

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                               |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <b>DIN EN 61511-1<br/>(VDE 0810-1)</b>                                                                                                                                                                                                                                                                        | <b>DIN</b> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Diese Norm ist zugleich eine <b>VDE-Bestimmung</b> im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden. | <b>VDE</b> |
| <p>ICS 01.040.25; 25.040.40</p> <p><b>Funktionale Sicherheit –<br/>Sicherheitstechnische Systeme für die Prozessindustrie –<br/>Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und<br/>Hardware<br/>(IEC 61511-1:2003 + Corrigendum 2004);<br/>Deutsche Fassung EN 61511-1:2004</b></p> <p>Functional safety –<br/>Safety instrumented systems for the process industry sector –<br/>Part 1: Framework, definitions, system, hardware and software requirements<br/>(IEC 61511-1:2003 + Corrigendum 2004);<br/>German version EN 61511-1:2004</p> <p>Sécurité fonctionnelle –<br/>Systèmes instrumentés de sécurité pour le secteur des industries de transformation –<br/>Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel<br/>(CEI 61511-1:2003 + Corrigendum 2004);<br/>Version allemande EN 61511-1:2004</p> <p style="text-align: right;">Gesamtumfang 89 Seiten</p> <p style="text-align: center;">DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE</p> |                                                                                                                                                                                                                                                                                                               |            |

## **Beginn der Gültigkeit**

Die von CENELEC am 2004-10-01 angenommene EN 61511-1 gilt als DIN-Norm ab 2005-05-01.

## **Nationales Vorwort**

*Vorausgegangener Norm-Entwurf: E DIN IEC 61511-1 (VDE 0810-1):2004-02.*

Für die vorliegende Norm ist das nationale Arbeitsgremium GK 914 „Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ erarbeitet.

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zum Jahr 2007 unverändert bleiben soll. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

- bestätigt,
- zurückgezogen,
- durch eine Folgeausgabe ersetzt oder
- geändert.

Die vorliegende Norm stellt Anforderungen an die Spezifikation, den Entwurf, die Installation, den Betrieb und die Instandhaltung eines sicherheitstechnischen Systems (SIS) für die Prozessindustrie.

Sie richtet sich in erster Linie an die für die Errichtung des sicherheitstechnischen Systems verantwortliche Organisation.

Die notwendigen Informationen zu den Anforderungen an die Installation, den Betrieb, die Instandhaltung und Änderung müssen in geeigneter Form zur Verfügung gestellt werden.

Die Betreiberpflichten nach Betriebssicherheitsverordnung bleiben unberührt.

## **Nationaler Anhang NA** (informativ)

### **Zusammenhang mit Europäischen und Internationalen Normen**

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

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

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

**Tabelle NA.1**

| <b>Europäische Norm</b> | <b>Internationale Norm</b> | <b>Deutsche Norm</b>   | <b>Klassifikation im VDE-Vorschriftenwerk</b> |
|-------------------------|----------------------------|------------------------|-----------------------------------------------|
| EN 60654-1:1993         | IEC 60654-1:1993           | DIN EN 60654-1:1994-02 | –                                             |
| EN 60654-3:1997         | IEC 60654-3:1983           | DIN EN 60654-3:1998-08 | –                                             |

| Europäische Norm                                                                | Internationale Norm                                                                                                           | Deutsche Norm                                        | Klassifikation im VDE-Vorschriftenwerk |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------|
| EN 61326:1997<br>+ EN 61326/A1:1998<br>+ EN 61326/A2:2001<br>+ EN 61326/A3:2003 | IEC 61326-1:1997<br>+ IEC 61326-1/A1:1998<br>+ IEC 61326-1/A2:2000<br>+ Anhänge E & F zu IEC 61326:2002<br>+ Corrigendum 2002 | <b>DIN EN 61326</b><br><b>(VDE 0843-20):2004-05</b>  | VDE 0843-20                            |
| Reihe der Normen<br>EN 61508                                                    | Reihe der Normen<br>IEC 61508                                                                                                 | Reihe der Normen<br>DIN EN 61508 (VDE 0803)          | VDE 0803                               |
| EN 61511-2:2004                                                                 | IEC 61511-2:2003                                                                                                              | <b>DIN EN 61511-2</b><br><b>(VDE 0810-2):2005-05</b> | VDE 0810-2                             |
| EN 61511-3:2004                                                                 | IEC 61511-3:2003<br>+ Corrigendum 2004                                                                                        | <b>DIN EN 61511-3</b><br><b>(VDE 0810-3):2005-05</b> | VDE 0810-3                             |

## Nationaler Anhang NB (informativ)

### Literaturhinweise

DIN EN 60654-1:1994-02, *Leittechnische Einrichtungen für industrielle Prozesse; Umgebungsbedingungen – Teil 1: Klimatische Einflüsse (IEC 60654-1:1993); Deutsche Fassung EN 60654-1:1993.*

DIN EN 60654-3:1998-08, *Einsatzbedingungen für Mess-, Steuer- und Regeleinrichtungen in der industriellen Prozesstechnik – Teil 3: Mechanische Einflüsse (IEC 60654-3:1983); Deutsche Fassung EN 60654-3:1997.*

**DIN EN 61326 (VDE 0843-20):2004-05**, *Elektrische Betriebsmittel für Leittechnik und Laboreinsatz – EMV-Anforderungen (IEC 61326-1:1997 + IEC 61326-1/A1:1998 + IEC 61326-1/A2:2000 + Anhänge E & F zu IEC 61326:2002 + Corrigendum 2002); Deutsche Fassung EN 61326:1997 + EN 61326/A1:1998 + EN 61326/A2:2001 + EN 61326/A3:2003.*

Normen der Reihe DIN EN 61508 (VDE 0803), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (Normen der Reihe IEC 61508); Deutsche Fassung Normen der Reihe EN 61508*

**DIN EN 61511-2 (VDE 0810-2):2005-05**, *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 2: Anleitungen zur Anwendung der IEC 61511-1 (IEC 61511-2:2003); Deutsche Fassung EN 61511-2:2004.*

**DIN EN 61511-3 (VDE 0810-3):2005-05**, *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2003 + Corrigendum 2004); Deutsche Fassung EN 61511-3:2004.*

– Leerseite –

**Funktionale Sicherheit**  
**Sicherheitstechnische Systeme für die Prozessindustrie**  
**Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und**  
**Hardware**  
(IEC 61511-1:2003 + Corrigendum 2004)

Functional safety  
Safety instrumented systems for the process  
industry sector  
Part 1: Framework, definitions, system,  
hardware and software requirements  
(IEC 61511-1:2003 + Corrigendum 2004)

Sécurité fonctionnelle  
Systèmes instrumentés de sécurité pour le  
secteur des industries de transformation  
Partie 1: Cadre, définitions, exigences pour le  
système, le matériel et le logiciel  
(CEI 61511-1:2003 + Corrigendum 2004)

Diese Europäische Norm wurde von CENELEC am 2004-10-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

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

## CENELEC

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

**Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel**

## **Vorwort**

Der Text der Internationalen Norm IEC 61511-1:2003, ausgearbeitet von dem SC 65A „System aspects“ des IEC TC 65 „Industrial-process measurement and control“, wurde dem Einstufigen Annahmeverfahren unterworfen und von CENELEC am 2004-10-01 ohne irgendeine Abänderung als EN 61511-1 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2005-10-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2007-10-01

Der Anhang ZA wurde von CENELEC hinzugefügt.

## **Anerkennungsnotiz**

Der Text der Internationalen Norm IEC 61511-1:2003 + Corrigendum November 2004 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

## Inhalt

|                                                                                                                                    | Seite |
|------------------------------------------------------------------------------------------------------------------------------------|-------|
| Vorwort.....                                                                                                                       | 2     |
| Einleitung .....                                                                                                                   | 6     |
| 1 Anwendungsbereich .....                                                                                                          | 8     |
| 2 Normative Verweisungen .....                                                                                                     | 12    |
| 3 Begriffe und Abkürzungen.....                                                                                                    | 13    |
| 3.1 Abkürzungen.....                                                                                                               | 13    |
| 3.2 Begriffe .....                                                                                                                 | 13    |
| 4 Übereinstimmung mit dieser Internationalen Norm.....                                                                             | 30    |
| 5 Management der funktionalen Sicherheit.....                                                                                      | 30    |
| 5.1 Ziel.....                                                                                                                      | 30    |
| 5.2 Anforderungen.....                                                                                                             | 31    |
| 6 Anforderungen an den Sicherheitslebenszyklus .....                                                                               | 36    |
| 6.1 Ziele .....                                                                                                                    | 36    |
| 6.2 Anforderungen.....                                                                                                             | 36    |
| 7 Verifikation .....                                                                                                               | 38    |
| 7.1 Ziel .....                                                                                                                     | 38    |
| 8 Beurteilung des Risikos und der Gefährdung aus dem Prozess.....                                                                  | 38    |
| 8.1 Ziele .....                                                                                                                    | 38    |
| 8.2 Anforderungen.....                                                                                                             | 39    |
| 9 Zuordnung der Sicherheitsfunktionen zu den Schutzebenen .....                                                                    | 40    |
| 9.1 Ziele .....                                                                                                                    | 40    |
| 9.2 Anforderungen an den Prozess der Zuordnung .....                                                                               | 40    |
| 9.3 Zusätzliche Anforderungen für Sicherheits-Integritätslevel 4.....                                                              | 41    |
| 9.4 Anforderungen an Betriebseinrichtungen, die als Schutzebene eingesetzt werden.....                                             | 42    |
| 9.5 Anforderungen zur Vermeidung von Ausfällen infolge gemeinsamer Ursache, gleichartigen Ausfällen und abhängigen Ausfällen ..... | 43    |
| 10 Spezifikation der Sicherheitsanforderungen an das SIS.....                                                                      | 43    |
| 10.1 Ziel .....                                                                                                                    | 43    |
| 10.2 Allgemeine Anforderungen .....                                                                                                | 43    |
| 10.3 Sicherheitsanforderungen an das SIS.....                                                                                      | 43    |
| 11 Entwurf und Planung des SIS.....                                                                                                | 45    |
| 11.1 Ziel .....                                                                                                                    | 45    |
| 11.2 Allgemeine Anforderungen .....                                                                                                | 45    |
| 11.3 Anforderungen an das Systemverhalten bei Entdeckung eines Fehlers .....                                                       | 46    |
| 11.4 Anforderungen an die Hardware-Fehlertoleranz .....                                                                            | 48    |
| 11.5 Anforderungen an die Auswahl von Komponenten und Teilsystemen .....                                                           | 49    |
| 11.6 Feldgeräte.....                                                                                                               | 52    |
| 11.7 Schnittstellen .....                                                                                                          | 52    |

|                                                                                               | Seite |
|-----------------------------------------------------------------------------------------------|-------|
| 11.8 Anforderungen an Instandhaltungs- oder Testeinrichtungen .....                           | 54    |
| 11.9 Ausfallwahrscheinlichkeit sicherheitstechnischer Funktionen .....                        | 55    |
| 12 Anforderungen an die Anwendungssoftware und Auswahlkriterien für Software-Hilfsmittel..... | 56    |
| 12.1 Anforderungen an den Sicherheitslebenszyklus der Anwendungssoftware.....                 | 56    |
| 12.2 Spezifikation der Sicherheitsanforderungen an die Anwendungssoftware .....               | 62    |
| 12.3 Validierungsplanung für die Sicherheit der Anwendungssoftware .....                      | 64    |
| 12.4 Entwurf und Erstellung der Anwendungssoftware.....                                       | 64    |
| 12.5 Integration der Anwendungssoftware in das SIS-Teilsystem .....                           | 69    |
| 12.6 Vorgehen bei Modifikation einer FPL- und LVL-Software .....                              | 70    |
| 12.7 Verifikation der Anwendungssoftware .....                                                | 71    |
| 13 Werksendprüfungen (FAT = Factory Acceptance Tests) .....                                   | 72    |
| 13.1 Ziele .....                                                                              | 72    |
| 13.2 Empfehlungen.....                                                                        | 72    |
| 14 SIS-Montage und Inbetriebnahme.....                                                        | 74    |
| 14.1 Ziele .....                                                                              | 74    |
| 14.2 Anforderungen .....                                                                      | 74    |
| 15 SIS-Sicherheits-Validierung.....                                                           | 75    |
| 15.1 Ziel .....                                                                               | 75    |
| 15.2 Anforderungen .....                                                                      | 75    |
| 16 Betrieb und Instandhaltung des SIS .....                                                   | 77    |
| 16.1 Ziele .....                                                                              | 77    |
| 16.2 Anforderungen .....                                                                      | 77    |
| 16.3 Wiederholungsprüfungen und Inspektionen .....                                            | 79    |
| 17 Modifikationen am SIS.....                                                                 | 80    |
| 17.1 Ziele .....                                                                              | 80    |
| 17.2 Anforderungen .....                                                                      | 80    |
| 18 Außerbetriebnahme des SIS .....                                                            | 81    |
| 18.1 Ziele .....                                                                              | 81    |
| 18.2 Anforderungen .....                                                                      | 81    |
| 19 Anforderungen an die Information und Dokumentation.....                                    | 81    |
| 19.1 Ziele .....                                                                              | 81    |
| 19.2 Anforderungen .....                                                                      | 82    |
| Anhang A (informativ) Unterschiede .....                                                      | 83    |
| A.1 Unterschiede im Aufbau .....                                                              | 83    |
| A.2 Terminologie .....                                                                        | 83    |
| Literaturverzeichnis .....                                                                    | 84    |
| <b>Bilder</b>                                                                                 |       |
| Bild 1 – Gesamtrahmen dieser Norm.....                                                        | 7     |
| Bild 2 – Beziehung zwischen IEC 61508 und IEC 61511 .....                                     | 9     |
| Bild 3 – Beziehung zwischen IEC 61508 und IEC 61511 (siehe Abschnitt 1) .....                 | 10    |

|                                                                                                                             | Seite |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| Bild 4 – Zusammenhang zwischen sicherheitstechnischen und anderen Funktionen .....                                          | 11    |
| Bild 5 – Zusammenhang in der IEC 61511-1 zwischen System, Hardware und Software .....                                       | 12    |
| Bild 6 – Programmierbares elektronisches System (PES), Struktur und Begriffe .....                                          | 22    |
| Bild 7 – Beispiel einer SIS-Architektur .....                                                                               | 25    |
| Bild 8 – Phasen des SIS-Sicherheitslebenszyklus und Stufen der Beurteilung der funktionalen<br>Sicherheit.....              | 34    |
| Bild 9 – Typische Methoden der Risikominderung in prozesstechnischen Anlagen .....                                          | 42    |
| Bild 10 – Sicherheitslebenszyklus der Anwendungssoftware und Verhältnis zum Lebenszyklus des<br>SIS .....                   | 57    |
| Bild 11 – Sicherheitslebenszyklus der Anwendungssoftware (in der Realisierungsphase) .....                                  | 59    |
| Bild 12 – Software-Entwicklungsprozess (das V-Modell) .....                                                                 | 59    |
| Bild 13 – Zusammenhang zwischen Hardware- und Software-Architektur des SIS .....                                            | 62    |
| <b>Tabellen</b>                                                                                                             |       |
| Tabelle 1 – In der IEC 61511 verwendete Abkürzungen.....                                                                    | 13    |
| Tabelle 2 – Übersicht über den Sicherheitslebenszyklus eines SIS .....                                                      | 36    |
| Tabelle 3 – Sicherheits-Integritätslevel: Ausfallwahrscheinlichkeit bei Anforderung.....                                    | 41    |
| Tabelle 4 – Sicherheits-Integritätslevel: Häufigkeit gefährbringender Ausfälle der<br>sicherheitstechnischen Funktion ..... | 41    |
| Tabelle 5 – Mindest-Hardware-Fehlertoleranz von PE-Logiksystemen .....                                                      | 48    |
| Tabelle 6 – Mindest-Hardware-Fehlertoleranz von Sensoren, Aktoren und nichtprogrammierbaren<br>Logiksystemen.....           | 49    |
| Tabelle 7 – Sicherheitslebenszyklus der Anwendungssoftware: Übersicht .....                                                 | 60    |

## Einleitung

Sicherheitstechnische Systeme sind seit vielen Jahren für sicherheitstechnische Aufgaben in der Prozessindustrie im Einsatz. Damit Prozessleittechnik für sicherheitstechnische Funktionen wirkungsvoll eingesetzt werden kann, muss sie bestimmten Mindestanforderungen und Leistungsstufen entsprechen.

Diese Internationale Norm behandelt die Anwendung sicherheitstechnischer Systeme in der Prozessindustrie. Sie fordert außerdem die Durchführung einer Gefährdungs- und Risikoanalyse, um daraus die Spezifikation sicherheitstechnischer Systeme ableiten zu können. Andere Sicherheitssysteme werden nur so weit betrachtet, dass ihr Beitrag bei der Betrachtung der Leistungsanforderung an die sicherheitstechnischen Systeme berücksichtigt werden kann. Das sicherheitstechnische System umfasst dabei alle zur Ausführung der sicherheitstechnischen Funktion erforderlichen Komponenten und Teilsysteme vom Sensor bis zum Aktor.

Der „Sicherheitslebenszyklus“ und die „Sicherheits-Integritätslevel“ (SIL) bilden die Grundlage für die Anwendung dieser Internationalen Norm.

Die in dieser Norm betrachteten sicherheitstechnischen Systeme beruhen auf elektrischer (E) /, elektronischer (E) / und programmierbarer elektronischer (PE) Technologie. Wenn andere Technologien zur Realisierung logischer Steuerungen verwendet werden, sollten die grundlegenden Prinzipien dieser Norm in entsprechender Weise angewendet werden. In dieser Norm werden auch die Sensoren und Aktoren sicherheitstechnischer Systeme betrachtet, unabhängig von der Technologie, in der sie ausgeführt sind. Diese Norm ist innerhalb des Rahmens der IEC 61508 zugeschnitten auf die Prozessindustrie (siehe IEC 61511-1, [Anhang A](#)).

Diese Internationale Norm beschreibt die notwendigen Tätigkeiten im Sicherheitslebenszyklus, damit die oben genannten Mindestanforderungen erfüllt werden können. Dieser Ansatz wurde gewählt, damit eine überlegte und einheitliche technische Vorgehensweise zustande kommt.

In den meisten Fällen lässt sich die Sicherheit am besten durch den Entwurf eines sicheren Prozesses gewährleisten. Wenn erforderlich kann dies mit einem oder mehreren Schutzsystemen im Hinblick auf jegliche identifizierte Restrisiken verbunden werden. Schutzsysteme können auf unterschiedlichen Technologien (chemische, mechanische, hydraulische, pneumatische, elektrische, elektronische, programmierbar elektronische Einrichtungen etc.) beruhen. Um diesen Ansatz zu erleichtern,

- fordert diese Norm die Durchführung einer Gefährdungs- und Risiko-Beurteilung, um die übergreifenden Sicherheitsanforderungen festzulegen;
- fordert diese Norm die Zuordnung der Sicherheitsanforderungen zu einzelnen sicherheitstechnischen Systemen;
- arbeitet diese Norm innerhalb eines Betrachtungsrahmens, der alle sicherheitstechnischen Methoden zur Erlangung funktionaler Sicherheit umfasst;
- führt diese Norm den Gebrauch bestimmter Tätigkeiten, wie z. B. Sicherheits-Management, im einzelnen auf, die sich auf alle Methoden zur Erlangung der funktionalen Sicherheit anwenden lassen.

Diese Internationale Norm über sicherheitstechnische Systeme für die Prozessindustrie

- behandelt alle Zeitpunkte innerhalb des Sicherheitslebenszyklus vom anfänglichen Konzept, Entwurf, Ausführung, Betrieb und Instandhaltung bis hin zur Außerbetriebnahme;
- erlaubt es, bereits bestehende oder neue landesspezifische Normen für die Prozessindustrie mit dieser Norm zu harmonisieren.

Diese Internationale Norm strebt nach einer hohen Übereinstimmung (beispielsweise bezüglich zugrundeliegender Prinzipien, Terminologie, Dokumentation) innerhalb der Prozessindustrie. Dies sollte sowohl sicherheitstechnische als auch ökonomische Vorteile bringen.

In Staaten, in denen von Seiten des Gesetzgebers (beispielsweise durch Bund, Länder oder Gemeinden) Vorschriften bezüglich Prozessentwurf, Prozessmanagement oder andere Anforderungen erlassen wurden, haben diese Vorrang gegenüber den Anforderungen dieser Norm.

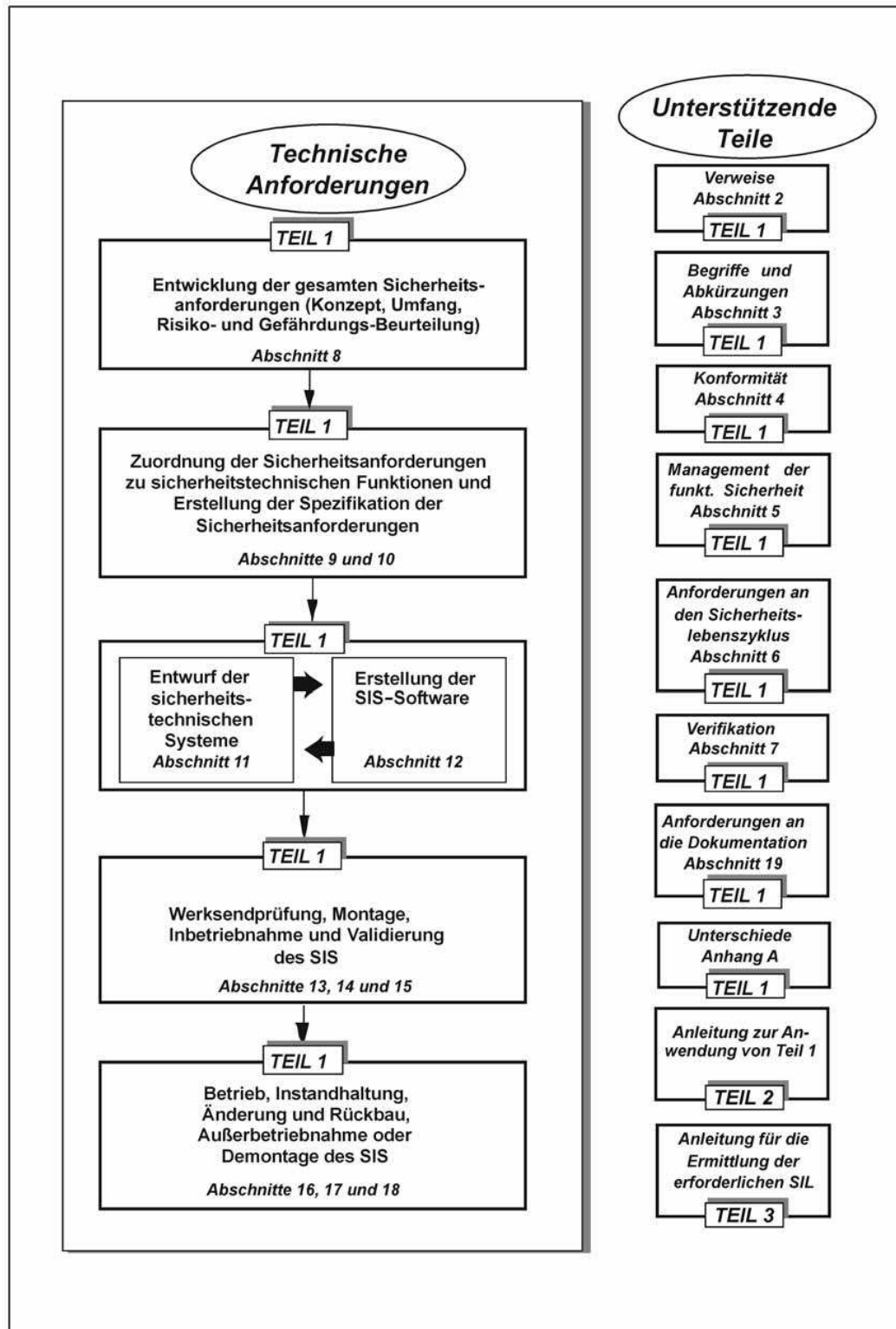


Bild 1 – Gesamtrahmen dieser Norm

## 1 Anwendungsbereich

Diese Internationale Norm stellt Anforderungen an die Spezifikation, den Entwurf, die Installation, den Betrieb und die Instandhaltung eines sicherheitstechnischen Systems (SIS) auf, so dass dieses den Prozess in einen sicheren Zustand versetzen oder in einem sicheren Zustand halten kann. Diese Norm wurde als Anwendung der Internationalen Norm IEC 61508 „Funktionale Sicherheit – Sicherheitssysteme (E/E/PES)“ für die Prozessindustrie erstellt.

Insbesondere

- a) stellt diese Internationale Norm Anforderungen zur Erreichung der funktionalen Sicherheit auf, legt jedoch nicht fest, wer verantwortlich für die Erfüllung dieser Anforderungen ist (beispielsweise Planer, Lieferanten, Eigentümer/Betreiber, Kontraktforen); diese Verantwortlichkeit wird den Beteiligten durch die Sicherheitsplanung und nationale Vorschriften zugewiesen.
- b) trifft sie auf Geräte zu, die den Anforderungen der IEC 61508 oder IEC 61511-1, [11.5](#) entsprechen und die in ein System integriert werden, das in der Prozessindustrie eingesetzt wird, nicht jedoch auf Geräte, für die der Hersteller die Eignung in sicherheitstechnischen Systemen der Prozessindustrie (siehe [IEC 61508-2](#) und [IEC 61508-3](#)) nachweisen will.
- c) beschreibt sie den Zusammenhang zwischen der IEC 61511 und der IEC 61508 ([Bild 2](#) und [Bild 3](#)),
- d) betrifft sie Anwendungssoftware, die für Systeme mit eingeschränktem Sprachumfang oder festen Programmen erstellt wurde; sie trifft nicht zu für Hersteller, Planer sicherheitstechnischer Systeme, Systemerrichter und Anwender, die Betriebssysteme entwickeln oder Sprachen mit nicht eingeschränktem Sprachumfang benutzen (siehe [IEC 61508-3](#)).
- e) gilt sie für einen weiten Bereich von Industrien innerhalb der Prozessindustrie einschließlich Chemieindustrie, Raffinerien, Öl- und Gasförderung, Papierherstellung, konventionelle Stromerzeugung;

ANMERKUNG Innerhalb der Prozessindustrie können einzelne Anwendungen (z. B. „Offshore“) zusätzliche Anforderungen haben, die beachtet werden müssen.

- f) zeigt sie den Zusammenhang zwischen sicherheitstechnischen Funktionen und anderen Funktionen ([Bild 4](#));
- g) führt sie zu einer Aufstellung der funktionalen Anforderungen und der Anforderungen an die Sicherheitsintegrität der sicherheitstechnischen Funktionen unter Berücksichtigung der mit anderen Mitteln erreichten Risikominderung;
- h) legt diese Norm Anforderungen an die Systemarchitektur und Hardwarekonfiguration, Anwendungssoftware und Systemintegration fest;
- i) legt sie Anforderungen an die Anwendungssoftware für Anwender und Systemerrichter sicherheitstechnischer Systeme ([Abschnitt 12](#)) fest. Im Einzelnen werden folgende Anforderungen festgelegt:
  - die Phasen und die Tätigkeiten des Sicherheitslebenszyklus, die während der Planung und Erstellung der Anwendungssoftware (Modell des Sicherheitslebenszyklus für Software) stattfinden. Diese Anforderungen schließen die Anwendung von Maßnahmen und Techniken ein, die Fehler in der Software vermeiden und Ausfälle beherrschen;
  - Umfang der Dokumentation bezüglich der Validierung der Software, die an die Organisation übergeben wird, die das SIS errichtet;
  - Vorbereitung von Dokumentation und Vorschriften für die Software, die der Anwender für Betrieb und Instandhaltung des SIS benötigt;
  - Verfahren und Spezifikationen, die von der Organisation eingehalten werden müssen, die Modifikationen an der Software durchführt;
- j) gilt sie dann, wenn die funktionale Sicherheit mit einer oder mehreren sicherheitstechnischen Funktionen zum Schutz der Mitarbeiter, der Öffentlichkeit oder der Umwelt erreicht wird;
- k) kann sie auch in Nicht-Sicherheitsanwendungen, beispielsweise zum Schutz eines Wirtschaftsguts angewendet werden;
- l) legt sie Anforderungen fest, nach denen sicherheitstechnische Funktionen als Teil einer Gesamtmethode zum Erlangen der funktionalen Sicherheit ausgeführt werden müssen;

- m) verwendet sie einen Sicherheitslebenszyklus (Bild 8) und legt eine Reihe von Tätigkeiten fest, die notwendig sind, um die funktionalen Anforderungen und die erforderliche Sicherheitsintegrität für sicherheitstechnische Systeme festzulegen;
- n) verlangt sie, dass eine Gefährdungs- und Risikoanalyse durchgeführt wird, in der die Anforderungen an die funktionale Sicherheit und an den Sicherheits-Integritätslevel für jede einzelne sicherheitstechnische Funktion festgelegt werden;

ANMERKUNG Bild 9 zeigt eine Übersicht über Methoden zur Risikominderung.

- o) definiert sie Zielwerte für die mittlere Ausfallwahrscheinlichkeit bei Anforderung und die Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde in den verschiedenen Sicherheits-Integritätsleveln;
- p) stellt sie Mindestanforderungen an die Fehlertoleranz der Hardware;
- q) schreibt sie die zum Erreichen der geforderten Integritätslevel notwendigen Vorgehensweisen und Maßnahmen vor;
- r) definiert sie den höchsten Sicherheits-Integritätslevel (SIL 4), welchen eine sicherheitstechnische Funktion erreichen kann, die nach dieser Norm ausgeführt wurde;
- s) definiert sie den niedrigsten möglichen Sicherheits-Integritätslevel (SIL 1), unterhalb dessen diese Norm nicht mehr gültig ist;
- t) gibt sie einen Rahmen zur Festlegung von Sicherheits-Integritätsleveln vor, ohne jedoch festzulegen, welche Sicherheits-Integritätslevel in spezifischen Anwendungen benötigt werden (was nur aufgrund von Erfahrungen mit der jeweiligen Anwendung möglich ist);
- u) schreibt sie Anforderungen für alle Teile des sicherheitstechnischen Systems von den Sensoren bis zu den Aktoren vor;
- v) legt sie fest, welche Dokumentation während des Sicherheitslebenszyklus benötigt wird,
- w) fordert sie, dass der Entwurf sicherheitstechnischer Funktionen menschliche Verhaltensweisen berücksichtigt;
- x) stellt sie keinerlei direkte Anforderungen an den einzelnen Anlagenfahrer oder an Mitarbeiter der Instandhaltung.



Bild 2 – Beziehung zwischen IEC 61508 und IEC 61511

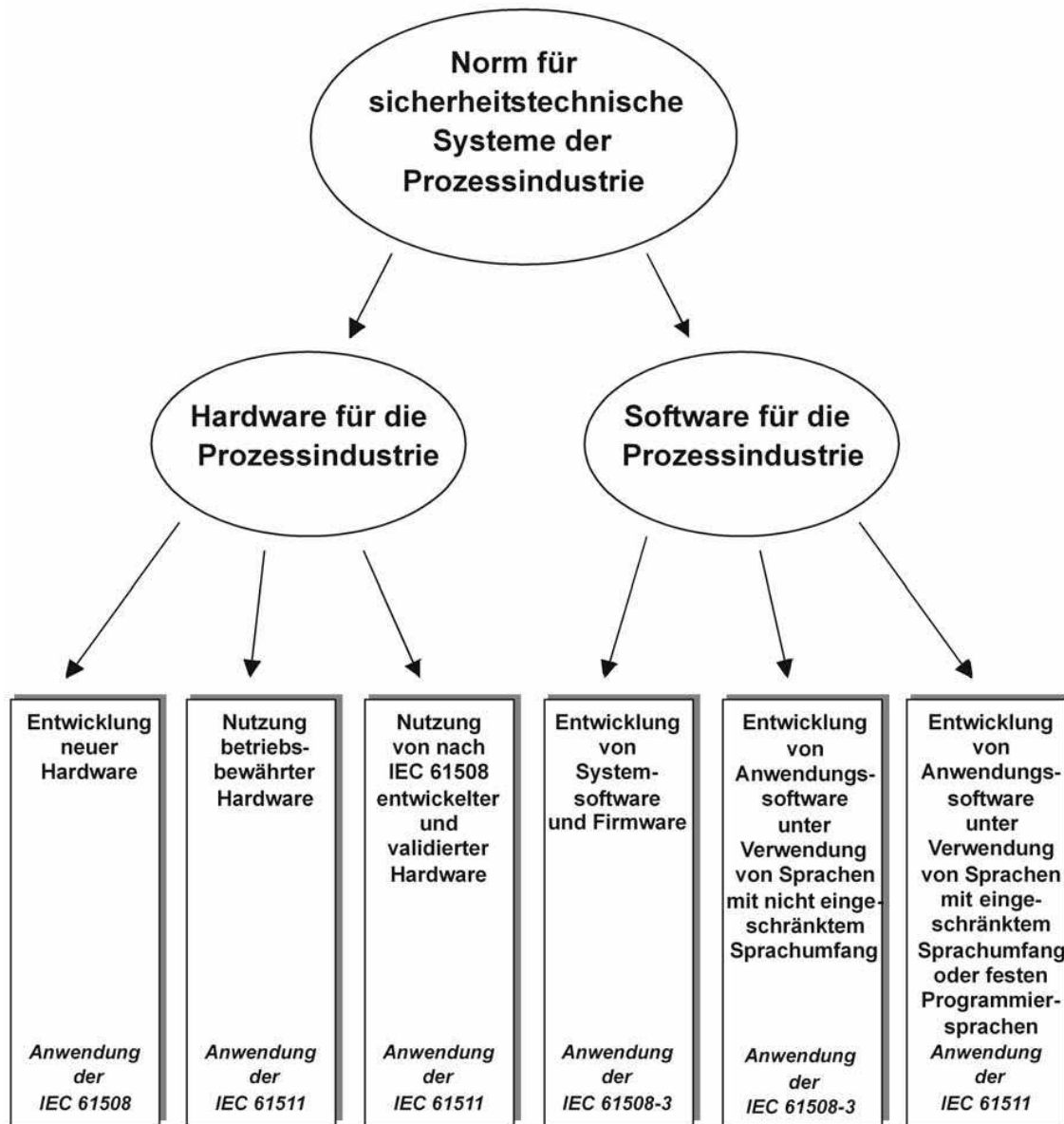
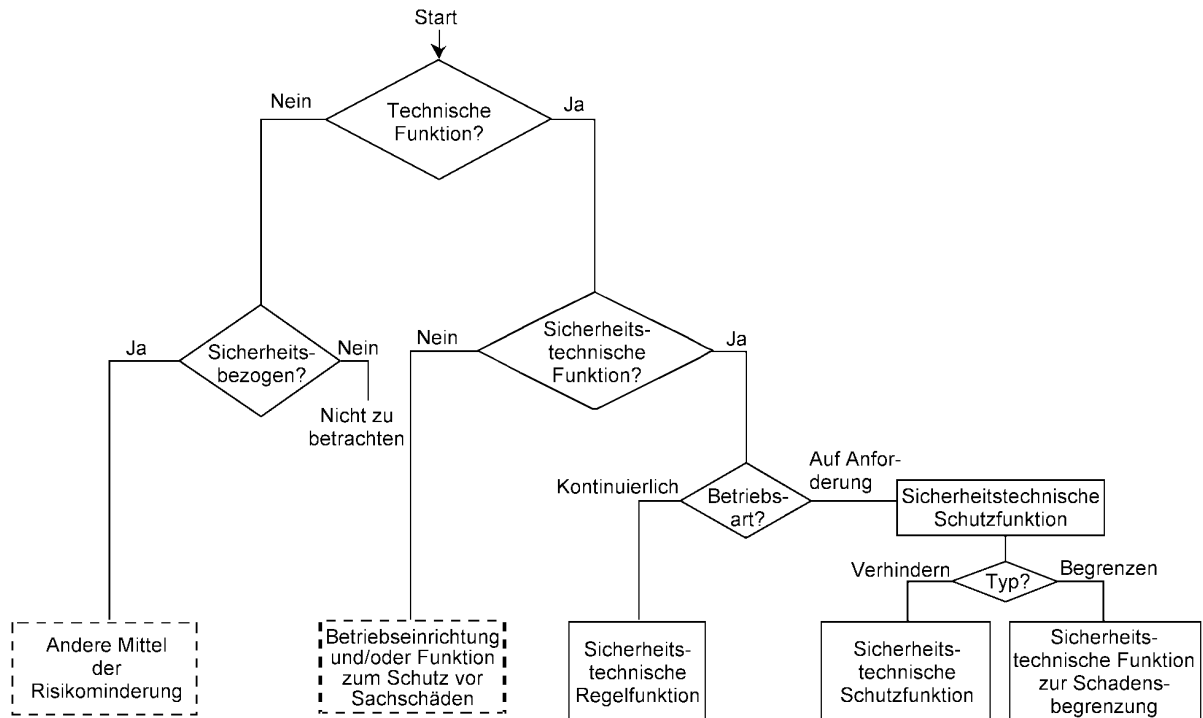


Bild 3 – Beziehung zwischen IEC 61508 und IEC 61511 (siehe [Abschnitt 1](#))



--- bedeutet: die Norm schreibt durchzuführende Tätigkeiten vor, ohne detaillierte Anforderungen vorzugeben

**Bild 4 – Zusammenhang zwischen sicherheitstechnischen und anderen Funktionen**

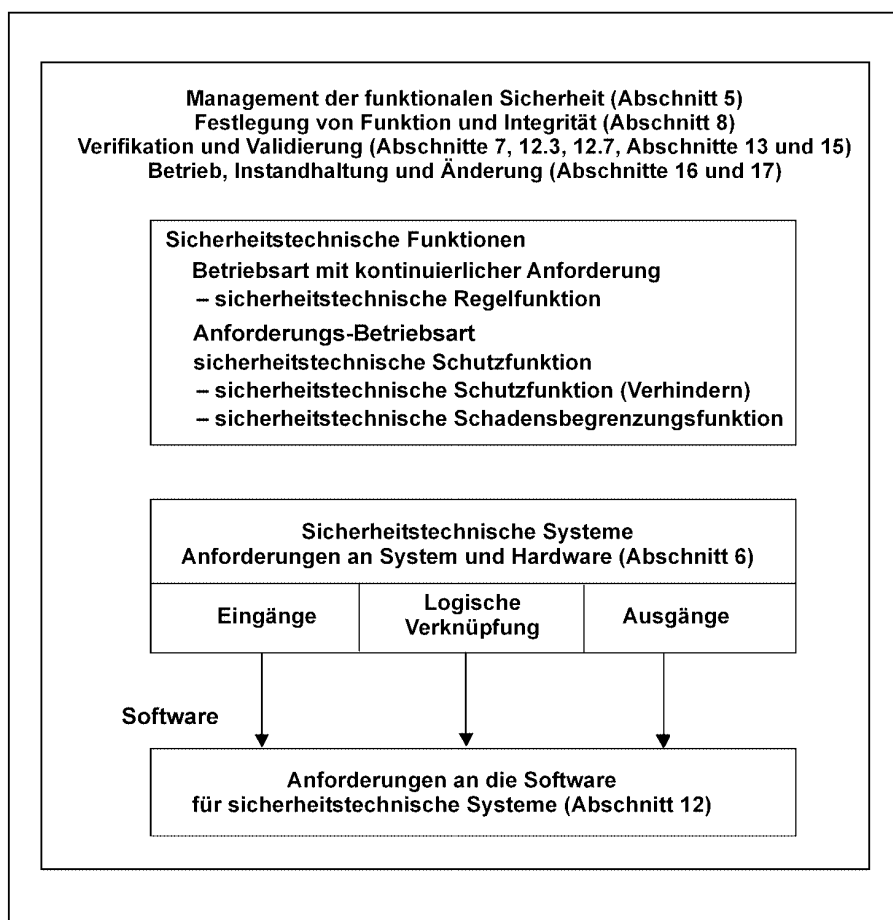


Bild 5 – Zusammenhang in der IEC 61511-1 zwischen System, Hardware und Software

## 2 Normative Verweisungen

Die im Folgenden angeführten Dokumente sind für die Anwendung dieses Dokuments unverzichtbar. Bei datierten Verweisungen gelten nur die angegebenen Ausgaben. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 60654-1, *Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions*

IEC 60654-3, *Industrial-process measurement and control equipment – Operating conditions – Part 3: Mechanical influences*

IEC 61326-1, *Electrical equipment for measurement, control and laboratory use – EMC requirements*

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

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

IEC 61511-2, *Safety instrumented systems for the process industry sector – Part 2: Guidelines in the application of IEC 61511-1*

### 3 Begriffe und Abkürzungen

#### 3.1 Abkürzungen

In der IEC 61511 verwendete Abkürzungen sind in Tabelle 1 angegeben.

**Tabelle 1 – In der IEC 61511 verwendete Abkürzungen**

| Abkürzung | Englische Benennung                                  | Deutsche Benennung                                                 |
|-----------|------------------------------------------------------|--------------------------------------------------------------------|
| AC/DC     | Alternating current/direct current                   | Wechsel-/Gleichstrom                                               |
| ALARP     | As low as reasonably practicable                     | So niedrig wie vernünftigerweise möglich                           |
| ANSI      | American National Standards Institute                | US-amerikanische Normungsorganisation                              |
| BPCS      | Basic process control system                         | Betriebs- und Überwachungseinrichtungen als ein System             |
| DC        | Diagnostic coverage                                  | Diagnose-Deckungsgrad                                              |
| E/E/PE    | Electrical/electronic/programmable electronic        | elektrisch/elektronisch/programmierbar elektronisch                |
| E/E/PES   | Electrical/electronic/programmable electronic system | elektrisches/elektronisches/programmierbares elektronisches System |
| EMV (EMC) | Electro-magnetic compatibility                       | Elektromagnetische Verträglichkeit                                 |
| FAT       | Factory acceptance testing                           | Werksendprüfung                                                    |
| FPL       | Fixed program language                               | Feste Programmiersprache                                           |
| FTA       | Fault tree analysis                                  | Fehlerbaumanalyse                                                  |
| FVL       | Full variability language                            | Programmiersprache mit nicht eingeschränktem Sprachumfang          |
| HFT       | Hardware fault tolerance                             | Hardware-Fehlertoleranz                                            |
| HMI       | Human machine interface                              | Mensch-Maschine-Schnittstelle                                      |
| H & RA    | Hazard & risk assessment                             | Gefährdungs- und Risikobeurteilung                                 |
| HRA       | Human reliability analysis                           | Analyse menschlicher Zuverlässigkeit                               |
| H/W       | Hardware                                             | Hardware                                                           |
| IEC       | International Electrotechnical Commission            | Internationale Elektrotechnische Kommission                        |
| IEV       | International Electrotechnical Vocabulary            | Internationales Elektrotechnisches Wörterbuch                      |
| ISA       | Instrument Society of America                        | Instrument Society of America                                      |
| ISO       | International Organization for Standardization       | Internationale Organisation für Normung                            |
| LVL       | Limited variability language                         | Sprache mit eingeschränktem Sprachumfang                           |
| Moon      | M out of N (see clause 3.2.45)                       | M von N (siehe 3.2.45)                                             |
| NP        | Non-programmable                                     | nicht programmierbar                                               |
| PE        | Programmable electronics                             | Programmierbare Elektronik                                         |
| PES       | Programmable electronic system                       | Programmierbares elektronisches System                             |
| PFD       | Probability of failure on demand                     | Wahrscheinlichkeit eines Ausfalls bei Anforderung                  |
| PFDavg    | Average probability of failure on demand             | mittlere Wahrscheinlichkeit eines Ausfalls bei Anforderung         |
| PLC       | Programmable logic controller                        | Speicherprogrammierbare Steuerung                                  |
| SAT       | Site acceptance test                                 | Vor-Ort-Abnahme                                                    |
| SFF       | Safe failure fraction                                | Anteil ungefährlicher Ausfälle                                     |
| SIF       | Safety instrumented function                         | Sicherheitstechnische Funktion                                     |
| SIL       | Safety integrity level                               | Sicherheits-Integritätslevel                                       |
| SIS       | Safety instrumented system                           | Sicherheitstechnisches System                                      |
| SRS       | Safety requirements specification                    | Spezifikation der Sicherheitsanforderungen                         |
| S/W       | Software                                             | Software                                                           |

#### 3.2 Begriffe

Für die Anwendung in dieser Norm gelten die folgenden Begriffe.

### 3.2.1

#### **Architektur (en: architecture)**

die Anordnung von Bestandteilen aus Hardware und/oder Software in einem System wie beispielsweise

- (1) die Zusammenstellung von sicherheitstechnischen Teilsystemen;
- (2) die innere Struktur eines sicherheitstechnischen Teilsystems;
- (3) eine Anordnung von Softwareprogrammen

ANMERKUNG Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in IEC 61508-4 ab.

### 3.2.2

#### **Schutz vor Sachschäden (en: asset protection)**

die dem Systementwurf zugeordnete Funktion zum Zwecke der Verhinderung von Sachschäden

### 3.2.3

#### **Betriebs- und Überwachungseinrichtungen (BPCS) (en: basic process control system (BPCS))**

System, das auf Eingangssignale vom Prozess und seinen zugehörigen technischen Einrichtungen, von anderen programmierbaren Systemen und/oder von einem Bediener antwortet und Ausgangssignale erzeugt, die den Prozess und seine zugehörigen technischen Einrichtungen in der gewünschten Weise steuern. Das BPCS übernimmt jedoch keine sicherheitstechnischen Funktionen mit einem SIL  $\geq 1$

ANMERKUNG Siehe A.2.

### 3.2.4

#### **Kanal (en: channel)**

Element oder Gruppe von Elementen, die eine Funktion unabhängig ausführen

ANMERKUNG 1 Die Elemente innerhalb eines Kanals können Eingabe-/Ausgabebaugruppen, ein Logiksystem (siehe 3.2.40), Sensoren und Aktoren beinhalten.

ANMERKUNG 2 Eine zweikanalige Konfiguration ist eine Konfiguration mit zwei Kanälen, die die gleiche Funktion unabhängig voneinander ausführen.

ANMERKUNG 3 Die Benennung kann verwendet werden, um ein vollständiges System oder ein Teil eines Systems (z. B. Sensoren oder Aktoren) zu beschreiben.

### 3.2.5

#### **kodieren (en: coding)**

siehe 3.2.57 „Programmierung“

### 3.2.6

#### **3.2.6.1**

##### **Ausfall infolge gemeinsamer Ursache (en: common cause failure)**

Ausfall, der das Ergebnis eines oder mehrerer Ereignisse ist, die Ausfälle von zwei oder mehreren getrennten Kanälen in einem mehrkanaligen System verursachen und zu einem Systemausfall führen

#### **3.2.6.2**

##### **Ausfall infolge gemeinsamer Ausfallart (en: common mode failure)**

gleichartiger Ausfall von zwei oder mehr Kanälen, der das gleiche falsche Ergebnis erzeugt

### 3.2.7

#### **Komponente (en: component)**

Teil eines Systems oder Teilsystems oder ein Gerät, das eine bestimmte Funktion ausführt

### 3.2.8

#### **Konfiguration (en: configuration)**

siehe 3.2.1 „Architektur“

**3.2.9****Konfigurationsmanagement (en: configuration management)**

Verfahren zur Identifikation der Komponenten eines sich in der Entwicklung befindenden (Hardware- und Software-) Systems zum Zwecke der Kontrolle von Veränderungen an diesen Komponenten und zur Aufrechterhaltung von Kontinuität und Zurückverfolgbarkeit während des Lebenszyklus

**3.2.10****Regelsystem (en: control system)**

System, das auf Eingangssignale vom Prozess und/oder des Bedieners reagiert und Ausgangssignale erzeugt, die den Prozess (verfahrenstechnische Anlage) veranlassen, in der gewünschten Weise zu arbeiten

ANMERKUNG Das Regelsystem schließt die Sensoren und Aktoren ein und kann entweder ein BPCS oder ein SIS oder eine Kombination von beiden sein.

**3.2.11****gefährlicher Ausfall (en: dangerous failure)**

Ausfall mit dem Potential, das sicherheitstechnische System in einen gefahrbringenden oder funktionsunfähigen Zustand zu versetzen

ANMERKUNG Ob dieser Fall eintritt, kann von der Systemarchitektur abhängen; in Systemen, die zur Verbesserung der Sicherheit mehrere Kanäle besitzen, führt ein gefahrbringender Hardware-Ausfall mit geringerer Wahrscheinlichkeit zu einem gefahrbringenden Gesamtausfall oder zur Funktionsunfähigkeit.

**3.2.12****abhängiger Ausfall (en: dependent failure)**

Ausfall, dessen Wahrscheinlichkeit nicht als das einfache Produkt der Wahrscheinlichkeiten der individuellen Ereignisse, die ihn verursacht haben, ausgedrückt werden kann

ANMERKUNG 1 Zwei Ereignisse A und B sind nur dann abhängig, wenn gilt, wobei  $P(z)$  die Wahrscheinlichkeit des Ereignisses z ist:  $P(A \text{ und } B) > P(A) \times P(B)$ .

ANMERKUNG 2 Siehe 9.5 als Beispiel für die Berücksichtigung abhängiger Ausfälle zwischen Schutzebenen.

ANMERKUNG 3 Zu den abhängigen Ausfällen gehören auch die Ausfälle gemeinsamer Ursache. Siehe 3.2.6.

**3.2.13****erkannt, offenkundig (en: detected, revealed, overt)**

in Verbindung mit Hardwareausfällen und Softwarefehlern erkannt durch Diagnosetests oder den üblichen Betrieb

**3.2.14****Gerät (en: device)**

aus Hardware oder Software oder beidem bestehende Funktionseinheit, die einem speziellen Zweck dient (z. B. Feldgeräte oder an den Eingangs- und Ausgangskarten des SIS angeschlossene Einrichtungen. Zu diesen Einrichtungen gehören auch Feldverdrahtung, Sensoren, Aktoren, Logiksysteme und Bediener-Schnittstellen, die mit der Ein-/Ausgangsebene des SIS verdrahtet sind)

**3.2.15****Diagnosedeckungsgrad (en: diagnostic coverage (DC))**

Verhältnis der Ausfallrate der durch Diagnosetests erkannten Fehler zur Gesamtausfallrate der Komponente oder des Teilsystems. Der Diagnosedeckungsgrad beinhaltet keine bei Wiederholungsprüfungen festgestellten Fehler.

ANMERKUNG 1 Der Diagnosedeckungsgrad wird benutzt, um die Rate erkannter ( $\lambda_{\text{detected}}$ ) und die Rate unerkannter Ausfälle ( $\lambda_{\text{undetected}}$ ) aus der Gesamtausfallrate ( $\lambda_{\text{total failure rate}}$ ) folgendermaßen zu berechnen:  $\lambda_{\text{detected}} = DC \times \lambda_{\text{total failure rate}}$  und  $\lambda_{\text{undetected}} = (1 - DC) \times \lambda_{\text{total failure rate}}$ .

ANMERKUNG 2 Der Diagnosedeckungsgrad wird für Bauteile oder Baugruppen eines sicherheitsbezogenen Systems angewendet. Typischerweise wird der Diagnosedeckungsgrad für Sensoren, Stellglieder oder Logiksysteme bestimmt.

ANMERKUNG 3 Für Sicherheitsanwendungen wird der Diagnosedeckungsgrad typischerweise auf sichere und gefahrbringende Ausfälle des Bauteils oder der Baugruppe angewendet. Beispielsweise kann der Diagnosedeckungsgrad für gefahrbringende Ausfälle bei einer Baugruppe  $DC = \lambda_{DD}/\lambda_{DT}$  betragen, wobei  $\lambda_{DD}$  die Rate erkannter gefahrbringender Ausfälle und  $\lambda_{DT}$  die Gesamtausfallrate für gefahrbringende Ausfälle ist.

### 3.2.16

#### **Diversität (en: diversity)**

Vorhandensein ungleichartiger Mittel zur Ausführung einer geforderten Funktion

ANMERKUNG Diversität kann durch unterschiedliche physikalische Methoden oder unterschiedliche Lösungen für die gleiche Aufgabenstellung erreicht werden.

### 3.2.17

#### **elektrisch/elektronisch/programmierbar elektronisch (E/E/PE)**

#### **(en: electrical/electronic/programmable electronic (E/E/PE))**

basierend auf elektrischer (E) und/oder elektronischer (E) und/oder programmierbar elektronischer (PE) Technologie

ANMERKUNG Dieser Begriff erfasst alle Einrichtungen oder Systeme, die auf elektrischen Prinzipien arbeiten. Elektrische/elektronische/programmierbare elektronische Geräte beinhalten:

- elektromechanische Bauteile (elektrisch);
- nichtprogrammierbare elektronische Einrichtungen (elektronisch);
- elektronische Einrichtungen basierend auf Rechnertechnologie (programmierbar elektronisch), siehe [3.2.55](#).

### 3.2.18

#### **Abweichung (en: error)**

Nichtübereinstimmung zwischen Rechenergebnissen, beobachteten oder gemessenen Werten oder Beschaffenheiten und den betreffenden wahren, spezifizierten oder theoretisch richtigen Werten oder Beschaffenheiten

ANMERKUNG Aus IEC 191-05-24 mit Ausnahme der Anmerkungen.

### 3.2.19

#### **externe Einrichtungen zur Risikominderung (en: external risk reduction facilities)**

Maßnahme, um die Risiken zu vermindern oder zu mildern, die getrennt und verschieden vom SIS ist

ANMERKUNG 1 Externe Einrichtungen zur Risikominderung sind zum Beispiel ein Entleerungssystem, eine Brand-schutzmauer oder ein Deich.

ANMERKUNG 2 Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in [IEC 61508-4](#) ab.

### 3.2.20

#### **Ausfall (en: failure)**

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen

ANMERKUNG 1 Diese Definition stimmt mit ISO/IEC 2382-14-01-09 überein.

ANMERKUNG 2 Weitergehende Informationen finden sich in [IEC 61508-4](#).

ANMERKUNG 3 Die Erbringung geforderter Funktionen schließt notwendigerweise bestimmte Verhaltensweisen aus, und einige Funktionen dürfen derart spezifiziert werden, dass sie ein bestimmtes Verhalten vermeiden. Das Eintreten solch eines Verhaltens ist dann ein Ausfall.

ANMERKUNG 4 Ausfälle sind entweder zufällig oder systematisch (siehe [3.2.62](#) und [3.2.85](#)).

**3.2.21****Fehler (en: fault)**

anormaler Zustand, der eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen

ANMERKUNG IEC 191-05-01 definiert den entsprechenden Begriff als den Zustand einer Einheit, in dem sie unfähig ist, eine geforderte Funktion zu erfüllen, wobei Wartung oder andere geplante Handlungen bzw. durch das Fehlen äußerer Mittel verursachte Funktionsunfähigkeit ausgeschlossen ist. [ISO/IEC 2382-14-01-09]

**3.2.22****Fehlervermeidung (en: fault avoidance)**

Verwendung von Techniken und Verfahren mit dem Ziel, die Entstehung von Fehlern während jeder Phase des Sicherheitslebenszyklus des SIS zu vermeiden

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

Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen

ANMERKUNG Die Definition in IEC 191-15-05 bezieht sich nur auf die Teilmenge der Fehler in Untereinheiten. Siehe die Anmerkung zum Begriff Fehler in 3.2.21.

[ISO/IEC 2382-14-04-06]

**3.2.24****Aktor (en: final element)**

Teil eines sicherheitstechnischen Systems, das die Eingriffe in den Prozess ausführt, um einen sicheren Zustand zu erreichen

ANMERKUNG Beispiele sind Ventile, Schalter und Motoren einschließlich ihrer Hilfsaggregate, also beispielsweise ein Magnetventil mit seinem Aktor, sofern beide in die sicherheitstechnische Funktion einbezogen sind.

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

Teil der Gesamtsicherheit, der sich auf den Prozess und das BPCS bezieht und der von der bestimmungsgemäßen Funktion des SIS und anderer Sicherheitsebenen abhängt

ANMERKUNG Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in IEC 61508-4 ab.

**3.2.26****Beurteilung der funktionalen Sicherheit (en: functional safety assessment)**

auf Nachweise gestützte Untersuchung, die die funktionale Sicherheit beurteilt, die durch eine oder mehrere Schutzebenen erreicht wird

ANMERKUNG Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in IEC 61508-4 ab.

**3.2.27****Audit der funktionalen Sicherheit (en: functional safety audit)**

systematische und unabhängige Untersuchung, die bestimmt, ob die Verfahren zur Festlegung der Anforderungen an die funktionale Sicherheit mit den geplanten Vorgehensweisen übereinstimmen, wirksam durchgeführt werden und angemessen sind, die spezifizierten Ziele zu erreichen

ANMERKUNG Ein Audit der funktionalen Sicherheit kann im Rahmen der Beurteilung der funktionalen Sicherheit ausgeführt werden.

**3.2.28****Funktionseinheit (en: functional unit)**

Einheit aus Hardware oder Software oder beidem, die zur Durchführung einer festgelegten Aufgabe geeignet ist

ANMERKUNG 1 In IEC 191-01-01 wird die allgemeinere Benennung „Einheit“ anstelle von „Funktionseinheit“ verwendet. Eine Einheit kann manchmal Menschen einschließen.

ANMERKUNG 2 Dieses ist die Definition, die in ISO/IEC 2382-14-01-01 angegeben ist.

### 3.2.29

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

Teil der Sicherheitsintegrität der sicherheitstechnischen Funktion, der sich auf zufällige Hardware-Ausfälle mit gefahrbringender Ausfallart bezieht

ANMERKUNG 1 Der Begriff bezieht sich auf Ausfälle mit gefahrbringender Ausfallart. Dieses sind die Ausfälle eines sicherheitsbezogenen Systems, die die Sicherheitsintegrität beeinträchtigen können. Die in diesem Zusammenhang relevanten beiden Parameter sind die Gesamtausfallrate für gefahrbringende Ausfälle und die Wahrscheinlichkeit eines Versagens im Anforderungsfall.

ANMERKUNG 2 Siehe [3.2.86](#).

ANMERKUNG 3 Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in [IEC 61508-4](#) ab.

### 3.2.30

#### **Schaden (en: harm)**

physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden an Eigentum oder an der Umwelt

ANMERKUNG Diese Definition stimmt mit dem ISO/IEC Guide 51 überein.

### 3.2.31

#### **Gefährdung (en: hazard)**

potentielle Schadensquelle

ANMERKUNG 1 Diese Definition (ohne Anmerkungen) stimmt mit 3.4 von ISO/IEC Guide 51 überein.

ANMERKUNG 2 Der Begriff schließt die Gefährdungen von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (zum Beispiel durch Feuer und Explosion) und auch die, die einen Langzeiteffekt auf die Gesundheit einer Person haben (zum Beispiel durch Freisetzung einer giftigen Substanz).

### 3.2.32

#### **menschliches Versagen (en: human error)**

##### **Irrtum (en: mistake)**

Handlung oder Unterlassung eines Menschen, die zu einem unerwünschten Ergebnis führt

ANMERKUNG Dieses ist die Definition aus ISO/IEC 2382-14-01-09, sie unterscheidet sich von IEC 191-05-25 durch das Hinzufügen von „oder Unterlassung“.

### 3.2.33

#### **Einflussanalyse (en: impact analysis)**

Tätigkeit zur Bestimmung des Einflusses, den eine Änderung einer Funktion oder eines Bauteils des Systems auf andere Funktionen oder Bauteile im System oder auf andere Systeme haben kann

### 3.2.34

#### **unabhängige Abteilung (en: independent department)**

Abteilung, die getrennt und nicht in Verbindung mit den Abteilungen steht, die verantwortlich für die Tätigkeiten sind, die während einer speziellen Phase des Sicherheitslebenszyklus, der Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, stattfinden

### 3.2.35

#### **unabhängige Organisation (en: independent organization)**

Organisation, die aufgrund ihrer Managements und ihrer anderen Mittel getrennt ist und nicht in Verbindung mit den Organisationen steht, die für die Tätigkeiten verantwortlich sind, die während einer speziellen Phase

des Sicherheitslebenszyklus, der Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, stattfinden

### 3.2.36

#### **unabhängige Person (en: independent person)**

Person, die getrennt und nicht eingebunden ist in die Tätigkeiten, die während einer speziellen Phase des Sicherheitslebenszyklus stattfinden, die Gegenstand der Beurteilung der funktionalen Sicherheit oder Validierung ist, und die keine direkte Verantwortung für diese Tätigkeiten trägt

### 3.2.37

#### **Eingangsfunktion (en: input function)**

Funktion, die den Prozess und seine zugehörige Ausrüstung überwacht und diese Information einer logischen Funktion zur Verfügung stellt.

ANMERKUNG Eine Eingangsfunktion kann auch eine manuelle Funktion sein.

### 3.2.38

#### **Instrument (en: instrument)**

Gerät, das zur Ausführung einer Aktion verwendet wird (typischerweise in prozessleittechnischen Systemen)

ANMERKUNG Prozessleittechnische Systeme in der Prozessindustrie bestehen typischerweise aus Sensoren (beispielsweise Druck-, Durchfluss-, Temperaturmessumformer), Logiksystemen oder Leitsystemen (beispielsweise SPSen, verteilte Leitsysteme) und Aktoren (beispielsweise Stellventile). In besonderen Fällen können prozessleittechnische Systeme sicherheitstechnische Systeme sein (siehe [3.2.72](#)).

### 3.2.39

#### **logische Funktion (en: logic function)**

Funktion, die die Umwandlung der Eingangsinformation (bereitgestellt durch eine oder mehrere Eingangsfunktionen) zur Ausgangsinformation (verwendet durch eine oder mehrere Ausgangsfunktionen) herstellt. Logische Funktionen bewirken also die Umwandlung einer oder mehrerer Eingangsfunktionen zu einer oder mehreren Ausgangsfunktionen

ANMERKUNG Weitere Hinweise finden sich in IEC 61131-3 und IEC 60617-12.

### 3.2.40

#### **Logiksystem (en: logic solver)**

Teil eines BPCS oder eines SIS, das eine oder mehrere logische Funktionen ausführt

ANMERKUNG 1 In der IEC 61511 werden folgende Begriffe für Logiksysteme verwendet:

- elektrische Logiksysteme für Logiksysteme in elektromechanischer Technologie;
- elektronische Logiksysteme für Logiksysteme in elektronischer Technologie;
- programmierbare elektronische Systeme (PE-Logiksysteme) für Logiksysteme mit programmierbarer Elektronik.

ANMERKUNG 2 Beispiele sind: elektrische Systeme, elektronische Systeme, programmierbare elektronische Systeme, pneumatische Systeme, hydraulische Systeme. Sensoren und Aktoren sind nicht Bestandteil des Logiksystems.

#### 3.2.40.1

##### **sicherheitskonfiguriertes Logiksystem (en: safety configured logic solver)**

Standard-Industrie-PE-Logiksystem, das nach [11.5](#) speziell für den Einsatz in Sicherheitsanwendungen konfiguriert wurde

### 3.2.41

#### **Instandhaltungs- und Engineering-Schnittstelle (en: maintenance/engineering interface)**

die Instandhaltungs- und Engineering-Schnittstelle bezeichnet jenen Teil der Hardware und Software, der zur Instandhaltung oder Modifikation eines SIS vorgesehen ist. Sie kann auch Anweisungen oder Diagnosemittel in Form von Software, Programmiergeräten, Diagnosewerkzeugen, Anzeigen, Überbrückungseinrichtungen, Prüf- und Kalibriergeräten einschließen

### 3.2.42

#### **Schadensbegrenzungsmaßnahme (en: mitigation)**

Maßnahme zur Verringerung der Auswirkung(en) eines gefahrbringenden Ereignisses

ANMERKUNG Beispiele für Schadensbegrenzungsmaßnahmen sind Notentspannungssysteme für den Brand- oder Leckagefall.

### 3.2.43

#### **Betriebsart (en: mode of operation)**

Art, in der eine sicherheitstechnische Funktion betrieben wird

#### 3.2.43.1

##### **sicherheitstechnische Funktion in Anforderungsbetriebsart (en: demand mode safety instrumented function)**

in Fällen, in denen die festgelegte Handlung (z. B. das Schließen eines Ventils) als Antwort auf Prozesszustände oder andere Anforderungen eingeleitet wird. Im Fall eines gefahrbringenden Ausfalls der sicherheitstechnischen Funktion tritt eine mögliche Gefährdung nur im Fall eines Ausfalls des Prozesses oder der BPCS ein

#### 3.2.43.2

##### **sicherheitstechnische Funktion in Betriebsart mit kontinuierlicher Anforderung (en: continuous mode safety instrumented function)**

in Fällen, in denen bei Ausfall der sicherheitstechnischen Funktion eine mögliche Gefährdung ohne einen weiteren Ausfall eintritt, wenn keine Maßnahme zu ihrer Verhinderung ergriffen wird

ANMERKUNG 1 Die Betriebsart mit kontinuierlicher Anforderung deckt diejenigen sicherheitstechnischen Funktionen ab, die kontinuierliche Steuerung oder Regelungen zur Aufrechterhaltung der funktionalen Sicherheit beinhalten.

ANMERKUNG 2 Wenn in Anwendungen der Anforderungsbetriebsart die Anforderungsrate größer ist als einmal pro Jahr, ist die Gefährdungsrate nicht größer als die gefahrbringende Ausfallrate der sicherheitstechnischen Funktion. In diesem Fall sind normalerweise die Kriterien der Betriebsart mit kontinuierlicher Anforderung geeigneter.

ANMERKUNG 3 Die Ausfallgrenzwerte für SIS in der Anforderungsbetriebsart und in der Betriebsart mit kontinuierlicher Anforderung werden in [Tabelle 3](#) bzw. [4](#) definiert.

ANMERKUNG 4 Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in [IEC 61508-4](#) ab.

### 3.2.44

#### **Modul, Baugruppe (en: module)**

abgeschlossene Einheit aus Hardware-Komponenten zur Ausführung einer bestimmten Hardware-Funktion (z. B. digitales Eingangsmodul, analoges Ausgangsmodul) oder wiederverwendbarer Anwendungscode (innerhalb eines Programms oder einer Menge von Programmen), der eine bestimmte Funktion ausführt; zum Beispiel Teil eines Computerprogramms, das eine bestimmte Funktion ausführt

ANMERKUNG 1 Eine Funktion oder ein Funktionsbaustein in der [IEC 61131-3](#) ist ein Software-Modul.

ANMERKUNG 2 Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in [IEC 61508-4](#) ab.

### 3.2.45

#### **MooN-System (en: MooN, M out of N)**

sicherheitstechnisches System oder Teil davon, das aus „N“ unabhängigen Kanälen besteht, die derart miteinander verbunden sind, dass jeweils „M“ Kanäle genügen, um die sicherheitstechnische Funktion auszuführen<sup>Na1)</sup>

---

Na1) Siehe auch Anmerkungen zu [11.4.1](#)

**3.2.46****notwendige Risikominderung (en: necessary risk reduction)**

Risikominderung, um sicherzustellen, dass das vertretbare Risiko (Grenzrisiko) nicht überschritten wird

**3.2.47****nicht programmierbares (NP) System (en: non-programmable (NP) system)**

ein nicht auf Computertechnologie basierendes System (d. h. ein nicht auf programmierbarer Elektronik (PE) oder Software basierendes System)

ANMERKUNG Beispiele sind festverdrahtete elektrische oder elektronische Systeme, mechanische, hydraulische oder pneumatische Systeme.

**3.2.48****Bediener-Schnittstelle (en: operator interface)**

als Bediener-Schnittstelle werden jene Einrichtungen bezeichnet (z. B. Bildschirme, Leuchtanzeigen, Drucktaster, Hupen, Alarme), die dazu dienen, Informationen zwischen dem Bediener und dem SIS auszutauschen. Die Bediener-Schnittstelle wird auch als Mensch-Maschine-Kommunikation bezeichnet

**3.2.49****Sicherheitssystem anderer Technologie (en: other technology safety related systems)**

Sicherheitssystem, das nicht auf elektrischer, elektronischer oder programmierbarer elektronischer Technologie basiert

ANMERKUNG Ein Sicherheitsventil ist ein Sicherheitssystem anderer Technologie. Weitere Beispiele finden sich im Bereich hydraulischer und pneumatischer Systeme.

**3.2.50****Ausgangsfunktion (en: output function)**

Funktion, die den Prozess und die zugehörigen Einrichtungen nach der durch die logische Funktion vorgegebenen Stellsignale steuert

**3.2.51****Phase (en: phase)**

Zeitraum im Sicherheitslebenszyklus, in dem in dieser Norm beschriebene Tätigkeiten stattfinden

**3.2.52****Schutzmaßnahme (en: prevention)**

Maßnahme zur Verringerung der Eintrittshäufigkeit eines gefahrbringenden Ereignisses

**3.2.53****Frühere Nutzung (en: prior use)**

siehe „betriebsbewährt“ (siehe [3.2.60](#))

**3.2.54****Prozessrisiko****verfahrenstechnisches Risiko (en: process risk)**

Risiko, das sich aus Prozesszuständen ergibt, die durch außergewöhnliche Ereignisse verursacht werden (einschließlich Fehlfunktionen des BPCS)

ANMERKUNG 1 In diesem Zusammenhang ist das mit einem bestimmten gefahrbringenden Ereignis verknüpfte Risiko gemeint, gegen das ein SIS verwendet wird, um die notwendige Risikominderung zu erreichen (d. h. das mit der funktionalen Sicherheit verknüpfte Risiko).

ANMERKUNG 2 Das verfahrenstechnische Risiko wird in [IEC 61511-3](#) beschrieben. Die Hauptaufgabe bei der Bestimmung des verfahrenstechnischen Risikos besteht darin, einen Bezugspunkt für das Risiko ohne Berücksichtigung der Schutzebenen zu ermitteln.

ANMERKUNG 3 Die Beurteilung dieses Risikos sollte auch damit zusammenhängende Fragen menschlichen Verhaltens einschließen.

ANMERKUNG 4 Dieser Begriff entspricht dem EUC-Risiko in [IEC 61508-4](#).

### 3.2.55

#### **programmierbare Elektronik (PE) (en: programmable electronics (PE))**

elektronische Komponente oder Gerät in einem PES, das auf Computertechnologie basiert. Der Ausdruck bezeichnet sowohl Hardware als auch Software und Eingangs- und Ausgangsgeräte

ANMERKUNG 1 Der Begriff erstreckt sich auf mikroelektronische Geräte mit einer oder mehreren Zentraleinheiten (CPU) und zugehörigen Speichern. Beispiele für elektronische Komponenten aus der Prozessindustrie sind:

- Sensoren mit Mikroprozessor („Smart-Sensoren“) und Aktoren;
- programmierbare elektronische Logiksysteme, wie
  - programmierbare Regler;
  - speicherprogrammierbare Steuerungen (SPS).
  - Regler.

ANMERKUNG 2 Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in IEC 61508-4 ab.

### 3.2.56

#### **programmierbares elektronisches System (PES) (en: programmable electronic system (PES))**

System zur Steuerung, zum Schutz oder zur Überwachung, basierend auf einem oder mehreren programmierbaren elektronischen Geräten, einschließlich aller Elemente des Systems wie z. B. Energieversorgungen, Sensoren und anderen Eingabegeräten, Datenverbindungen und anderen Kommunikationswegen sowie Aktoren und anderen Ausgabeeinrichtungen (siehe Bild 6)

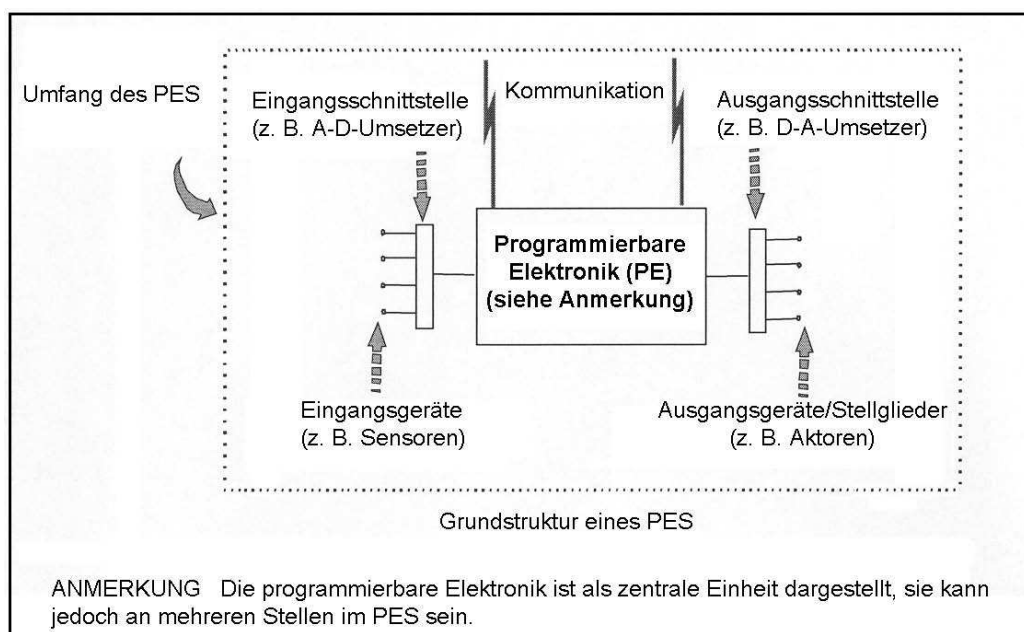


**Bild 6 – Programmierbares elektronisches System (PES), Struktur und Begriffe**

### 3.2.57

#### **Programmierung (en: programming)**

Entwurf, Erstellung und Test einer Reihe von Programmbefehlen zur Lösung einer Aufgabe oder zur Datenverarbeitung

ANMERKUNG In dieser Norm wird Programmierung normalerweise im Zusammenhang mit programmierbarer Elektronik verwendet.

**3.2.58****Wiederholungsprüfung (en: proof test)**

Prüfung zur Aufdeckung verdeckter Fehler in einem sicherheitstechnischen System, so dass das System, wenn nötig, wieder in den Zustand gebracht werden kann, in dem es seine geplante Funktion erfüllt

**3.2.59****Schutzebene (en: protection layer)**

jede unabhängige Maßnahme, die das Risiko durch Regelung oder Steuerung, Schutz- oder Schadensbegrenzungsmaßnahmen vermindert

ANMERKUNG Dazu gehören auch verfahrenstechnische Maßnahmen wie die Auslegung der Größe von Behältern mit gefährbringenden Chemikalien, Vorrichtungen wie Sicherheitsventile, ein sicherheitstechnisches System oder organisatorische Maßnahmen wie ein Alarmplan gegen eine drohende Gefahr. Diese Maßnahmen können automatisch oder durch menschlichen Eingriff ausgelöst werden (siehe [Bild 9](#)).

**3.2.60****betriebsbewährt (en: proven-in-use)**

eine Komponente ist betriebsbewährt, wenn eine entsprechend dokumentierte Untersuchung ergeben hat, dass Nachweise aus früheren Einsätzen belegen, dass die Komponente für den Einsatz in einem sicherheitstechnischen System geeignet ist (siehe „frühere Nutzung“ in [11.5](#))

ANMERKUNG Diese Definition weicht wegen in der Prozessindustrie vorhandener Unterschiede in der Terminologie von der Definition in IEC 61508 ab.

**3.2.61****Qualität (en: quality)**

Gesamtheit von Merkmalen einer Einheit bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen

ANMERKUNG Siehe auch ISO 9000:2000.

**3.2.62****zufälliger Hardware-Ausfall (en: random hardware failure)**

Ausfall, der zu einem zufälligen Zeitpunkt auftritt und der aus einem oder mehreren möglichen Mechanismen in der Hardware resultiert, die zu einer Verschlechterung der Eigenschaften von Bauteilen führen

ANMERKUNG 1 Es gibt viele mit unterschiedlicher Häufigkeit in verschiedenen Bauteilen auftretende Mechanismen, die die Eigenschaften der Bauteile verschlechtern können. Aufgrund von Fertigungstoleranzen treten Ausfälle der Bauteile aufgrund dieser Mechanismen nach unterschiedlichen Betriebszeiten auf. Ausfälle von Einrichtungen, die viele Bauteile enthalten, ereignen sich deshalb mit einer vorhersagbaren Häufigkeit aber zu unbestimmten (d. h. zufälligen) Zeiten.

ANMERKUNG 2 Ein wichtiges Unterscheidungsmerkmal zwischen zufälligen Hardware-Ausfällen und systematischen Ausfällen (siehe [3.2.85](#)) ist, dass Systemausfallraten (oder andere angemessene Kenngrößen) aufgrund zufälliger Hardware-Ausfälle vorausgesagt werden können, systematische Ausfälle aber schon von Natur aus nicht genau vorausgesagt werden können. Das heißt, dass Systemausfallraten, die durch zufällige Hardware-Ausfälle entstehen, mit vernünftiger Genauigkeit quantifiziert werden können, aber diejenigen, die durch systematische Ausfälle entstehen, statistisch nicht genau quantifizierbar sind, weil die Ereignisse, die zu diesen führen, nicht leicht vorausgesagt werden können.

**3.2.63****Redundanz (en: redundancy)**

Verwendung mehrerer Elemente oder Systeme zur Durchführung der gleichen Funktion. Redundanz kann mit gleichartigen Elementen (homogene Redundanz) oder mit unterschiedlichen Elementen (Diversität) realisiert werden

ANMERKUNG 1 Doppelte Funktionskomponenten und das Hinzufügen von Prüfbits (Paritätsbits) sind Beispiele von Redundanz.

ANMERKUNG 2 Redundanz wird hauptsächlich verwendet, um die Zuverlässigkeit oder Verfügbarkeit zu verbessern.

ANMERKUNG 3 Die Definition in IEC 191-15-01 ist weniger vollständig [ISO/IEC 2382-14-10-11].