wahrscheinlichkeit erkannter gefährlicher Ausfälle ist und λ_{Dtotal} die Wahrscheinlichkeit aller gefahrbringenden Ausfälle ist.

3.1.33

systematischer Ausfall

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 (abgeleitet aus 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.

[IEV 191-04-19]

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

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

3.1.34

Wiederholungsprüfung

wiederkehrende Prüfung, die zur Erkennung von Fehlern in einem SRECS ausgeführt wird, so dass, falls notwendig, das System in einen "Wie-Neu-Zustand" gebracht oder so nah wie praktisch möglich an diesen Zustand heran gebracht werden kann (abgeleitet aus IEC 61508-4, 3.8.5)

ANMERKUNG Die Wirksamkeit der Wiederholungsprüfung wird davon abhängig sein, wie nah das SRECS an den "Wie-Neu-Zustand" heran gebracht wird. Damit die Wiederholungsprüfung vollständig wirksam ist, ist es notwendig, 100 % aller gefahrbringenden Ausfälle zu erkennen. Obwohl dies in der Praxis für andere als einfache SRECS nicht leicht erreichbar ist, sollte dies das Ziel sein. Es werden mindestens alle Sicherheitsfunktionen gemäß der Spezifikation der SRECS-Sicherheitsanforderungen überprüft. Falls separate Kanäle verwendet werden, werden diese Prüfungen für jeden Kanal getrennt ausgeführt.

3.1.35

Programmiersprache mit uneingeschränktem Sprachumfang

textuelle oder graphische Software-Programmiersprache für kommerzielle und industrielle programmierbare elektronische Controller mit einem auf die spezielle Anwendung unbegrenzten Leistungsspektrum

3.1.36

Programmiersprache mit eingeschränktem Sprachumfang

textuelle oder graphische Software-Programmiersprache für kommerzielle und industrielle programmierbare elektronische Controller mit einem auf die spezielle Anwendung begrenzten Leistungsspektrum

3.1.37

Software-Sicherheitslebenszyklus

Aktivitäten, die sich während eines Zeitraums ereignen, der mit der Formulierung der sicherheitsbezogenen Software beginnt und endet, wenn die sicherheitsbezogene Software nicht mehr verwendet wird

3.1.38

Sicherheitsbezogene Software

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

ANMERKUNG Die Verifikationsergebnisse sollten zum Nachweis des Ziels dokumentiert werden.^{N1)}

BEISPIEL Verifikationsaktivitäten schließen ein:^{N1)}

- 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 von Umgebungseinflüssen um sicherzustellen, dass alle Teile in der festgelegten Art und Weise zusammenwirken.

3.1.39

Verifikation

Bestätigung durch Untersuchung (z. B. Tests, Analysen), dass die Ergebnisse die durch die zugehörige Spezifikation gestellten Anforderungen erfüllen (abgeleitet aus IEC 61508-4, 3.8.1 und IEC 61511, 3.1.102)

3.1.40

Validierung

Bestätigung durch Untersuchung (z. B. Tests, Analysen), dass das sicherheitsbezogene elektrische Steuerungssystem die Anforderungen zur funktionalen Sicherheit der spezifischen Anwendung erfüllt (abgeleitet aus IEC 61508-4, 3.8.2 und IEC 61511, 3.1.101)

^{N1)} Nationale Fußnote: Anmerkung und Beispiel gehören in Unterabschnitt 3.1.39

3.2 Abkürzungen

Die folgenden Abkürzungen werden in dieser Norm verwendet.

SIL	Sicherheits-Integritätslevel
SRECS	sicherheitsbezogenes elektrisches Steuerungssystem
SRPCS	sicherheitsbezogene Teile von Steuerungssystemen
SFF	Anteil sicherer Ausfälle
DC	Diagnosedeckungsgrad
E/E/PES	elektrisches/elektronisches/programmierbar elektronisches System
SRS	Spezifikation der Sicherheitsanforderungen
MTTR	mittlere Zeit bis zur Wiederherstellung
SR	sicherheitsbezogen
P _{DF}	Wahrscheinlichkeit gefahrbringender Ausfälle
P _{TE}	Wahrscheinlichkeit von Übertragungsfehlern
SYS	System
EMI	elektromagnetische Beeinflussung
E/A	Eingang/Ausgang

4 Management der funktionalen Sicherheit

4.1 Zweck

Der Zweck dieses Abschnitts ist es Folgendes festzulegen:

- Managementaktivitäten und technische Aktivitäten, die für das Erreichen der erforderlichen funktionalen Sicherheit der SRECS notwendig sind; und
- Verantwortlichkeiten, die für Personen, Abteilungen und Organisationen zutreffen, die für Aktivitäten in Bezug auf die Entwicklung eines SRECS verantwortlich sind.

4.2 Anforderungen

4.2.1 Es muss ein Plan der funktionalen Sicherheit erstellt und für jedes Projekt dokumentiert und wie erforderlich aktualisiert werden. Der Plan muss Verfahren für die Steuerung der in den Abschnitten 5 bis 9 festgelegten Aktivitäten einschließen.

ANMERKUNG 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;
- Sicherheits-Integritätslevel;
- Auswirkungen beim Auftreten eines Ausfalls.

Im Einzelnen muss der Plan:

- a) die relevanten Aktivitäten in den Abschnitten 5 bis 9 identifizieren;
- b) die Vorgehensweise und die Strategie zum Erreichen der festgelegten Anforderungen zur funktionalen Sicherheit identifizieren;

- c) Personen, Abteilungen oder andere Einheiten, die für die Ausführung und Überprüfung aller in den Abschnitten 5 bis 9 festgelegten Aktivitäten verantwortlich sind, bestimmen. Die Aufteilung von Verantwortlichkeiten muss festgelegt werden und die Betroffenen müssen über die ihnen zugewiesenen Verantwortlichkeiten informiert werden.
- d) die Verfahren zur Protokollierung und Pflege der für die funktionale Sicherheit eines SRECS relevanten Informationen identifizieren oder festsetzen.

ANMERKUNG 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.
- e) Aufstellung eines Verifikationsplans, der Folgendes einschließen muss:
 - Einzelheiten wann die Verifikation stattfinden muss;
 - die Auswahl der Verifikationsstrategien und Verifikationstechniken;
 - die Auswahl und Verwendung von Testeinrichtungen;
 - die Auswahl der Verifikationsaktivitäten; und
 - die Bewertung der durch die Verifikationseinrichtungen und durch Tests gewonnenen Verifikationsergebnisse.
 - f) Aufstellung eines Validierungsplans, der Folgendes umfasst:
 - Einzelheiten wann die Validierung stattfinden muss;
 - Einzelheiten zu den Personen, die die Validierung durchführen müssen;
 - Identifizierung der relevanten Betriebsarten der Maschine (z. B. Normalbetrieb, Einrichten);
 - Identifizierung des relevanten sicherheitsbezogenen elektrischen Steuerungssystems für jede Betriebsart;
 - Anforderungen, gegen die das sicherheitsbezogene elektrische Steuerungssystem zu validieren ist;
 - die technische Strategie zur Validierung, zum Beispiel analytische Methoden oder statistische Tests;
 - Akzeptanzkriterien; und
 - auszuführende Aktion bei Nichterreichen der Akzeptanzkriterien.

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

- in den Abschnitten 5 bis 9 festgelegte Aktivitäten;
- Verifikationsaktivitäten; und
- Validierungsaktivitäten.

5 Anforderungen zur Spezifikation der sicherheitsbezogenen Steuerungsfunktionen

5.1 Zweck

Dieser Abschnitt beschreibt die Verfahren zur Spezifikation der Anforderungen für sicherheitsbezogene Steuerungsfunktion(en), die durch die SRECS zu implementieren sind.

5.2 Spezifikation der Anforderungen für sicherheitsbezogene Steuerungsfunktionen

5.2.1 Allgemeines

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

ANMERKUNG Anhang A enthält eine Methodologie zur Bestimmung des SILs.

5.2.1.2 Wenn Sicherheitsfunktionen ausgewählt werden, um sie durch SRECS zu verwirklichen (im Ganzen oder teilweise), müssen die zugehörigen sicherheitsbezogenen Steuerungsfunktionen spezifiziert werden.

5.2.1.3 Die Spezifikationen für jede sicherheitsbezogene Steuerungsfunktion müssen umfassen:

- 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 Wo nichtelektrische Einrichtungen zur Ausführung einer Sicherheitsfunktion in Kombination mit elektrischen Mitteln beitragen, werden die auf nichtelektrische Einrichtungen bezogenen Ausfallgrenzwerte im Rahmen dieser Norm nicht betrachtet. Elektrische Mittel umfasst alle Geräte oder Systeme, die auf Basis elektrischer Prinzipien arbeiten, einschließlich:

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

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

ANMERKUNG Dies kann zum Beispiel durch Inspektion, Walkthrough, Analyse, Checklisten erreicht werden. Siehe auch B.2.6 von IEC 61508-7.

5.2.2 Benötigte Informationen

Die folgenden Informationen müssen vorhanden sein, um die Spezifikation der funktionalen Anforderungen für jede sicherheitsbezogene Steuerungsfunktion zu erstellen:

- Ergebnisse der Risikoanalyse für die Maschine einschließlich aller während des Prozesses der Risikominderung als notwendig bestimmten Sicherheitsfunktionen;
- Betriebscharakteristika der Maschine, einschließlich:
 - Betriebsarten,
 - Zykluszeit,
 - Leistungsfähigkeit in Bezug auf Reaktionszeit,
 - Umgebungsbedingungen,
 - Wechselwirkung zwischen Person(en) und der Maschine (z. B. Reparatur, Einrichten, Waschen).
- alle in Bezug auf die sicherheitsbezogenen Steuerungsfunktionen relevanten Informationen, die einen Einfluss auf den Entwurf des SRECS haben können, einschließlich zum Beispiel:
 - eine Beschreibung des Verhaltens der Maschine, das eine sicherheitsbezogene Steuerungsfunktion erreichen oder verhindern soll;
 - alle Schnittstellen zwischen den sicherheitsbezogenen Steuerungsfunktionen und zwischen jeder anderen Funktion (entweder direkt in Verbindung stehend innerhalb oder außerhalb der Maschine);
 - erforderliche Fehlerreaktionen der sicherheitsbezogenen Steuerungsfunktion.

ANMERKUNG Einige Informationen sind eventuell nicht vorhanden oder ausreichend definiert, bevor der iterative Entwurfsprozess des SRECS beginnt, so dass die Spezifikation der SRECS-Sicherheitsanforderungen zu aktualisieren ist, während dieser Entwurfsprozess entwickelt wird.

5.2.3 Spezifikation der funktionalen Anforderungen für sicherheitsbezogene Steuerungsfunktionen

Die Spezifikation der funktionalen Anforderungen für sicherheitsbezogene Steuerungsfunktionen muss jedes Detail jeder auszuführenden sicherheitsbezogenen Steuerungsfunktion beschreiben, einschließlich zum Beispiel:

- die Bedingung(en) (z. B. Betriebsart) der Maschine unter denen die sicherheitsbezogene Steuerungsfunktion aktiviert oder ausgeschaltet werden muss;
- die Priorität derjenigen Funktionen, die gleichzeitig aktiv sein können und die in Widerspruch stehende Aktionen auslösen können;
- die erforderliche Reaktionszeit jeder sicherheitsbezogenen Steuerungsfunktion;
- die Schnittstelle(n) des SRECS zu anderen Maschinenkomponenten;
- die erforderliche Reaktionszeit von Eingangs- und Ausgangssignalen;
- eine Beschreibung der sicherheitsbezogenen Steuerungsfunktion (einschließlich der Beschreibung der Fehlerreaktionsfunktion(en), d. h. Verhalten des SRECS bei Erkennung eines Fehlers, der zu einem gefährbringenden Ausfall der sicherheitsbezogenen Steuerungsfunktion führen kann);
- eine Beschreibung der Betriebsumgebung (z. B. Temperatur, Feuchtigkeit, EMV);
- Tests und alle zugehörigen Einrichtungen (z. B. Testeinrichtungen, Testschnittstellen).

5.2.4 Spezifikation der Anforderungen zur Sicherheitsintegrität für sicherheitsbezogene Steuerungsfunktionen

5.2.4.1 Die Anforderungen zur Sicherheitsintegrität für jede sicherheitsbezogene Steuerungsfunktion müssen aus der Risikobeurteilung abgeleitet werden, um sicherzustellen, dass die notwendige Risikominderung erreicht werden kann. In dieser Norm ist diese Sicherheitsintegrität als ein Ausfallgrenzwert für die Wahrscheinlichkeit gefährbringender Ausfälle pro Stunde jeder sicherheitsbezogenen Steuerungsfunktion ausgedrückt.

ANMERKUNG Bild 3 zeigt die Verbindung zwischen einem gefährbringenden Ausfall einer Sicherheitsfunktion und dem Auftreten einer Gefährdungssituation.

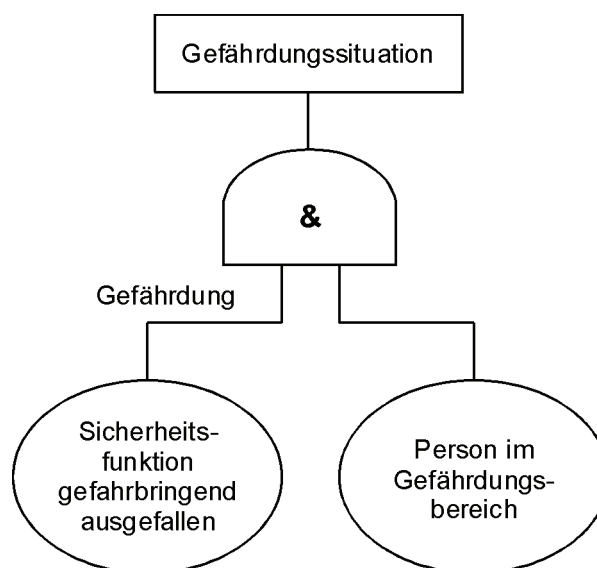


Bild 3

5.2.4.2 Die Anforderungen zur Sicherheitsintegrität für jede sicherheitsbezogene Steuerungsfunktion müssen in Form eines SILs in Übereinstimmung mit Tabelle 1 festgelegt (siehe Anhang A zur Methodologie) und dokumentiert werden.

Tabelle 1 – Sicherheits-Integritätslevels: Ausfallgrenzwerte für sicherheitsbezogene Steuerungsfunktionen

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

ANMERKUNG Es ist wichtig anzumerken, dass die Sicherheits-Integritätslevels 1, 2, und 3 Zielwerte für sicherheitsbezogene Steuerungsfunktionen sind. Es ist allgemein anerkannt, dass es nur im Hinblick auf die Sicherheitsintegrität der Hardware möglich ist, zu quantifizieren und Zuverlässigkeits-Voraussagemethoden bei der Beurteilung, ob ein SIL-Zielwert erreicht worden ist, anzuwenden. Qualitative Methoden müssen unter Berücksichtigung der notwendigen Vorsichtsmaßnahmen durchgeführt werden, um einen SIL-Zielwert hinsichtlich der systematischen Sicherheitsintegrität zu erreichen.

5.2.4.2^{N2)} Wo die erforderliche Sicherheitsintegrität einer sicherheitsbezogenen Steuerungsfunktion kleiner als SIL 1 ist, müssen mindestens die Anforderungen von Kategorie B nach ISO 13849-1 und IEC 60204-1, 9.4.3.1 erfüllt werden.

6 Entwurf und Integration des sicherheitsbezogenen elektrischen Steuerungssystems

6.1 Zweck

Der Zweck der Anforderungen dieses Abschnitts ist es, SRECS auszuwählen oder zu entwerfen und zu implementieren, 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 angemessener Berücksichtigung aller Anforderungen aus Abschnitt 6 so 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 Der Entwurf des SRECS (einschließlich der gesamten Hardware- und Softwarearchitektur, Sensoren, Aktoren, programmierbarer Elektronik, Embedded-Software, Anwendungssoftware usw.) kann entweder 6.5 oder 6.6 erfüllen. Unabhängig davon welche Methode verwendet wird, muss das SRECS die folgenden Anforderungen erfüllen:

- a) die Anforderungen zur Sicherheitsintegrität der Hardware einschließlich:
 - 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) einschließlich:
 - den Anforderungen zur Vermeidung von Ausfällen; und
 - den Anforderungen zur Beherrschung systematischer Fehler;
- c) die Anforderungen zum Systemverhalten bei Erkennung eines Fehlers (siehe 6.3);

^{N2)} Nationale Fußnote: Die korrekte Nummerierung dieses Unterabschnitts muss 5.2.4.3 lauten.

d) die Anforderungen für den Entwurf und die Entwicklung von sicherheitsbezogener Software (siehe 6.11).

6.2.3 Der Entwurf des SRECS muss menschliche Fähigkeiten und Einschränkungen berücksichtigen und muss für die notwendigen Handlungen des Bedienungs- und Instandhaltungspersonals geeignet sein. Der Entwurf aller Schnittstellen muss guter praktischer Erfahrung folgen (siehe IEC 60310) und muss auf den wahrscheinlichen Ausbildungsstand oder das Bewusstsein der Benutzer abgestimmt sein, zum Beispiel bei in großen Stückzahlen produzierten Teilsystemen, wo der Benutzer ein Teil der Öffentlichkeit ist.

ANMERKUNG Es sollte Entwurfsziel sein, dass vorhersehbare Irrtümer, die von Benutzern oder dem Instandhaltungspersonal gemacht werden, durch den Entwurf, wo immer möglich, verhindert oder beseitigt werden oder, dass eine manuelle Aktion eine zweite Bestätigung vor der Ausführung erfordert.

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 Diagnosefunktionen muss dokumentiert werden. Diese Dokumentation muss:

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

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 jedem Teilsystem, das eine Fehlertoleranz der Hardware 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. Wenn die Reparatur nicht innerhalb der mittleren Zeit bis zur Wiederherstellung (MTTR) abgeschlossen ist, die in der Berechnung der Wahrscheinlichkeit eines zufälligen Hardwareausfalls (siehe 6.7.7) angenommen ist, muss eine zweite Fehlerreaktion ausgeführt werden, um einen sicheren Zustand aufrechtzuerhalten.

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

ANMERKUNG 1 Die Methode der Isolation eines fehlerhaften Bestandteils ist nur anwendbar, wenn das SRECS für eine Reparatur während des Betriebs ohne einen Einfluss auf seine Sicherheitsintegrität entworfen worden ist.

ANMERKUNG 2 Die mittlere Zeit bis zur Wiederherstellung (siehe IEC 191-13-08), die im Zuverlässigkeitsmodell betrachtet wird, muss das Diagnose-Testintervall, die Reparaturzeit und alle anderen Verzögerungen vor der Wiederherstellung berücksichtigen.

6.3.2 Wenn eine Diagnosefunktion(en), die zum Erreichen der erforderlichen Wahrscheinlichkeit notwendig ist (sind), einen gefahrbringenden Fehler in irgendeinem Teilsystem, das eine Fehlertoleranz der Hardware von Null besitzt, erkennt, muss die spezifizierte Fehlerreaktionsfunktion ausgeführt werden, **bevor die Gefährdung auf Grund dieses Fehlers auftreten kann.**

ANMERKUNG Zu weiteren Anforderungen bezüglich des Diagnose-Testintervalls siehe 6.7.7.1.3 und 6.7.7.1.4.

6.3.3 Der nachfolgende Betrieb des SRECS (z. B. Freigabe des Neustarts der Maschine) darf nicht möglich sein, bevor der fehlerhafte Bestandteil repariert worden ist.

6.4 Anforderungen zur systematischen Sicherheitsintegrität

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 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) Beachtung der Anwendungshinweise des Herstellers, z. B. Katalogangaben, Installationsanweisungen, Spezifikationen und Anwendung bewährter Betriebspraxis (siehe auch prEN 954-2, Anhang D.1);
- d) Verwendung von Teilsystemen, die vergleichbare Betriebseigenschaften haben (siehe auch prEN 954-2, Anhang D.1);
- e) Das SRECS sollte gemäß IEC 60204-1, 7.2 und 9.1.1 geschützt sein;

ANMERKUNG Diese Anforderung trifft auch auf Teilsystemebene zu.

6.4.1.2 Zusätzlich muss mindestens eine der folgenden Maßnahmen unter Berücksichtigung der Komplexität des SRECS und der SILs 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 Schwachpunkte 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) Rechnerunterstützte Entwurfswerkzeuge zur Durchführung von Simulation oder Analyse: systematische Ausführung des Entwurfsverfahrens und Einbeziehung vorentwickelter Elemente, die bereits vorhanden und getestet sind.

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

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

ANMERKUNG 3 Die Schaltungsfunktion des sicherheitsbezogenen Systems kann mit einem Rechner durch ein softwarebasierendes Verhaltensmodell simuliert werden, wobei jedes einzelne Bauelement des Schaltkreises sein eigenes simuliertes Verhalten besitzt und die Reaktion des Schaltkreises, mit dem die Bauelemente verbunden sind, untersucht wird, in dem die Grenzwerte jedes Bauteils 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 werden kann oder beibehalten wird.
- b) Maßnahmen zur Beherrschung der Auswirkungen vorübergehender Teilsystemausfälle: Das SRECS muss so entworfen sein, dass zum Beispiel:

- die Auswirkungen eines Spannungsausfalls usw. an einem einzelnen Teilsystem nicht zu einer Gefährdungssituation führen (z. B. darf ein vorübergehender Spannungsausfall, der sich nur auf ein Schütz auswirkt, nicht zu einem unerwarteten Anlauf eines Motors führen); und

ANMERKUNG Siehe auch relevante Abschnitte 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 Sekundärspannung 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 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 ein Teilsystem(e) dürfen nicht zu einer Gefährdungssituation führen.
- c) Maßnahmen zur Beherrschung der Auswirkungen von Fehlern und anderer Effekte, die von irgendeinem Datenkommunikationsprozess herrühren, in Übereinstimmung mit 7.4.8 von IEC 61508-2.
- 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 die Fehler-toleranz der Hardware zu Null reduziert, muss diese Fehlerreaktion stattfinden, bevor die berechnete MTTR (siehe 6.7.7.1.2 (g) und Anmerkung 5) überschritten ist.

Schnittstellen sind für diese Betrachtung Eingänge und Ausgänge von Teilsystemen und alle anderen Einheiten von Teilsystemen, die während der Integration einer Verkabelung bedürfen, z. B. die Ausgangsschalt-elemente eines Lichtvorhangs oder der Ausgang eines Positionssensors einer Türüber-wachung.

ANMERKUNG Dies erfordert nicht, dass die Erkennung eines Fehlers an den Ausgängen eines Teilsystems oder Teil-system-Elements selbst durchgeführt werden muss. Die Fehlerreaktionsfunktion kann auch von irgendeinem nachfolgen-den Teilsystem nach der Ausführung eines Diagnosetests eingeleitet werden.

6.5 Auswahl eines sicherheitsbezogenen elektrischen Steuerungssystems

Wenn ein Lieferant ein SRECS für eine spezifische Funktion vorsieht, die in der Spezifikation der Sicher-heitsanforderungen erwähnt wird, kann ein bereits entwickeltes SRECS anstatt einer eigenen Entwicklung gewählt werden, vorausgesetzt es erfüllt die Anforderungen der Spezifikation der Sicherheitsanforderungen und die Abschnitte 6.3, 6.4 und 6.6.1 dieser Norm.

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

6.6 Entwurf und Entwicklung eines sicherheitsbezogenen elektrischen Steuerungs-systems (SRECS)

6.6.1 Allgemeine Anforderungen

6.6.1.1 Das SRECS muss in Übereinstimmung mit der Spezifikation der SRECS-Sicherheitsanforderungen (siehe 5.2) und unter Berücksichtigung der funktionalen Anforderungen und der Anforderungen zur Sicher-heitsintegrität 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 Bei Erkennung eines Fehlers muss der Entwurf die Ausführung der spezifizierten Fehlerreaktions-funktion (siehe 5.2 und 6.3) vorsehen.

6.6.1.4 Wo ein SRECS oder seine Teilsysteme sowohl sicherheitsbezogene Steuerungsfunktionen, als auch andere Funktionen enthalten soll, muss seine gesamte Hardware und Software als sicherheitsbezogen behandelt werden, es sei denn, es kann gezeigt werden, dass die Implementierung der sicherheitsbezogenen

Steuerungsfunktionen und der anderen Funktionen ausreichend unabhängig voneinander ist (d. h., dass der Ausfall irgendwelcher anderen Funktionen nicht die sicherheitsbezogenen Steuerungsfunktionen 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 im Vergleich zum Sicherheits-Integritätslevel des SRECS ausreichend gering ist.

6.6.1.5 Für ein SRECS oder seine Teilsysteme, das Sicherheitsfunktionen verschiedener Sicherheits-Integritätslevels implementiert, muss die Hardware und Software als zum höchsten Sicherheits-Integritätslevel zugehörig betrachtet werden, es sei denn, es kann gezeigt werden, dass die Implementierung von Sicherheitsfunktionen verschiedener Sicherheits-Integritätslevels 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 Sicherheitsfunktionen unterschiedlicher Sicherheits-Integritätslevels enthalten, im Vergleich zum Sicherheits-Integritätslevel des SRECS ausreichend gering ist.

6.6.1.6 Verbindungen (z. B. Verdrahtung, Verkabelung) außer digitaler Datenkommunikation müssen als Teil eines Teilsystems, mit dem sie verbunden sind, betrachtet werden.

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

6.6.1.8 Die Dokumentation des SRECS-Entwurfs muss diejenigen Methoden und Maßnahmen festlegen, die während des Einsatzes der Maschine notwendig sind, um den Sicherheits-Integritätslevel zu erreichen.

6.6.1.9 Die Dokumentation des SRECS-Entwurfs muss die Begründung für die Methoden und Maßnahmen enthalten, die gewählt worden sind, um eine Zusammenstellung zu bilden, die für den erforderlichen Sicherheits-Integritätslevel ausreichend ist.

6.6.2 Entwurfs- und Entwicklungsprozess

Der Entwurf und die Entwicklung muss einem klar definierten Prozess unter Berücksichtigung aller Aspekte, die von dem im Bild 4 gezeigten Prozess abgedeckt werden, folgen.

ANMERKUNG Der Ansatz dieser Norm ist ein systematischer "top-down"-Entwurf des SRECS beginnend bei den Anforderungen, die in der Spezifikation der Sicherheitsanforderungen festgelegt sind. Bild 5 zeigt den Ablauf des Entwurfs 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 sicherheitsbezogene Steuerungsfunktion muss, wie zum Beispiel in Bild 4 gezeigt, in eine Struktur von Funktionsblöcken zerlegt werden. Diese Struktur muss dokumentiert werden einschließlich:

- der Beschreibung der Struktur;
- den Anforderungen zu jedem Funktionsblock (funktional, in Bezug auf Integrität);
- der Begriffe 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 sicherheitsbezogenen Steuerungsfunktion 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, die einem Funktionsblock zugehörig sind, 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 Abschnitt 6.7.4 "Entwurf und Entwicklung von Teilsystemen" zu berücksichtigen.

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

ANMERKUNG 3 Die Funktionsblöcke sind ein Teil der sicherheitsbezogenen Steuerungsfunktion (siehe 3.1.21) und umfassen nicht die SRECS-Diagnosefunktionen (siehe 3.1.22). Im Rahmen dieser Norm werden die Diagnosefunktionen als gesonderte Funktionen betrachtet, die eine andere Struktur als die sicherheitsbezogene Steuerungsfunktion haben können (siehe 6.8.2).

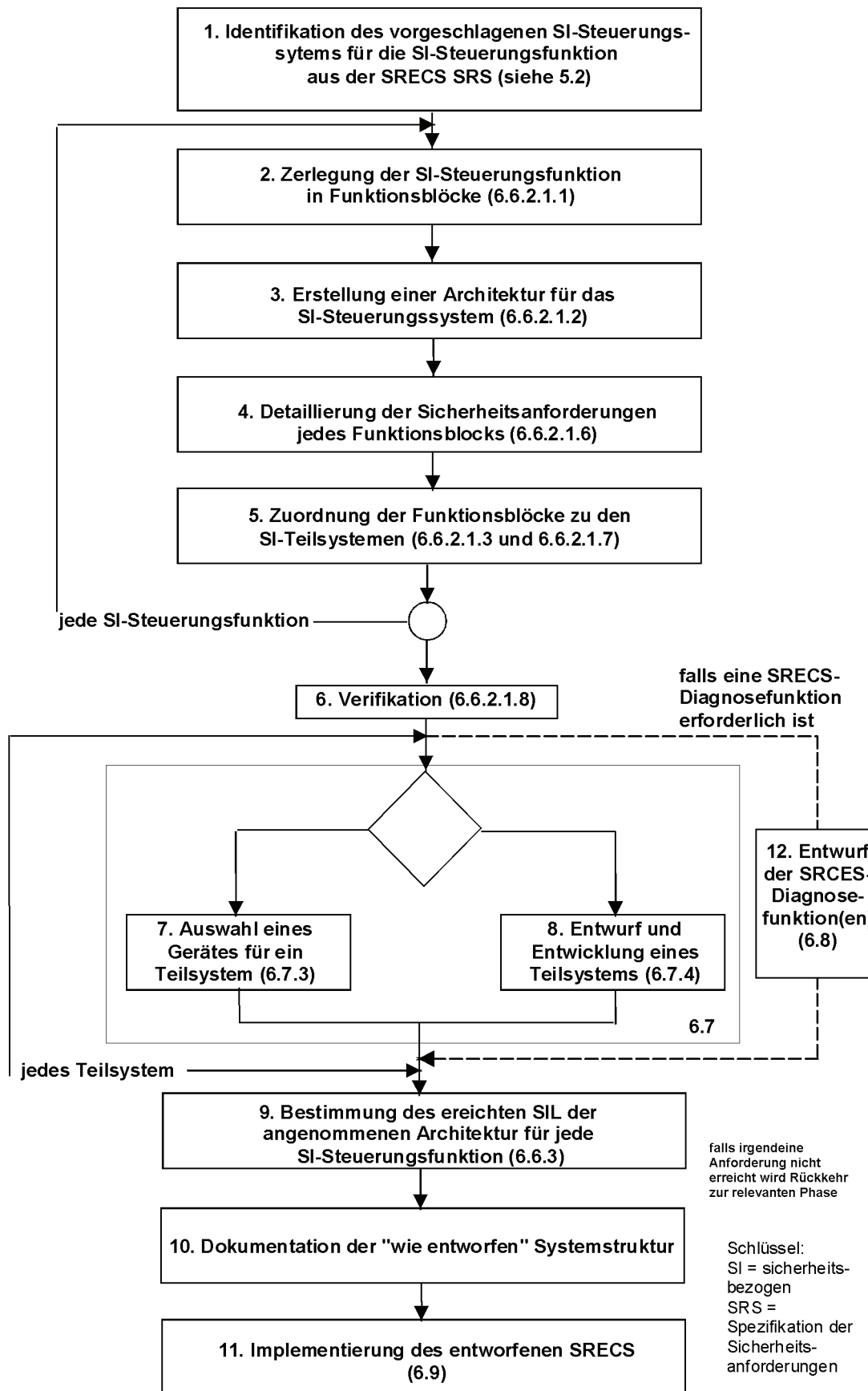


Bild 4 – Arbeitsablauf des SRECS-Entwurfs- und Entwicklungsprozesses

6.6.2.1.2 In Übereinstimmung mit der Struktur der Funktionsblöcke muss eine Architektur des SRECS geschaffen werden.

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

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

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

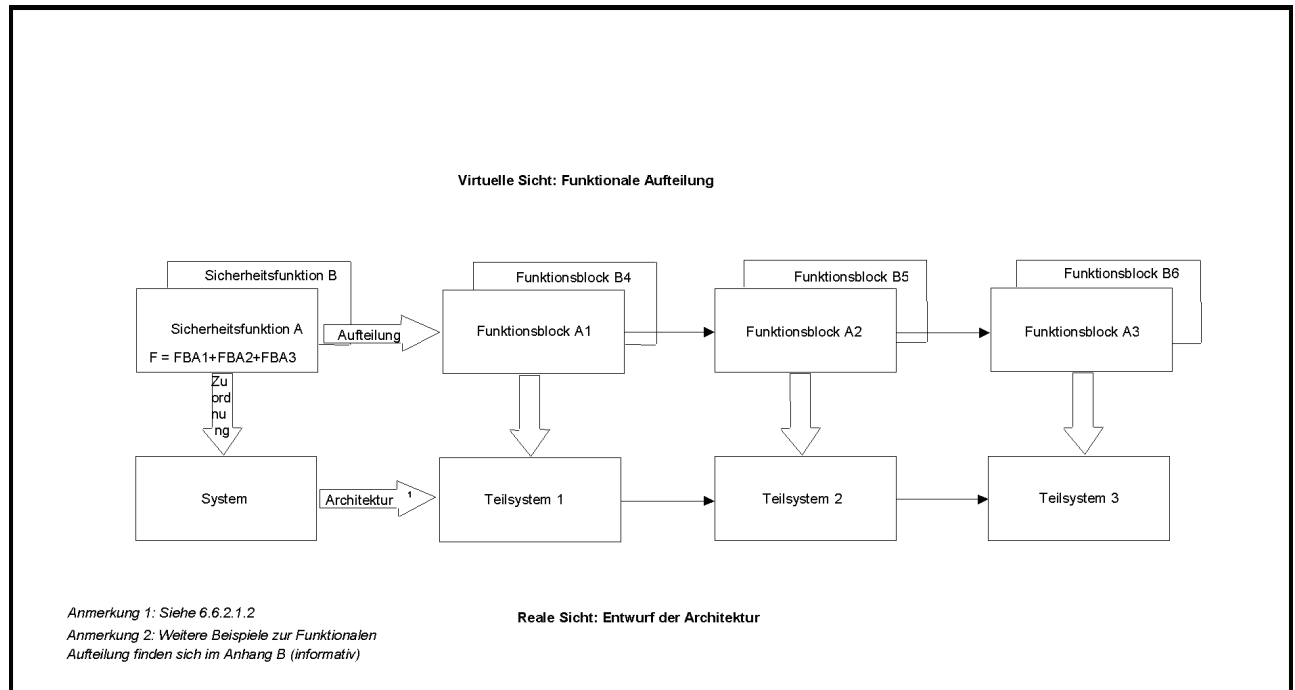


Bild 5 – Zuordnung von Sicherheitsanforderungen der Funktionsblöcke zu Teilsystemen^{N3)}

6.6.2.1.6 Die Sicherheitsanforderungen für jeden Funktionsblock müssen aus der Spezifikation der Sicherheitsanforderungen der entsprechenden sicherheitsbezogenen Steuerungsfunktion in Form von:

- funktionalen Anforderungen (z. B. Eingabe, Funktion und Ausgabe des Funktionsblocks);
- Anforderungen zur Sicherheitsintegrität

abgeleitet werden.

6.6.2.1.7 Die Sicherheitsanforderungen eines Teilsystems müssen diejenigen des(der) ihm zugeordneten Funktionsblocks(blöcke) 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 Spezifikation der Sicherheitsanforderungen des Teilsystems dokumentiert werden.

6.6.2.1.8 Die Architektur muss gegen die Spezifikation der Sicherheitsanforderungen aller zugeordneten sicherheitsbezogenen Steuerungsfunktionen verifiziert werden.

^{N3)} Nationale Fußnote: Anhang B ist gelöscht.

6.6.3 Bestimmung des Sicherheits-Integritätslevels (SIL) des SRECS

6.6.3.1 Allgemeines

Der Sicherheits-Integritätslevel, der für das SRECS in Anspruch genommen werden kann, muss geringer oder gleich dem niedrigsten Wert der SIL-Anspruchsgrenzen für die Sicherheitsintegrität der Hardware, der systematischen Integrität und den strukturellen Einschränkungen von irgendeinem der Teilsysteme sein.

ANMERKUNG Die Abschätzung des SILs des SRECS basiert auf den angenommenen SIL-Anforderungen zu jedem Teilsystem, die in ihrer Spezifikation der Sicherheitsanforderungen festzulegen sind.

6.6.3.2 Sicherheitsintegrität der Hardware

6.6.3.2.1 Die Wahrscheinlichkeit eines Ausfalls jeder sicherheitsbezogenen Steuerungsfunktion infolge gefahrbringender zufälliger Hardwareausfälle muss gleich oder kleiner als der in der Spezifikation der Sicherheitsanforderungen festgelegte Ausfallgrenzwert sein.

6.6.3.2.2 Die Wahrscheinlichkeit eines Ausfalls jeder sicherheitsbezogenen Steuerungsfunktion infolge gefahrbringender zufälliger Hardwareausfälle muss unter Berücksichtigung von Folgendem abgeschätzt werden:

- a) der Architektur des SRECS in Bezug zu jeder betrachteten sicherheitsbezogenen Steuerungsfunktion;

ANMERKUNG Dieses schließt die Entscheidung ein, welche Ausfallarten der Teilsysteme in einer seriellen Konfiguration vorhanden sind (d. h. jeder Ausfall führt zu einem Ausfall der Ausführung der relevanten sicherheitsbezogenen Steuerungsfunktion) und welche in einer parallelen (redundanten) Konfiguration vorhanden sind (d. h. es sind gemeinsam auftretende Ausfälle notwendig, damit die relevante sicherheitsbezogene Steuerungsfunktion ausfällt).

- b) der geschätzten Ausfallrate jedes Teilsystems seine zugeordneten Funktionsblöcke in allen Modi, die zu einem gefahrbringenden Ausfall des SRECS führen können, auszuführen;
- c) der Anfälligkeit des SRECS für Ausfälle infolge gemeinsamer Ursache.

6.6.3.2.3 Die Abschätzung muss auf der Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls jedes relevanten Teilsystems basieren, wie aus den in 6.7.2.3 erforderlichen Informationen, und wo zutreffend 6.7.2.4 für digitale Datenkommunikationsprozesse zwischen Teilsystemen, abgeleitet. Die Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls des Systems ist die Summe der Wahrscheinlichkeiten gefahrbringender zufälliger Hardwareausfälle aller Teilsysteme, die an der Ausführung der sicherheitsbezogenen Steuerungsfunktion beteiligt sind und muss, wo angemessen, die Wahrscheinlichkeit gefahrbringender Übertragungsfehler für digitale Datenkommunikationsprozesse einschließen:

$$P_{DF} = P_{DF1} + \dots + P_{DFn} + P_{TE}$$

ANMERKUNG 1 Dieser Ansatz basiert auf dem Begriff eines Funktionsblocks^{N4)}, die aussagt, dass ein Ausfall irgendeines Funktionsblocks zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion führt (siehe 3.1.24).

ANMERKUNG 2 Andere Verbindungen als digitale Datenkommunikation werden als Teil eines Teilsystems betrachtet.

6.6.3.3 Strukturelle Einschränkungen

Die SIL-Anspruchsgrenze des SRECS auf Grund der strukturellen Einschränkungen ist geringer oder gleich der niedrigsten SIL-Anspruchsgrenze irgendeines Teilsystems (siehe 6.7.5), das an der Ausführung der sicherheitsbezogenen Steuerungsfunktion beteiligt ist.

$$SIL_{SRECS} \leq (SIL_{Teilsystem})_{niedrigst}$$

^{N4)} Nationale Fußnote: Die Definition eines Funktionsblocks ist in 3.1.25 zu finden.

6.6.3.4 Systematische Integrität

Die SIL-Anspruchsgrenze des SRECS auf Grund der systematischen Integrität ist geringer oder gleich der niedrigsten SIL-Anspruchsgrenze irgendeines Teilsystems, das an der Ausführung der sicherheitsbezogenen Steuerungsfunktion beteiligt ist.

$$SIL_{SRECS} \leq (SIL_{Teilsystem})_{niedrigst}$$

ANMERKUNG Die in 6.7.8 beschriebenen Maßnahmen ergeben eine Grenze des SIL-Anspruchs von SIL 3 für die systematische Sicherheitsintegrität eines nach 6.7.4 und 6.7.8 realisierten Teilsystems.

6.7 Realisierung von Teilsystemen

6.7.1 Zweck

Der Zweck ist es, ein Teilsystem zu realisieren, das alle Sicherheitsanforderungen der zugeordneten Funktionsblöcke (siehe Bild 5) erfüllt. Zwei Möglichkeiten sind vorgesehen.

- Auswahl eines Geräts, das ausreichend ist, um die Anforderungen für das Teilsystem zu erfüllen, 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.

6.7.2.2 Das Teilsystem muss so gestaltet sein, das es die Anforderungen a) bis c) wie folgt erfüllt:

- a) die Anforderungen zur Sicherheitsintegrität der Hardware, die Folgendes umfassen:
 - die strukturellen Einschränkungen zur Sicherheitsintegrität der Hardware (siehe 6.7.6), und
 - die Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle (siehe 6.7.7)
- b) die Anforderungen zur systematischen Sicherheitsintegrität, die Folgendes umfassen:
 - die Anforderungen zur Vermeidung von Ausfällen (siehe 6.7.8.1) und die Anforderungen zur Beherrschung systematischer Fehler (siehe 6.7.8.2), oder
 - Nachweis, das die Einrichtungen "betriebsbewährt" sind. In diesem Fall muss das Teilsystem die relevanten Anforderungen von IEC 61508-2 erfüllen (siehe IEC 61508-2, 7.4.7.5 – 7.4.7.12).
- c) die Anforderungen an das Verhalten des Teilsystems bei Erkennung eines Fehlers (Fehlerreaktion) (siehe 6.3).

6.7.2.3 Die folgenden Informationen müssen für jedes Teilsystem vorhanden sein:

- a) eine funktionale Spezifikation derjenigen Funktionen und Schnittstellen des Teilsystems, die für sicherheitsbezogene Steuerungsfunktionen verwendet werden können;
- b) für komplexe Teilsysteme, die geschätzten Ausfallraten (auf Grund gefahrbringender zufälliger Hardwareausfälle) in allen Modi, die zu einem gefahrbringenden Ausfall des Teilsystems führen, die:
 - durch Diagnosetests erkannt werden; und
 - durch Diagnosetests nicht erkannt werden.

ANMERKUNG Ein erkannter Ausfall wird zu einem ungefährlichen Ausfall, wenn eine angemessene Fehlerreaktionsfunktion ausgeführt wird. Dies ist auf Systemebene im Zusammenhang mit den vorgesehenen Sicherheitsfunktionen relevant.

E DIN IEC 62061 (VDE 0113 Teil 50):2003-06

- c) für einfache Teilsysteme, den Schwellenwert für die Ausfallrate (auf Grund gefahrbringender zufälliger Hardwareausfälle), angegeben in allen Modi, die zu einen gefahrbringenden Ausfall des SRECS führen können;
- d) Einschränkungen für das Teilsystem in Bezug auf:
 - die Umgebung, die beachtet werden sollte, um die Gültigkeit der geschätzten Ausfallraten auf Grund zufälliger Hardwareausfälle zu gewährleisten; und
 - die Gebrauchsdauer des Teilsystems, die nicht überschritten werden sollte, um die Gültigkeit der geschätzten Ausfallraten auf Grund zufälliger Hardwareausfälle zu gewährleisten;
- e) alle Anforderungen zu Test und/oder Instandhaltung;
- f) der Diagnosedeckungsgrad und das Diagnose-Testintervall (falls erforderlich, siehe Anmerkung 1);

ANMERKUNG 1 Der obige Punkt f) bezieht sich auf interne 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.

- g) jede zusätzliche Information (z. B. Reparaturzeiten), die notwendig ist, um die Ableitung einer mittleren Zeit bis zur Wiederherstellung (MTTR) zu ermöglichen, die auf die Erkennung eines Fehlers durch die Diagnose folgt;

ANMERKUNG 2 Die Punkte b) bis g) sind nötig, um die Abschätzung der Wahrscheinlichkeit eines Ausfalls der sicherheitsbezogenen Steuerungsfunktion bei Anforderung oder der Wahrscheinlichkeit eines Ausfalls der sicherheitsbezogenen Steuerungsfunktion pro Stunde zu erlauben.

ANMERKUNG 3 Die Punkte b), c), f) und g) sind als separate Parameter nur für Teilsysteme wie Sensoren und Aktoren erforderlich, die in redundanten Architekturen kombiniert werden können, um die Sicherheitsintegrität der Hardware zu verbessern. Für Teile wie Logiksteuerungen, die selbst nicht in redundanten Strukturen im SRECS kombiniert werden, ist es ausreichend, die Leistungsfähigkeit als Wahrscheinlichkeit eines Ausfalls bei Anforderung oder Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde unter Berücksichtigung der Punkte b), f) und g) festzulegen. Für solche Teile (z. B. Logiksteuerungen) ist es auch notwendig, das Intervall für die Wiederholungsprüfung für nicht erkannte Ausfälle festzusetzen.

- h) jegliche Information, die notwendig ist, um die Ableitung des Anteils sicherer Ausfälle (SFF) des Teilsystems, wie es im SRECS Verwendung findet, zu ermöglichen;

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

ANMERKUNG 5 Siehe 6.7.6.4 zu Einzelheiten zur Abschätzung des SFF.

- i) die Fehlertoleranz der Hardware des Teilsystems;

ANMERKUNG 6 Die Punkte h) und i) sind nötig, um den höchsten Sicherheits-Integritätslevel, der gemäß den strukturellen Einschränkungen für eine sicherheitsbezogene Steuerungsfunktion in Anspruch genommen werden kann, zu bestimmen.

Die Punkte h) und i) können verwendet werden, um eine Verbindung zu den Kategorie-Anforderungen von ISO 13849-1/EN 954-1 sowohl in Form von Fehlererkennung, als auch der Fehlertoleranz der Hardware bereitzustellen.

- j) alle Grenzen für die Anwendung des Teilsystems, die zur Vermeidung von systematischen Ausfällen beachtet werden sollten;
- k) den höchsten Sicherheits-Integritätslevel, der für eine sicherheitsbezogene Steuerungsfunktion 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.
- l) jede Information, die erforderlich ist, um die Hardware- und Softwarekonfiguration des Teilsystems zu identifizieren, um das Konfigurationsmanagement des SRECS in Übereinstimmung mit 6.11.3.2 zu ermöglichen.

6.7.2.4 Die Wahrscheinlichkeit gefahrbringender Übertragungsfehler von digitalen Datenkommunikationsprozessen.

6.7.3 Anforderungen zur Auswahl vorhandener (bereits entwickelter) Teilsysteme

6.7.3.1 Wo ein Lieferant ein Teilsystem für eine spezifische sicherheitsbezogene Steuerungsfunktion, die in der Spezifikation der Sicherheitsanforderungen aufgeführt ist, vorsieht, kann ein solches bereits entwickeltes Teilsystem anstatt eines angepassten Entwurfs ausgewählt werden, vorausgesetzt, dass es sowohl die Anforderungen der Spezifikation der Sicherheitsanforderungen des Teilsystems, als auch 6.7.3.2 oder 6.7.3.3 erfüllt.

6.7.3.2 Teilsysteme, die komplexe Komponenten enthalten, müssen entsprechend dem erforderlichen SIL IEC 61508 entsprechen.

6.7.3.3 Teilsysteme, die aus einfachen Bauteilen niedriger Komplexität bestehen, müssen nur mit den Abschnitten 6.7.4.4, 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 Zwecke

6.7.4.1.1 Der erste Zweck ist es, ein Teilsystem zu entwerfen, das die Sicherheitsanforderungen der zugeordneten Funktionsblöcke erfüllt.

6.7.4.1.2 Der zweite Zweck ist es, Teilsystem-Elemente zu verwenden, die in Kombination zusammenwirken, um die funktionalen Anforderungen und die Anforderungen zur Sicherheitsintegrität aller dem Teilsystem zugeordneten Funktionsblöcke zu erfüllen.

ANMERKUNG Um die Fehlertoleranz der Hardware zu erhöhen, kann der zugeordnete Funktionsblock durch redundante Teilsystem-Elemente ausgeführt werden. Darum kann es notwendig sein, den Funktionsblock in Funktionsblock-Elemente aufzuteilen, die getrennt zu den Teilsystem-Elementen zugeordnet werden können (siehe Bild 7).

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 Wenn der Entwurf eines Teilsystems ein komplexes Bauteil (als ein Teilsystem-Element) enthält, das alle relevanten Anforderungen aus IEC 61508 für den erforderlichen Sicherheits-Integritätslevel erfüllt, kann dieses Teilsystem als einfaches Bauteil im Zusammenhang eines Entwurfs eines Teilsystems betrachtet werden, da seine relevanten Ausfallmodi, Verhalten bei Erkennung eines Fehlers, geschätzte Ausfallrate und andere sicherheitsrelevante Informationen bekannt sind. Dieses Bauteil darf nur in Übereinstimmung mit 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 festgelegten Prozess folgen, der alle Aspekte des in Bild 6 gezeigten Prozesses abdeckt.

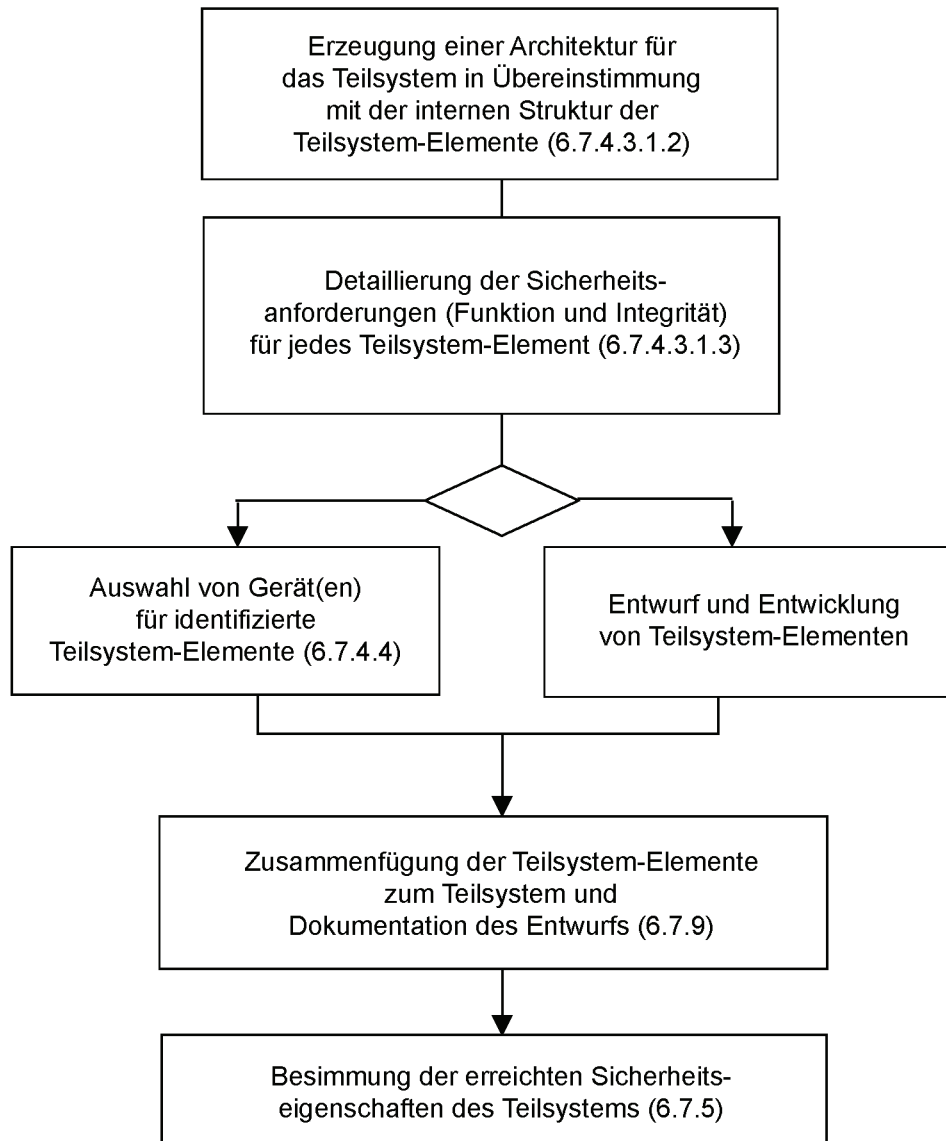


Bild 6 – Arbeitsablauf für Entwurf und Entwicklung eines Teilsystems (siehe Kästchen 8 von Bild 4)

6.7.4.3.1 Entwurf der Architektur des Teilsystems

ANMERKUNG Der Aufteilungsprozess auf Ebene von Teilsystemen sollte zu einer Struktur von Funktionsblock-Elementen führen, die die funktionalen Anforderungen des Funktionsblocks vollständig beschreiben. Dieser Prozess sollte bis auf die Ebene angewendet werden, die es erlaubt, die für jedes Funktionsblock-Element festgelegten funktionalen Anforderungen Teilsystem-Elementen zuzuordnen.

6.7.4.3.1.1 Die interne Struktur der Funktionsblöcke, die einem Teilsystem zugeordnet sind, muss unter dem Gesichtspunkt ihrer Funktionsblock-Elemente und ihrer gegenseitigen Beziehungen innerhalb des Funktionsblocks beschrieben werden.

6.7.4.3.1.2 Es muss eine Architektur des Teilsystems in Übereinstimmung mit der internen Struktur der Teilsystem-Elemente (d. h. die Funktionsblock-Elemente der zugeordneten Funktionsblock(blöcke) und ihre gegenseitigen Beziehungen) erstellt werden.

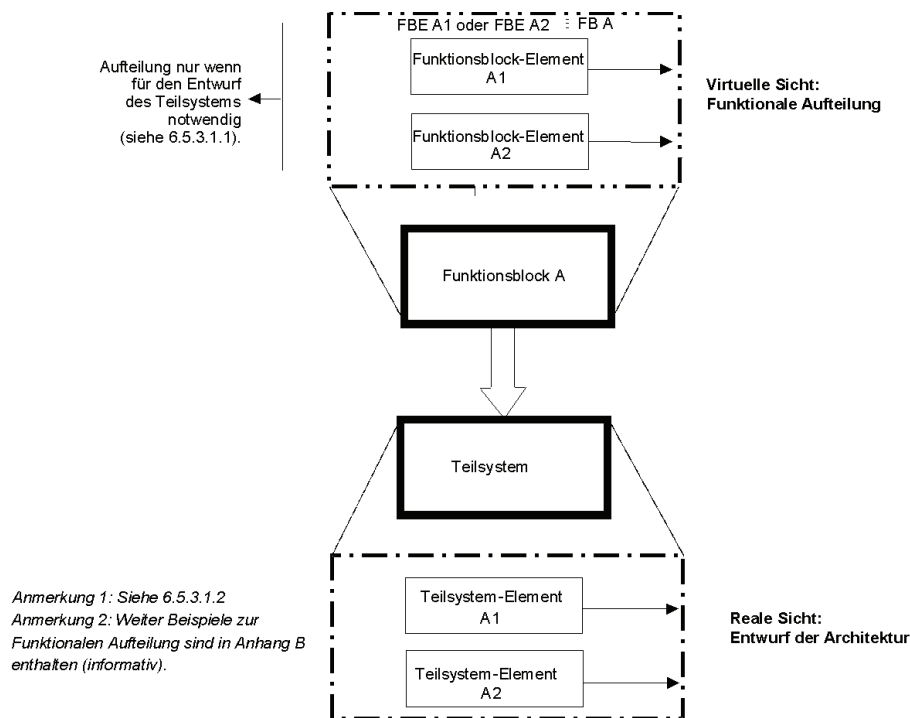


Bild 7 – Aufteilung der Funktionsblöcke in Funktionsblock-Elemente und ihre zugehörigen Teilsystem-Elemente^{N5)}

6.7.4.3.1.3 Die Architektur des Teilsystems muss unter dem Gesichtspunkt der Teilsystem-Elemente des Teilsystems und ihrer gegenseitigen Beziehungen dokumentiert werden.

ANMERKUNG Der Ablauf des Entwurfsprozesses ist in Bild 6 gezeigt.

6.7.4.4 Anforderungen für die Auswahl und den Entwurf der Teilsystem-Elemente

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

- eine funktionale Spezifikation des Teilsystem-Elements;
- Spezifikation der Schnittstellen des Teilsystem-Elements (z. B. elektrische Eigenschaften);
- jeder Ausfallmodus und seine Auftretswahrscheinlichkeit und wenn relevant (z. B. für komplexe Bauteile, die in Übereinstimmung mit 6.7.4.2.2 verwendet werden), der Diagnosedeckungsgrad und die Wahrscheinlichkeit gefährbringender Ausfälle.
- Einschränkungen für das Teilsystem-Element in Bezug auf:
 - die Umgebung, die beachtet werden sollte, um die Gültigkeit der unter b) angegebenen Informationen zu gewährleisten; und
 - die Gebrauchsdauer des Teilsystem-Elements, die nicht überschritten werden sollte, um die Gültigkeit der unter b) angegebenen Informationen zu gewährleisten;
- jede wiederkehrende Wiederholungsprüfung und/oder Instandhaltungsanforderungen;
- Eigenschaften, die zur Diagnose beitragen können (z. B. Kontakte mit Zwangsführung);

^{N5)} Nationale Fußnote: Die Unterabschnitte 6.5.3.1.1 und 6.5.3.1.2 existieren nicht, Anhang B ist gelöscht.

- g) jede zusätzliche Information (z. B. Reparaturzeiten), die notwendig ist, 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) Fehlertoleranz der Hardware.

6.7.5 Bestimmung der sicherheitsbezogenen Leistungsfähigkeit des Teilsystems

Die sicherheitsbezogene Leistungsfähigkeit eines Teilsystems ist durch die SIL-Anspruchsgrenze gekennzeichnet, die durch seine strukturellen Einschränkungen (6.7.6), seine SIL-Anspruchsgrenze auf Grund systematischer Integrität (6.7.8) und seine Wahrscheinlichkeit eines gefahrbringenden zufälligen Hardwareausfalls (6.7.7) bestimmt ist.

ANMERKUNG 1 Die SIL-Anspruchsgrenze 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 sicherheitsbezogene Steuerungsfunktion 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 sicherheitsbezogene Steuerungsfunktion in Anspruch genommen werden kann, durch die Fehlertoleranzen der Hardware und die Anteile sicherer Ausfälle der Teilsysteme, die die sicherheitsbezogene Steuerungsfunktion ausführen, begrenzt. Die Tabelle 2 legt den höchsten Sicherheits-Integritätslevel fest, der für eine sicherheitsbezogene Steuerungsfunktion in Anspruch genommen werden kann, die ein Teilsystem verwendet. Dabei wird die Fehlertoleranz der Hardware und der Anteil sicherer Ausfälle dieses Teilsystems betrachtet. Die in Tabelle 2 angegebenen strukturellen Einschränkungen müssen auf jedes Teilsystem angewendet werden. Im Hinblick auf diese Anforderungen:

- a) bedeutet eine Fehlertoleranz der Hardware von N, dass N+1 Fehler zu einem Verlust der sicherheitsbezogenen Steuerungsfunktion führen können. Bei der Bestimmung der Fehlertoleranz der Hardware darf keine Berücksichtigung von anderen Maßnahmen erfolgen, 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;
- c) können bei der Bestimmung der Fehlertoleranz der Hardware 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 Anmerkung 3^{N6)}).

ANMERKUNG 1 Ein erkannter Fehler wird ein ungefährlicher Ausfall, wenn eine angemessene Fehlerreaktionsfunktion ausgeführt worden ist. Dies ist auf Systemebene im Zusammenhang mit den vorgesehenen Sicherheitsfunktionen relevant. Ob ein Ausfall ein ungefährlicher oder ein gefahrbringender Ausfall ist, hängt von dem SRECS und den vorgesehenen Sicherheitsfunktionen ab.

ANMERKUNG 2 Die Architektur und das abgeleitete Teilsystem zur Erfüllung der Anforderungen zur Fehlertoleranz der Hardware sind die unter normalen Betriebsbedingungen verwendeten. Die Anforderungen zur Fehlertoleranz können verringert werden, während das SRECS im Betrieb repariert wird. Jedoch müssen die Schlüsselparameter in Bezug auf jede Verringerung vorher bewertet worden sein (zum Beispiel Zeit bis zur Wiederherstellung im Vergleich zur Wahrscheinlichkeit einer Anforderung).

6.7.6.2 Die strukturellen Einschränkungen der Tabelle 2 müssen auf jedes Teilsystem, das eine sicherheitsbezogene Steuerungsfunktion ausführt (d. h. als ein Funktionsblock), angewendet werden.

^{N6)} Nationale Fußnote: Anmerkung 3 ist nicht vorhanden.

Tabelle 2 – Strukturelle Einschränkungen von Teilsystemen: Maximal in Anspruch nehmbarer SIL für eine sicherheitsbezogene Steuerungsfunktion, die dieses Teilsystem verwendet

Anteil sicherer Ausfälle	Fehlertoleranz der Hardware (siehe Anmerkung 1)		
	0	1	2
< 60 %	nicht erlaubt (siehe Anmerkung 3)	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 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 Fehlertoleranz der Hardware von N bedeutet, dass N + 1 Fehler zu einem Verlust der Sicherheitsfunktion führen können.			
ANMERKUNG 2 Ein SIL 4 Anspruch wird in dieser Norm nicht betrachtet, da er für die Anforderungen zur Risikominderung, die normalerweise bei Maschinen anzutreffen sind, nicht relevant ist. Zu SIL 4 siehe IEC 61508.			
ANMERKUNG 3 Ausnahme siehe 6.7.6.4.			

6.7.6.3 Wenn ein Teilsystem in Übereinstimmung mit ISO 13849-1:1996 entworfen und gemäß prEN 954-2 validiert worden ist, kann die folgende Korrelation allein in Bezug auf die strukturellen Einschränkungen in Übereinstimmung mit Tabelle 3 angewendet werden.

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

Tabelle 3 – Strukturelle Einschränkungen

Kategorie	Fehlertoleranz der Hardware	SFF	Maximale SIL-Anspruchsgrenze in Bezug auf die strukturellen Einschränkungen
	Es wird angenommen, dass Teilsysteme mit der angegebenen Kategorie die unten angegebenen Merkmale besitzen.		
1	0	< 60 %	Siehe 6.7.6.4
2	0	60 ... 90 %	SIL 1
3	1	< 60 %	SIL 1
	1	60 ... 90 %	SIL 2
4	>1	60 ... 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 % ist, werden im Zusammenhang von ISO 13849-1 als nicht relevant betrachtet und Teilsysteme, die in Übereinstimmung mit ISO 13849-1 entworfenen sind, werden in Praxis einen SFF erreichen, der oberhalb von 60 % liegt.

ANMERKUNG 2 Der Fall einer Kategorie 2, bei der der Anteil sicherer Ausfälle > 90 % ist, wird so betrachtet, dass er durch die Entwurfsanforderungen von ISO 13849-1 nicht erreicht wird.

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

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

ANMERKUNG 5 Es wird angenommen, dass ein Teilsystem mit einer bestimmten Kategorie in Übereinstimmung mit ISO 13849-1 eine zugehörige Fehlertoleranz der Hardware und einen Anteil sicherer Ausfälle besitzt, wie in Tabelle 6.2^{N7)} angezeigt.

ANMERKUNG 6 Kategorie B gemäß ISO 13849-1:1996 kann für sich allein nicht als ausreichend betrachtet werden, um SIL 1 zu erreichen.

6.7.6.4 Abschätzung des Anteils sicherer Ausfälle (SFF)

6.7.6.4.1 Der SFF muss abgeschätzt werden, wo es erforderlich ist, die SIL-Anspruchsgrenze auf Grund struktureller Einschränkungen zu bestimmen.

6.7.6.4.2 Zur Abschätzung der SFF muss eine Analyse (z. B. Fehlerbaumanalyse, Ausfallarten- und Effektanalyse) ausgeführt werden, um alle relevanten Fehler und ihre korrespondierenden Ausfallmodi zu bestimmen. Die Wahrscheinlichkeit jeder Ausfallart muss auf Basis der Wahrscheinlichkeit der zugehörigen Fehler bestimmt werden.

6.7.6.4.3 Die Wahrscheinlichkeit jedes zugehörigen Fehlers muss abgeleitet werden aus:

- a) verlässlichen Daten zu Ausfallraten, die durch Felderfahrung gewonnen wurden; oder
- b) BauteilAusfalldaten aus einer anerkannten industriellen Quelle (siehe Referenzen in Anhang E); oder
- c) in Anhang E angegebenen Ausfallmodi und Daten zu Ausfallraten; oder
- d) Daten zu Ausfallraten, die aus den Ergebnissen von Tests und Analyse abgeleitet sind (noch zu entwickeln).

Ausnahme: Für ein Teilsystem mit einer Fehlertoleranz der Hardware von Null und niedriger Wahrscheinlichkeit eines Ausfalls dieses Teilsystems im Vergleich zum Zielwert der Wahrscheinlichkeit gefahrbringender Ausfälle des Teilsystems gilt:

- wenn Fehler, die zu einem gefahrbringenden Ausfall führen können, ausgeschlossen worden sind, so dass der SFF nicht abgeschätzt werden kann, ist die Sicherheitsintegrität dieses Teilsystems auf Grund struktureller Einschränkungen auf eine Anspruchsgrenze von SIL 1 begrenzt; oder

^{N7)} Nationale Fußnote: Tabelle 6.2 existiert nicht, es ist Tabelle 3 gemeint.

- wenn Fehler derart sind, dass der Ausfall in die ungefährliche Richtung orientiert ist, so dass der SFF nicht abgeschätzt werden kann, ist die Sicherheitsintegrität dieses Teilsystems auf Grund struktureller Einschränkungen auf eine Anspruchsgrenze von SIL 2 begrenzt;

Die Anwendung von Fehlerausschlüssen und Annahmen zu ungefährlichen Ausfallmodi müssen begründet und dokumentiert werden.

ANMERKUNG 1 Es kann zulässig sein, Fehlerausschlüsse in Übereinstimmung mit 3.3 und Tabelle D.5 von prEN 954-2 vorzunehmen.

ANMERKUNG 2 Niedrig im Zusammenhang mit der Wahrscheinlichkeit eines Ausfalls dieses Teilsystems im Vergleich zum Zielwert der Wahrscheinlichkeit gefahrbringender Ausfälle des Teilsystems kann zumindest eine Größenordnung bedeuten (d. h. ein Faktor von 10).

6.7.7 Anforderungen zur Wahrscheinlichkeit gefahrbringender zufälliger Hardwareausfälle von Teilsystemen

6.7.7.1 Allgemeine Anforderungen

6.7.7.1.1 Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls muss gleich oder kleiner dem in der Spezifikation der Sicherheitsanforderungen des Teilsystems (siehe 6.6.3.2) festgelegten Ausfallgrenzwert sein.

6.7.7.1.2 Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls jedes Teilsystems infolge 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 Dieses schließt die Entscheidung ein, ob eine Fehlertoleranz der Hardware 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 infolge gemeinsamer Ursache (siehe Anmerkungen 2 und 11^{N8)});

ANMERKUNG 2 Für weitere Anleitung zur Quantifizierung der Auswirkung von hardwarebezogenen Ausfällen infolge gemeinsamer Ursache siehe auch IEC 61508-6, Anhang D.

- e) dem Diagnosedeckungsgrad der Diagnosetests (siehe 3.1.32) und dem zugehörigen Diagnose-Testintervall;
- f) den Intervallen, innerhalb denen Wiederholungsprüfungen ausführt werden müssen, um gefahrbringende Fehler zu erkennen, die durch Diagnosetests nicht erkannt werden (siehe auch IEC 61508-2);
- g) den Reparaturzeiten für erkannte Fehler.

ANMERKUNG 3 Die Reparaturzeit bildet einen Teil der mittleren Zeit bis zur Wiederherstellung (siehe IEC 191-13-08), 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, zum Beispiel 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 Es steht eine Anzahl von Modellierungsmethoden zur Verfügung und die Auswahl der am besten passenden Methode ist Sache des Analytikers und wird von den Umständen abhängen. Verfügbare Methoden schließen ein:

^{N8)} Nationale Fußnote: Anmerkung 11 ist nicht vorhanden, der Hinweis gilt für Anmerkung 5.

E DIN IEC 62061 (VDE 0113 Teil 50):2003-06

- Fehlerbaum-Analyse (siehe B.6.6.5 von IEC 61508-7);
- Markov-Modelle (siehe C.6.4 von IEC 61508-7);
- Zuverlässigkeits-Blockdiagramme (siehe C.6.5 von IEC 61508-7).

ANMERKUNG 5 Ausfälle infolge gemeinsamer Ursachenfolgen und Datenkommunikationsprozesse können von anderen Effekten als tatsächlichen Ausfällen von Hardwarebauteilen herrühren (z. B. elektromagnetischer Beeinflussung, Dekodierfehlern, usw.). Solche Ausfälle werden im Sinne dieser Norm jedoch als zufällige Hardwareausfälle betrachtet.

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

ANMERKUNG Dieses Diagnose-Testintervall hat so zu sein, dass ein Fehler erkannt wird, bevor die Wahrscheinlichkeit des Auftretens eines nachfolgenden Fehlers, der zu einem gefährbringenden Ausfall des Teilsystems führen kann.

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

Ausnahme: Im Falle eines Teilsystems, dass eine besondere sicherheitsbezogene Steuerungsfunktion ausführt, bei der das Verhältnis der Diagnose-Testrate zur Anforderungsrate den Wert 100 überschreitet, muss das Diagnose-Testintervall dieses Teilsystems so gewählt werden, dass das Teilsystem die Anforderung zur Wahrscheinlichkeit eines gefährbringenden zufälligen Hardwareausfalls erfüllen kann.

6.7.7.1.5 Wenn ein einfaches Teilsystem niedriger Komplexität in Übereinstimmung mit ISO 13849-1:1996 entworfen und gemäß prEN 954-2 validiert worden ist, kann die folgende Korrelation allein in Bezug auf die Wahrscheinlichkeit gefährbringender Ausfälle (P_{DF}) in Übereinstimmung mit Tabelle 4 angewendet werden.

ANMERKUNG Um einen erforderlichen SIL zu erreichen, ist es ebenso notwendig, die Anforderungen zu strukturellen Einschränkungen und zur systematischen Integrität zu erfüllen.

Tabelle 4 – Wahrscheinlichkeit gefährbringender Ausfälle

Kategorie	Fehlertoleranz der Hardware	DC	P_{DF} Grenzwert (pro Stunde), der für das Teilsystem in Anspruch genommen werden kann $P_{DF}(MTTF_{Teilsystem}, T_{Test}, DC)^1$
	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 E)
2	0	60 ... 90 %	$\leq 10^{-5}$
3	1	60 ... 90 %	$\leq 10^{-6}$
4	> 1	60 ... 90 %	$\leq 10^{-7}$
	1	> 90 %	$\leq 10^{-7}$
ANMERKUNG 1 Der P_{DF} 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 prEN 954-2, 3.5 erforderlich) und dem Diagnosedeckungsgrad wie in Tabelle 4 gezeigt (diese Werte basieren auf den Anforderungen der in ISO 13849-1 beschriebenen Kategorien). ANMERKUNG 2 Kategorie B gemäß ISO 13849-1:1996 kann für sich allein nicht als ausreichend betrachtet werden um SIL 1 zu erreichen.			

6.7.7.2 Vereinfachter Ansatz zur Abschätzung der Wahrscheinlichkeit gefährbringender zufälliger Hardwareausfälle von Teilsystemen

6.7.7.2.1 Allgemeines

Dieser Unterabschnitt beschreibt einen vereinfachten Ansatz zur Abschätzung der Wahrscheinlichkeit gefährbringender zufälliger Hardwareausfälle für eine Anzahl von grundlegenden Teilsystemarchitekturen und enthält Formeln für einfache Teilsystem-Elemente niedriger Komplexität oder komplexe Teilsystem-Elemente, die IEC 61508 einhalten. Die Formeln selbst stellen eine Vereinfachung der Zuverlässigkeitsanalyse dar und sind dazu bestimmt, Abschätzungen in die sichere Richtung bereitzustellen.

ANMERKUNG Die erhaltenen Ergebnisse stellen eine Einschränkung in Bezug auf die Wahrscheinlichkeit gefährbringender zufälliger Hardwareausfälle von Teilsystemen dar und in Fällen, wo dieses unakzeptabel erscheint, ist es möglich, die in 6.7.7.1 beschriebenen Modellierungsmethoden anzuwenden, um eine eher genauere Abschätzung zu erhalten.

6.7.7.2.2 Basis-Teilsystemarchitektur A: Nullfehlertoleranz ohne Diagnosefunktion

Jeder gefährbringende Ausfall eines Teilsystem-Elements führt zu einem Ausfall der sicherheitsbezogenen Steuerungsfunktion. Für das Teilsystem ergibt sich die Wahrscheinlichkeit eines gefährbringenden Ausfalls des Teilsystems aus der Summe der Wahrscheinlichkeiten gefährbringender Ausfälle aller Teilsystem-Elemente:

$$P_{DFssA} = P_{DFe1} + \dots + P_{DFen}$$

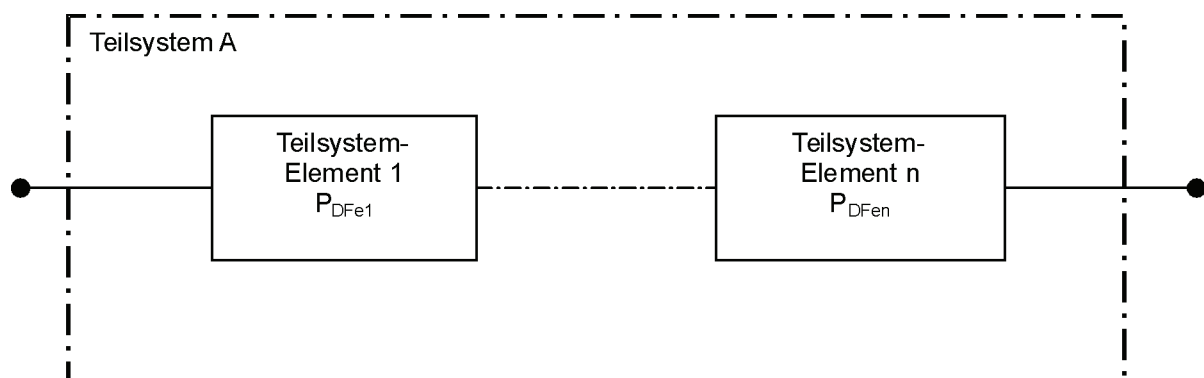


Bild 8 – Teilsystem A: logische Sicht

ANMERKUNG Bild 8 stellt eine logische Sicht der Architektur des Teilsystems A dar und sollte nicht als seine physikalische Implementierung betrachtet werden. (Beispiele zur physikalischen Implementierung sind noch zu entwickeln)

6.7.7.2.3 Basis-Teilsystemarchitektur B: Einfehlertoleranz ohne Diagnosefunktion

Diese Architektur ist so ausgelegt, dass ein einzelner Ausfall irgendeines Teilsystem-Elements nicht zu einem Verlust der sicherheitsbezogenen Steuerungsfunktion führt. Deshalb müsste ein gefährbringender Ausfall in mindestens mehr als einem Element vorliegen, bevor ein Ausfall der sicherheitsbezogenen Steuerungsfunktion auftreten kann. Für das Teilsystem beträgt die Wahrscheinlichkeit eines gefährbringenden Ausfalls des Teilsystems:

$$P_{DFssB} = \text{noch zu entwickeln}$$

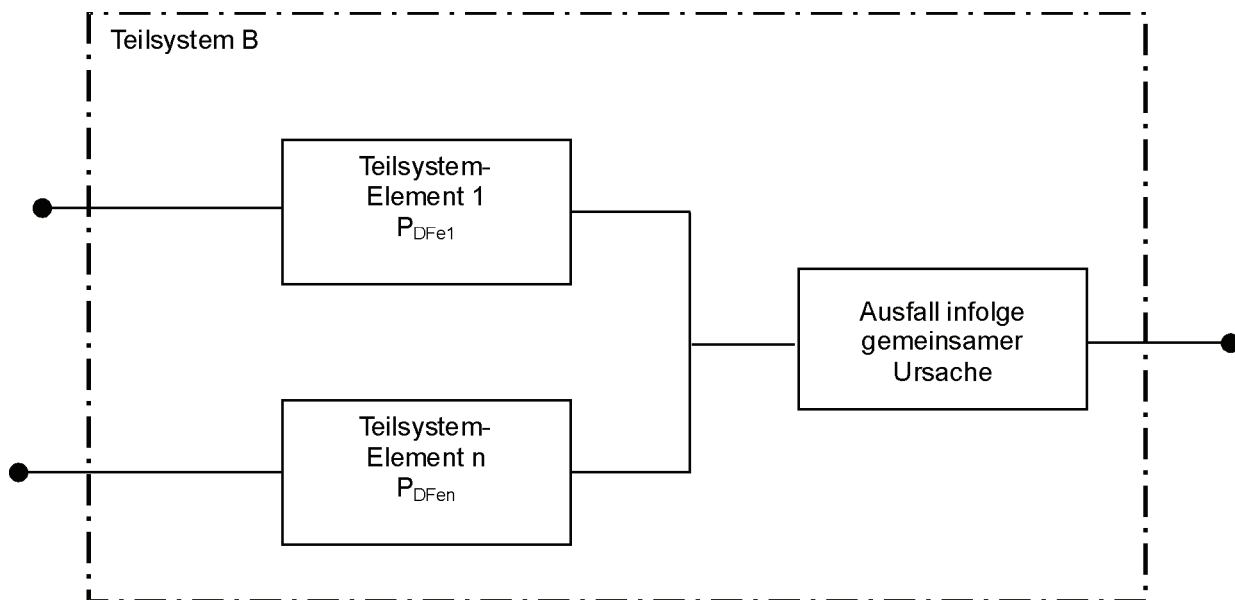


Bild 9 – Teilsystem B: logische Sicht

ANMERKUNG Bild 9 stellt eine logische Sicht der Architektur des Teilsystems B dar und sollte nicht als seine physikalische Implementierung betrachtet werden. (Beispiele zur physikalischen Implementierung sind noch zu entwickeln)

6.7.7.2.3 Basis-Teilsystemarchitektur C: Nullfehlertoleranz mit Diagnosefunktion^{N9)}

Jeder unerkannte gefahrbringende Ausfall eines Teilsystem-Elements führt zu einem gefahrbringenden Ausfall der sicherheitsbezogenen Steuerungsfunktion. Wenn ein Ausfall eines Teilsystem-Elements erkannt wird, leitet(n) die Diagnosefunktion(en) eine Fehlerreaktionsfunktion ein. Für das Teilsystem beträgt die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Teilsystems:

$$P_{DFssC} = P_{DFe1}(1 - DC_{D1}) + \dots + P_{DFen}(1 - DC_{Dn})$$

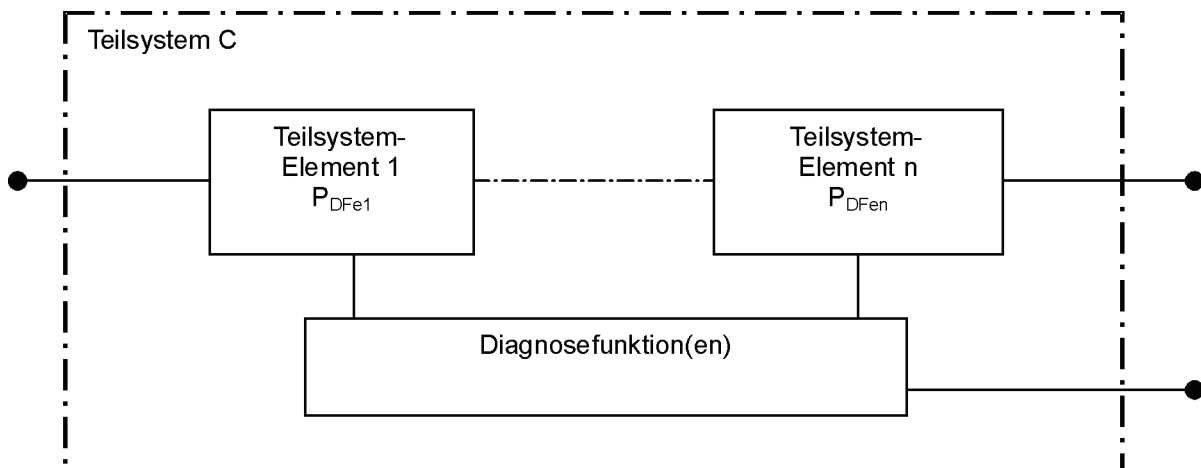


Bild 10 – Teilsystem C: logische Sicht

ANMERKUNG 1 Bild 10 stellt eine logische Sicht der Architektur des Teilsystems C dar und sollte nicht als seine physikalische Implementierung betrachtet werden. Die gezeigte Diagnose kann durchgeführt werden durch:

- das Teilsystem, für das die Diagnose erforderlich ist; oder
- andere Teilsysteme des SRECS; oder

^{N9)} Nationale Fußnote: Die korrekte Nummerierung dieses Unterabschnitts muss 6.7.7.2.4 lauten

- Teilsysteme, die nicht an der Ausführung der Sicherheitsfunktion beteiligt sind.

(Beispiele zur physikalischen Implementierung sind noch zu entwickeln)

ANMERKUNG 2 Für ein Teilsystem C sollte die Abschätzung der P_{DF} die Wahrscheinlichkeit eines Ausfalls der relevanten Diagnosefunktion(en) in Betracht ziehen. Der Beitrag der Diagnosefunktion(en) kann durch einen Faktor, abhängig vom erreichten SIL-Anspruch des Teilsystems, das die Diagnosefunktion(en) ausführt, geändert werden. Dies kann durch Anpassung des Diagnosedeckungsgrads wie folgt berücksichtigt werden:

SIL-Anspruch	DC-Anpassungsfaktor
SIL 1	<i>noch festzulegen</i>
SIL 2	<i>noch festzulegen</i>
SIL 3	<i>noch festzulegen</i>

Die Wahrscheinlichkeit gefahrbringender Ausfälle kann durch Modellierung von Zuverlässigkeitsblockdiagrammen und Analysemethoden wie folgt abgeschätzt werden:

$$P_{DF} = (1 - (\text{Diagnosedeckungsgrad} \times F_{\text{mod}}))P_d$$

mit P_{ud} Wahrscheinlichkeit eines unerkannten gefahrbringenden Ausfalls,

P_d Wahrscheinlichkeit eines gefahrbringenden Ausfalls,

DC Diagnosedeckungsgrad,

F_{mod} Anpassungsfaktor.

6.7.7.2.4 Basis-Teilsystemarchitektur D: Einfehlertoleranz mit Diagnosefunktion(en)^{N10)}

Diese Architektur ist so ausgelegt, dass ein einzelner Ausfall irgendeines Teilsystem-Elements nicht zu einem Verlust der sicherheitsbezogenen Steuerungsfunktion führt. Jeder unerkannte gefahrbringende Ausfall eines Teilsystem-Elements führt zu einem gefahrbringenden Ausfall der sicherheitsbezogenen Steuerungsfunktion. Wenn ein Ausfall eines Teilsystem-Elements erkannt wird, leitet(n) die Diagnosefunktion(en) eine Fehlerreaktionsfunktion ein. Für das Teilsystem beträgt die Wahrscheinlichkeit eines gefahrbringenden Ausfalls des Teilsystems:

^{N10)} Nationale Fußnote: Die korrekte Nummerierung dieses Unterabschnitts muss 6.7.7.2.5 lauten.

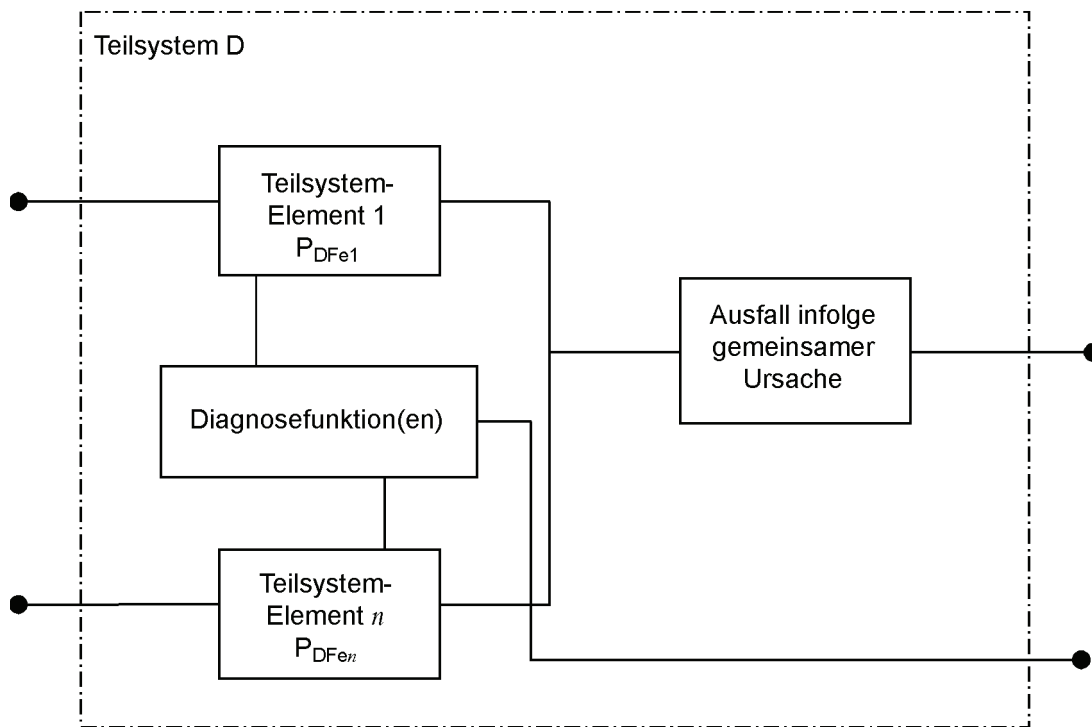


Bild 11 – Teilsystem D: logische Sicht

ANMERKUNG 1 Bild 11 stellt eine logische Sicht der Architektur des Teilsystems D dar und sollte nicht als seine physikalische Implementierung betrachtet werden. Die gezeigte Diagnose kann durchgeführt werden durch:

- das Teilsystem, für das die Diagnose erforderlich ist; oder
- andere Teilsysteme des SRECS; oder
- Teilsysteme, die nicht an der Ausführung der Sicherheitsfunktion beteiligt sind.

(Beispiele zur physikalischen Implementierung sind noch zu entwickeln)

ANMERKUNG 2 Für ein Teilsystem D sollte die Abschätzung der P_{DF} die Wahrscheinlichkeit eines Ausfalls der relevanten Diagnosefunktion(en) in Betracht ziehen. Der Beitrag der Diagnosefunktion(en) kann durch einen Faktor, abhängig vom erreichten SIL-Anspruch des Teilsystems, das die Diagnosefunktion(en) ausführt, geändert werden. Dies kann durch Anpassung des Diagnosedeckungsgrads wie folgt berücksichtigt werden:

SIL-Anspruch	DC-Anpassungsfaktor
SIL 1	<i>noch festzulegen</i>
SIL 2	<i>noch festzulegen</i>
SIL 3	<i>noch festzulegen</i>

Die Wahrscheinlichkeit gefährbringender Ausfälle kann durch Modellierung von Zuverlässigkeitsblockdiagrammen und Analysemethoden wie folgt abgeschätzt werden:

$$P_{DF} = (1 - (\text{Diagnosedeckungsgrad} \times F_{\text{mod}}))P_d$$

mit P_{ud} Wahrscheinlichkeit eines unerkannten gefährbringenden Ausfalls,

P_d Wahrscheinlichkeit eines gefährbringenden Ausfalls,

DC Diagnosedeckungsgrad,

F_{mod} Anpassungsfaktor.

6.7.8 Anforderungen zur systematischen Sicherheitsintegrität von Teilsystemen

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.

Die Implementierung der in 6.7.8.1 und 6.7.8.2 beschriebenen Maßnahmen ergibt eine Anspruchsgrenze von SIL 3 für die systematische Sicherheitsintegrität eines Teilsystems.

6.7.8.1 Anforderungen zur Vermeidung von systematischen Ausfällen

Die folgenden Maßnahmen müssen angewendet werden:

- a) Verwendung von angemessenen Materialien und passender Verarbeitung: Auswahl des Materials, Verarbeitungsmethoden und Behandlung im Zusammenhang mit z. B. Beanspruchung, Haltbarkeit, Elastizität, Reibung, Abnutzung, Korrosion, Temperatur, Leitfähigkeit, dielektrischer Festigkeit.
- b) Korrekte Dimensionierung und Gestaltung: Betrachtung der Einflüsse von z. B. Beanspruchung, Belastung, Abnutzung, Temperatur, Oberflächenrauigkeit, Toleranzen, Verarbeitung.
- c) Richtige Auswahl, Kombination, Anordnung, Montage und Installation von Bauteilen einschließlich Verkabelung, Verdrahtung und allen Verbindungen: Beachtung der Herstellerangaben zur Anwendung, z. B. von Katalogblättern, Installationsvorgaben, Spezifikationen und Anwendung bewährter Praktiken.
- d) Verträglichkeit: Verwendung von Bauteilen mit zusammenpassenden Betriebseigenschaften.
- e) 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, z. B. Temperatur, Feuchtigkeit, Vibration und elektromagnetischer Beeinflussung (EMI) (siehe EN 954-2, Anhang D.1).
- f) Verwendung von Bauteilen, die gemäß einer angemessenen Norm entworfen worden sind und deren Ausfallmodi klar definiert sind: Reduzierung des Risikos unerkannter Fehler durch die Verwendung von Bauteilen mit spezifischen Eigenschaften.

ANMERKUNG 1 Die Auswahl von Bauteilen für die Verwendung in sicherheitsbezogenen Anwendungen sollte vom Hersteller unter Berücksichtigung der Verfügbarkeit dieser Bauteile (zum Beispiel die Verwendung von betrieblich getesteten physikalischen Einheiten, um hohe Sicherheitsanforderungen zu erfüllen oder die Speicherung von sicherheitsbezogenen Programmen nur in Sicherheitsspeicherbausteinen) im Zusammenhang mit ihrer beabsichtigten Verwendung durchgeführt werden. Die Sicherheit von Speicherbausteinen kann sich sowohl auf den unerlaubten Zugriff, als auch auf umgebungsbedingte Einflüsse (elektromagnetische Verträglichkeit, Strahlung, usw.) und das Verhalten der Bauteile bei Auftreten eines Ausfalls beziehen.

Zusätzlich müssen eine oder mehrere der folgenden Maßnahmen unter Berücksichtigung der Komplexität des Teilsystems und seiner SIL-Anspruchsgrenze angewendet werden:

- g) Hardware-Entwurfsüberprüfung (z. B. durch Inspektion oder Walkthrough): Durch Reviews und/oder Analyse Unstimmigkeiten zwischen der Spezifikation und der Implementierung aufzudecken.

ANMERKUNG 2 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, das beim Inspektionsverfahren der Autor passiv und der Inspektor aktiv ist, während bei einem Walkthrough-Verfahren der Autor aktiv und der Inspektor passiv ist.

- h) Rechnergestützte Entwurfswerkzeuge mit der Fähigkeit zu Simulation oder Analyse: Systematische Ausführung der Entwurfsverfahren und Einbeziehung passender automatischer Konstruktionselemente, die bereits verfügbar und getestet sind.

ANMERKUNG 3 Die Integrität dieser Werkzeuge kann durch spezifische Tests, durch eine umfassende Historie zufriedenstellender Verwendung oder durch eine unabhängige Verifikation ihrer Ausgaben demonstriert werden.

- i) Simulation: Ausführung einer systematischen vollständigen Inspektion eines Teilsystementwurfs sowohl im Hinblick auf die funktionale Leistungsfähigkeit, als auch die korrekte Dimensionierung seiner Bauteile.

E DIN IEC 62061 (VDE 0113 Teil 50):2003-06

ANMERKUNG 3^{N11)} Die Funktion des Teilsystems kann auf einem Rechner durch ein Softwareverhaltensmodell simuliert werden, wobei einzelne Bauteile der Schaltung ihr eigenes simuliertes Verhalten haben und die Reaktion des Teilsystems, in dem sie verbunden sind, untersucht wird, in dem die Grenzdaten jedes Bauteils betrachtet werden.

6.7.8.2 Anforderungen zur Beherrschung von systematischen Ausfällen

Die folgenden Maßnahmen müssen angewendet werden:

- a) Überwachung des Programmablaufs muss bei allen Teilsysteme, die Software enthalten, verwendet werden: Erkennung eines fehlerhaften Programmablaufs. Ein fehlerhafter Programmablauf liegt vor, wenn die einzelnen Teile eines Programms (zum Beispiel Softwaremodule, Unterprogramme oder Befehle) in der falschen Reihenfolge oder Zeitdauer abgearbeitet werden oder wenn der Takt des Prozessors fehlerhaft ist.

ANMERKUNG 1 Weitere Informationen sind in IEC 61508-7, A.9 enthalten.

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

ANMERKUNG 2 Siehe auch relevante Abschnitte 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 Sekundärspannung 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 alle Ausgänge durch die Power-down-Routine in einen sicheren Zustand geschaltet werden können oder eine Umschaltung auf eine zweite Energieversorgung erfolgen kann.

- c) 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 60529, IEC 60204-1.
- d) Maßnahmen zur Beherrschung der Einflüsse eines Temperaturanstiegs: Das Teilsystem muss so entworfen werden, dass zum Beispiel Übertemperaturen erkannt werden können, bevor es außerhalb der Spezifikation betrieben wird.

ANMERKUNG 3 Weitere Informationen sind in IEC 61508-7, A.10 enthalten.

- e) Maßnahmen zur Beherrschung der Auswirkungen der Fehler und andere Effekte, die von irgendeinem Datenkommunikationsprozess herrühren in Übereinstimmung mit 7.4.8 von IEC 61508-2.

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

- a) Erkennung von Ausfällen durch Überwachung während des Betriebs;
- b) Tests durch redundante Hardware;
- c) diversitäre Hardware;
- d) zwangsläufiger Betätigungsmodus (z. B. zwangsgeführte Kontakte);
- e) gerichtete Ausfälle;
- f) Überdimensionierung: Unterlastung von Bauteilen, die in Sicherheitsschaltungen verwendet werden, z. B. durch:
- g) der Strom über Schaltkontakte sollte kleiner als die Hälfte ihres Nennstroms sein,

^{N11)} Nationale Fußnote: Die korrekte Nummerierung dieser Anmerkung muss Anmerkung 4 lauten.

- h) die Schalthäufigkeit von Bauteilen sollte kleiner als die Hälfte ihres Nennwertes sein, und
- i) die Gesamtanzahl der erwarteten Schaltspiele sollte 10-mal kleiner als die Haltbarkeit des Gerätes sein.

ANMERKUNG 4 Wo Überdimensionierung angemessen ist, sollte mindestens ein Überdimensionierungsfaktor von 1,5 verwendet werden.

ANMERKUNG 5 Weitere Informationen sind in prEN 954-2, Anhang D.3 enthalten.

6.7.9 Teilsystemmontage

Die Teilsystem-Elemente müssen in Übereinstimmung mit 6.7.4.3.1.3 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 (siehe 6.7.7) zu erfüllen.

6.8.2 Die Diagnosefunktionen werden als separate Funktionen betrachtet, die eine andere Struktur als die sicherheitsbezogene Steuerungsfunktion 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 sicherheitsbezogenen Steuerungsfunktion beteiligt sind.

ANMERKUNG Siehe auch Anmerkung 3 von 6.6.2.1.1.

6.8.3 Diagnosefunktionen müssen folgenden Punkten, die auf sicherheitsbezogene Steuerungsfunktionen anwendbar sind, genügen:

- Anforderungen für die Vermeidung von Ausfällen (siehe 6.7.8.1); und
- Anforderungen für die Beherrschung von systematischen Ausfällen (siehe 6.7.8.2).

6.8.4 Die Wahrscheinlichkeit eines Ausfalls der Diagnosefunktion(en) muss bei der Abschätzung der Wahrscheinlichkeit gefahrbringender Ausfälle der sicherheitsbezogenen Steuerungsfunktion berücksichtigt werden.

ANMERKUNG 1 Siehe auch Anmerkung 3 in 6.6.2.1.1.

ANMERKUNG 2 Zeitliche Einschränkungen, die auf die Testung des Teilsystems, das eine Diagnosefunktion ausführt, anwendbar sind, können von denjenigen, die auf die sicherheitsbezogenen Steuerungsfunktionen anwendbar sind, abweichen. Allgemein sollte das Testintervall diejenigen Anforderungen für ein Teilsystem mit einer Fehlertoleranz der Hardware von Eins erfüllen.

ANMERKUNG 3 Der Ausfall einer Diagnosefunktion(en) sollte erkannt werden, und es sollte eine angemessene Reaktion erfolgen, um sicherzustellen, dass der Beitrag der Diagnosefunktion zur Sicherheitsintegrität der sicherheitsbezogenen Steuerungsfunktion erhalten bleibt. Der Ausfall einer 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 Diagnosefunktion(en) und eine Analyse ihres Beitrages zur Sicherheitsintegrität der zugehörigen sicherheitsbezogenen Steuerungsfunktionen erfolgen.

6.9 Hardware-Implementierung

Das SRECS muss gemäß dem dokumentierten SRECS-Entwurf implementiert werden.

6.9.1 SRECS-Verbindung

ANMERKUNG Verbindungen außer digitaler Datenkommunikation werden als Teil der Teilsysteme betrachtet.

6.9.1.1 Das SRECS muss so verbunden werden, dass die entsprechenden Teile der Spezifikation der SRECS-Sicherheitsanforderungen und diejenigen Anforderungen in den Abschnitten 13 und 14 von IEC 60204-1, die für die Handhabung von Leitern, Verkabelung und Verdrahtung relevant sind, 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 Sicherheitsfunktion(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 abgeleitet werden aus (1) den spezifizierten Sicherheitsanforderungen der sicherheitsbezogenen Steuerungsfunktion, (2) den Anforderungen, die aus der SRECS-Architektur resultieren und (3) allen Anforderungen des Plans der funktionalen Sicherheit (siehe 4.2). Diese Informationen müssen dem Entwickler der Anwendungssoftware zur Verfügung gestellt werden.

ANMERKUNG Diese Anforderung bedeutet nicht, dass es keine Iterationen zwischen dem Entwickler der sicherheitsgerichteten Steuerungsarchitektur, der Organisation, die für die Konfiguration der Geräte verantwortlich ist, und dem Entwickler der Anwendungssoftware geben sollte. Wenn die Sicherheitsanforderungen der Anwendungssoftware und die mögliche Anwendungssoftware-Architektur präziser werden, kann ein Einfluss auf die SRECS-Hardwarearchitektur erfolgen. Deswegen ist eine enge Zusammenarbeit zwischen dem Entwickler der SRECS-Architektur, dem Lieferanten des Teilsystems und dem Softwareentwickler wesentlich.

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 zu erlauben eine Beurteilung der funktionalen Sicherheit durchführen zu können.

ANMERKUNG Der Detaillierungsgrad der Spezifikation kann mit der Komplexität der Anwendung variieren.

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

- sicherheitsbezogene Steuerungsfunktionen;
- Konfiguration oder Architektur des Systems;
- Kapazität und Leistungsfähigkeit in Bezug auf Reaktionszeit;
- Einrichtungen und Anwenderschnittstellen;
- alle relevanten Betriebsmodi der Maschine wie in der Spezifikation der Sicherheitsanforderungen festgelegt;
- Diagnostetests 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 zweideutigen Ausdrücken und Beschreibungen.

6.10.2.6 Die Spezifikation der Software-Sicherheitsanforderungen für jedes Teilsystem muss Folgendes einschließen:

- Eigenüberwachung der Software (z. B. Erkennung eines Stacküberlaufs);
- Überwachung anderer Geräte innerhalb des SRECS (z. B. Sensoren und Stellglieder);
- periodischer Test der sicherheitsbezogenen Steuerungsfunktionen wenn die Maschine im Betrieb ist.

6.10.2.7 Die Spezifikation der Software-Sicherheitsanforderungen muss die erforderlichen Eigenschaften des Teilsystems durch Angabe von Informationen beschreiben, die eine richtige Auswahl von Einrichtungen erlauben. Die Anforderungen zu den folgenden sicherheitsbezogenen Softwaresteuerungsfunktionen müssen spezifiziert werden:

- Funktionen, die es der Maschine ermöglichen, einen sicheren Zustand zu erreichen oder aufrechtzuerhalten;
- Funktionen bezüglich der Detektion, Meldung und Kontrolle von Fehlern in allen Teilsystemen des SRECS;
- Funktionen bezüglich periodischer Tests sicherheitsbezogener Steuerungsfunktionen während des Betriebs und Off-Line;
- Funktionen, die es erlauben Modifikationen am SRECS sicher durchführen zu können;
- Schnittstellen zu nicht-sicherheitsbezogenen Steuerungsfunktionen;
- Kapazität und Leistungsfähigkeit in Bezug auf Reaktionszeit.

ANMERKUNG Schnittstellen umfassen sowohl während des Betriebs verwendete, als auch Off-Line Programmier-einrichtungen.

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

6.11 Software-Entwurf und Entwicklung

6.11.1 Entwurf und Entwicklung von Embedded-Software

Teilsysteme, die komplexe Komponenten mit Embedded-Software enthalten, müssen entsprechend dem erforderlichen SIL IEC 61508 entsprechen.

ANMERKUNG Anhang C (informativ) ist dazu vorgesehen beim Entwurf und Entwicklung von Embedded-Software behilflich zu sein, die dazu verwendet wird, um sicherheitsbezogene Steuerungsfunktionen in einem SRECS zu implementieren.

6.11.2 Software basierende Parametrisierung und Link

Noch zu entwickeln.

WG7 ANMERKUNG Dies ist ein wichtiger Aspekt des Systementwurfs, der Bedeutung für Softwareelemente innerhalb von Geräten und Teilsystemen hat, die Software enthalten, zum Beispiel in digitalen Kommunikationsanwendungen verwendet werden.

6.11.3 Entwurf und Entwicklung der Anwendungssoftware

ANMERKUNG Dieser Unterabschnitt von IEC 62061 basiert auf IEC 61508, Teil 3. Anwendungssoftware ist die Software, die dazu vorgesehen ist, durch den Anwender implementiert zu werden.

6.11.3.1 Allgemeine Anforderungen

6.11.3.1.1 Das Ausführen von Tests muss die wichtigste verwendete Methode zur Verifikation sein. Die Verifikation muss aufzeigen, dass die Software den festgelegten SIL erfüllt.

6.11.3.1.2 Um den erforderlichen SIL der sicherheitsbezogenen Steuerungsfunktion zu erreichen, müssen die gewählte Entwurfsmethode und die Programmiersprache der Anwendung 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 der Anwendungsfunktionen;
 - Reihenfolge und zeitbezogene Anforderungen;
 - zeitlichen Einschränkungen;
 - Gleichzeitigkeit von Anwendungsfunktionen und der Möglichkeit von konkurrierenden Zuständen;
 - Datenstrukturen und ihren Eigenschaften, einschließlich Datentypen, Gültigkeit von Datenbereichen;
 - Voraussetzungen für den Entwurf und ihre Abhängigkeiten.
- c) Verständnis durch Entwickler und andere, die den Entwurf verstehen müssen, sowohl von einem funktionalen Verständnis der Anwendung, als auch von einem Wissen um die Einschränkungen der Technologie;
- d) Verifikation und Validierung, einschließlich struktureller Abdeckung (White-Box) der Anwendungssoftware, funktionaler Abdeckung (Black-Box) des integrierten Anwendungsprogramms und Schnittstellenvvalidierung (Grey-Box) der Wechselwirkung mit dem SRECS und seiner anwendungsspezifischen Hardwarekonfiguration.
- e) Testbarkeit und die Möglichkeit sicher ausgeführter Modifikation.

6.11.3.1.1^{N12)} Die Testplanung muss Folgendes betrachten:

- die Grundsätze für die Integration von Software und Hardware;
- Testfälle und Testdaten;
- Arten der auszuführenden Tests;
- Testumgebung einschließlich Werkzeuge, Software zur Unterstützung und eine Beschreibung der Konfiguration;
- Testkriterien, nach denen die Vollständigkeit der Tests beurteilt werden muss;
- Ort(e) (z. B. Fabrik oder Lage);
- Abhängigkeit von externer Funktionalität; und
- passendes Personal.

6.11.3.1.4 Die verwendete Entwurfsmethode muss Merkmale besitzen, die eine Modifikation der Anwendungssoftware erleichtern. Diese Merkmale schließen Modularität und gute Dokumentation ein.

6.11.3.1.5 Soweit es praktisch möglich ist, muss der Entwurf den sicherheitsbezogenen Anteil der Anwendungssoftware gering halten.

6.11.3.1.6 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.

^{N12)} Nationale Fußnote: Die korrekte Nummerierung dieses Unterabschnitts muss 6.11.3.1.3 lauten.