

	DIN EN 61511-3 (VDE 0810-3)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 25.040.40 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 Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels (IEC 61511-3:2003 + Corrigendum 2004); German version EN 61511-3:2004 Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux d'intégrité de sécurité (CEI 61511-3:2003 + Corrigendum 2004); Version allemande EN 61511-3:2004 Gesamtumfang 56 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Die von CENELEC am 2004-10-01 angenommene EN 61511-3 gilt als DIN-Norm ab 2005-05-01.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN IEC 61511-3 (VDE 0810-3):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 enthält eine Anleitung zur Bestimmung der Sicherheits-Integritätslevel nach **DIN EN 61511-1**.

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

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 61511-1:2004	IEC 61511-1:2003 + Corrigendum 2004	DIN EN 61511-1 (VDE 0810-1):2005-05	VDE 0810-1
EN 61511-2:2004	IEC 61511-2:2003	DIN EN 61511-2 (VDE 0810-2):2005-05	VDE 0810-2
Reihe der Normen EN 61508	Reihe der Normen IEC 61508	Reihe der Normen DIN EN 61508 (VDE 0803)	VDE 0803

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 61511-1 (VDE 0810-1):2005-05, *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003 + Corrigendum 2004); Deutsche Fassung EN 61511-1:2004*

DIN EN 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*

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*

– Leerseite –

Deutsche Fassung

Funktionale Sicherheit
Sicherheitstechnische Systeme für die Prozessindustrie
Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-
Integritätslevel
(IEC 61511-3:2003 + Corrigendum 2004)

Functional safety
Safety instrumented systems for the process
industry sector
Part 3: Guidance for the determination of the
required safety integrity levels
(IEC 61511-3:2003 + Corrigendum 2004)

Sécurité fonctionnelle
Systèmes instrumentés de sécurité pour le
secteur des industries de transformation
Partie 3: Conseils pour la détermination des
niveaux d'intégrité de sécurité
(CEI 61511-3:2003 + 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 61511-3:2003, 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 61511-3 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

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61511-3:2003 + Corrigendum Oktober 2004 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

Inhalt

	Seite
Vorwort.....	2
Einführung.....	6
1 Anwendungsbereich	9
2 Definitionen und Abkürzungen	10
3 Risiko und Sicherheitsintegrität – Allgemeine Anleitung	10
3.1 Allgemeines	10
3.2 Notwendige Risikominderung	11
3.3 Die Rolle der sicherheitstechnischen Systeme	11
3.4 Sicherheitsintegrität	11
3.5 Risiko und Sicherheitsintegrität	13
3.6 Zuordnung der Sicherheitsanforderungen.....	14
3.7 Sicherheits-Integritätslevel	14
3.8 Auswahl einer Methode zur Bestimmung der erforderlichen Sicherheits-Integritätslevel	15
Anhang A (informativ) Konzept für ALARP und tolerierbares Risiko (ALARP: Prinzip der Verhältnismäßigkeit).....	16
A.1 Allgemeines	16
A.2 ALARP-Modell	16
A.2.1 Einleitung	16
A.2.2 Grenzwerte für das tolerierbare Risiko	17
Anhang B (informativ) Teilquantitative Methode.....	19
B.1 Allgemeines	19
B.2 Übereinstimmung mit der IEC 61511-1	19
B.3 Beispiel	19
B.3.1 Grenzwert für die Prozess-Sicherheit.....	20
B.3.2 Gefährdungsanalyse	20
B.3.3 Teilquantitative Methode der Risikoanalyse.....	21
B.3.4 Risikoanalyse eines bestehenden Verfahrens	22
B.3.5 Ereignisse außerhalb des Sicherheitsgrenzwerts	23
B.3.6 Risikominderung mit Hilfe anderer Schutzebenen	23
B.3.7 Risikominderung durch eine sicherheitstechnische Funktion	24
Anhang C (informativ) Matrixmethode für die Schutzebenen.....	26
C.1 Einleitung	26
C.2 Grenzwert für die Prozess-Sicherheit.....	27
C.3 Gefährdungsanalyse	27
C.4 Risikoanalyse	28
C.5 Matrix der Schutzebenen.....	29
C.6 Allgemeine Vorgehensweise	30
Anhang D (informativ) Bestimmung der erforderlichen Sicherheits-Integritätslevel – Eine teilqualitative Methode: der kalibrierte Risikograph.....	32

	Seite
D.1 Einleitung	32
D.2 Aufbau des Risikographen.....	32
D.3 Kalibrierung.....	33
D.4 Mitglieder und Organisation des für die SIL-Bestimmung eingesetzten Teams	34
D.5 Dokumentation der Ergebnisse der SIL-Bestimmung	35
D.6 Beispiel für eine Kalibrierung auf Basis eines typische Maßstabs	35
D.7 Risikograph für Umweltschäden	38
D.8 Risikograph für Vermögensschäden.....	39
D.9 Bestimmung des Integritätslevels von sicherheitstechnischen Schutzfunktionen, wenn die Auswirkungen eines Versagens mehr als einen Schadenstyp einschließen	39
Anhang E (informativ) Bestimmung der erforderlichen Sicherheits-Integritätslevel – Eine qualitative Methode: der Risikograph.....	40
E.1 Allgemeines	40
E.2 Typischer Einsatz von PLT-Funktionen.....	40
E.3 Aufbau des Risikographen.....	41
E.4 Einsatz des Risikographen beim Risiko von Personenschäden	41
E.5 Wichtige Gesichtspunkte bei der Anwendung von Risikographen	44
Anlage F (informativ) Analyse der Schutzebenen (LOPA-Layer of Protection Analysis)	45
F.1 Einführung.....	45
F.2 Analyse der Schutzebenen	45
F.3 Schadensereignis	47
F.4 Schweregrad.....	47
F.5 Auslösende Ursache.....	47
F.6 Eintrittswahrscheinlichkeit.....	47
F.7 Schutzebenen	47
F.8 Zusätzliche Schadensbegrenzungsmaßnahmen	48
F.9 Unabhängige Schutzebenen	48
F.10 Vorläufige Ereigniswahrscheinlichkeit	49
F.11 Integritätslevel der sicherheitstechnischen Funktion	49
F.12 Vermeidenswahrscheinlichkeit für das Ereignis	49
F.13 Gesamtrisiko	50
F.14 Beispiel	50
F.14.1 Schadensereignis und Schweregrad	50
F.14.2 Auslösende Ursache.....	50
F.14.3 Eintrittswahrscheinlichkeit.....	50
F.14.4 Auslegung der Schutzebenen.....	51
F.14.5 BPCS	51
F.14.6 Alarme.....	51
F.14.7 Zusätzliche Schadensbegrenzungsmaßnahmen	51
F.14.8 Unabhängige Schutzebenen (en: Independent Protection Layer, IPL)	51

F.14.9 Vorläufige Ereigniswahrscheinlichkeit	51
F.14.10 Sicherheitstechnisches System	52
F.14.11 Nächste sicherheitstechnische Funktion	52

Bilder

Bild 1 – Gesamtrahmen dieser Norm	8
Bild 2 – Typische Methoden der Risikominderung in prozesstechnischen Anlagen (z. B. Modell der Schutzebenen)	10
Bild 3 – Risikominderung: Allgemeiner Ansatz	13
Bild 4 – Risiko und Konzepte der Sicherheitsintegrität	14
Bild 5 – Zuordnung der Sicherheitsanforderungen zum SIS, zu Nicht-SIS-Systemen zum Schutz oder zur Schadensbegrenzung und anderen Schutzebenen	15
Bild A.1 – Tolerierbares Risiko und ALARP	17
Bild B.1 – Druckbehälter mit vorhandenen Sicherheitssystemen	20
Bild B.2 – Fehlerbaum für Überdruck im Behälter	22
Bild B.3 – Gefährliche Ereignisse bei vorhandenem Sicherheitssystem	23
Bild B.4 – Gefährliche Ereignisse bei redundanter Schutzebene	24
Bild B.5 – Gefährliche Ereignisse bei einer SIS-Sicherheitsfunktion, die SIL 2 entspricht	25
Bild C.1 – Schutzebenen	26
Bild C.2 – Beispiel für eine Matrix der Schutzebenen	30
Bild D.1 – Allgemeiner Risikograph	36
Bild D.2 – Risikograph für Umweltschäden	39
Bild E.1 – Risikograph aus DIN V 19250 zum Personenschutz (siehe Tabelle E.1)	42
Bild E.2 – Beziehung zwischen IEC 61511, DIN V 19250 und VDI/VDE 2180	44
Bild F.1 – Dokumentationsblatt zur Analyse der Schutzebenen (LOPA)	46

Tabellen

Tabelle A.1 – Beispiel für die Risikoklassifizierung von Unfällen	18
Tabelle A.2 – Interpretation der Risikoklassen	18
Tabelle B.1 – Ergebnisse der HAZOP-Analyse	21
Tabelle C.1 – Häufigkeit für gefährliche Ereignisse (ohne Berücksichtigung von Schutzebenen)	29
Tabelle C.2 – Kriterien zur Bewertung der Schwere von gefährlichen Ereignissen	29
Tabelle D.1 – Beschreibung der Parameter des Risikographen für die Prozessindustrie	33
Tabelle D.2 – Beispiel für eine Kalibrierung des allgemeinen Risikographen	36
Tabelle D.3 – Allgemeine Auswirkungen auf die Umwelt	38
Tabelle E.1 – Legende zum Risikographen (siehe Bild E.1)	43
Tabelle F.1 – LOPA-Informationen aus der HAZOP-Studie	46
Tabelle F.2 – Schweregrade von Schadensereignissen	47
Tabelle F.3 – Wahrscheinlichkeit von Ereignissen	47
Tabelle F.4 – Typische Ausfallwahrscheinlichkeiten von Schutzebenen (Schutz und Schadensbegrenzung)	48

Einführung

Sicherheitstechnische Systeme sind seit vielen Jahren für sicherheitstechnische Aufgaben in der Prozessindustrie im Einsatz. Wenn der Einsatz der Prozessleittechnik für sicherheitstechnische Funktionen effizient sein soll, dann muss sie bestimmten Mindestanforderungen 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 insofern betrachtet, als 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 Subsysteme vom Sensor bis zum Aktor.

Der „Sicherheitslebenszyklus“ und der „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 [Anhang A von IEC 61511-1](#)).

Diese Internationale Norm beschreibt die notwendigen Tätigkeiten im Sicherheits-Lebenszyklus, 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 Sicherheits-Lebenszyklus 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 zugrunde liegender 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.

Diese Norm gibt Anleitungen zur Ermittlung der erforderlichen Sicherheits-Integritätslevel in einer Gefährdungs- und Risikoanalyse. Dies soll einen Überblick über das weite Feld von Methoden ermöglichen, die weltweit hierfür angewendet werden. Zur betrieblichen Umsetzung einer dieser Methoden sind die vorliegenden Informationen jedoch nicht ausreichend.

Vor dem Fortfahren sollte sich der Leser die Grundsätze und die Bestimmung der Sicherheits-Integritätslevel (SIL) in der **IEC 61511-1** ansehen. Diese Norm enthält folgende Anhänge:

- Anhang A gibt einen Überblick über das Konzept des tolerierbaren Risikos und die „ALARP“-Methode
- Anhang B gibt einen Überblick über eine teilquantitative Methode zur Ermittlung des erforderlichen Sicherheits-Integritätslevels
- Anhang C gibt einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels eine Matrix verwendet
- Anhang D gibt einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels einen teilqualitativen Risikographen verwendet
- Anhang E gibt einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels einen qualitativen Risikographen verwendet
- Anhang F gibt einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels seine Analyse der Sicherheitsebenen vornimmt (LOPA)

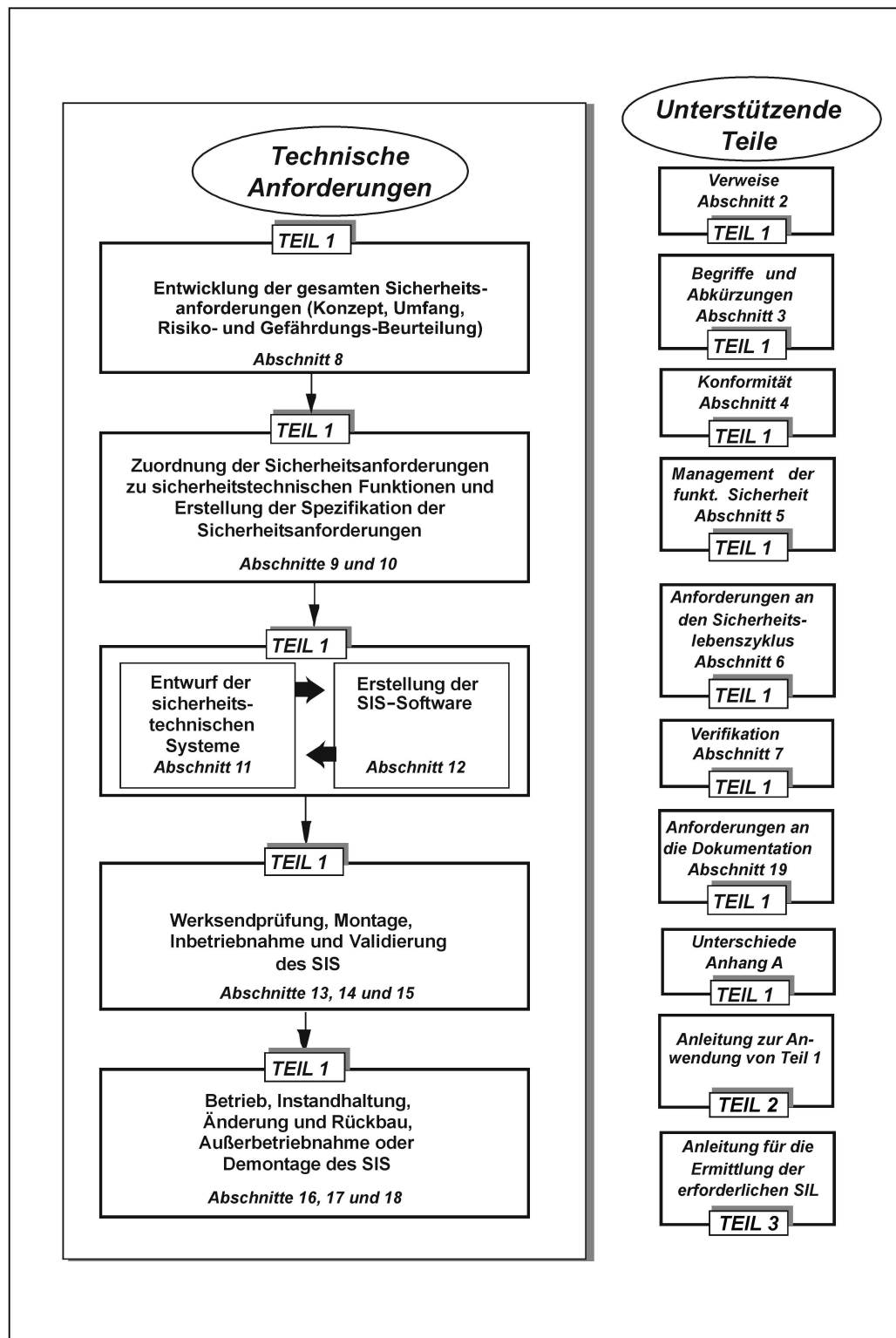


Bild 1 – Gesamtrahmen dieser Norm

1 Anwendungsbereich

1.1 Dieser Teil enthält Informationen über

- das grundlegende Konzept des Risikos und seiner Beziehung zur Sicherheitsintegrität, siehe [Abschnitt 3](#);
- die Bestimmung des tolerierbaren Risikos, siehe [Anhang A](#);
- verschiedene Methoden zur Bestimmung der SILs für die sicherheitstechnischen Funktionen, siehe [Anhänge B bis F](#).

Im Besonderen

- a) gilt dieser Teil dann, wenn die funktionale Sicherheit mit einer oder mehreren sicherheitstechnischen Funktionen dem Schutz der Mitarbeiter, der Öffentlichkeit oder der Umwelt dient;
- b) kann er auch in Fällen angewendet werden, bei denen nicht die Sicherheit, sondern beispielsweise der Schutz eines Wirtschaftsguts im Vordergrund steht;
- c) veranschaulicht er typische Methoden der Gefährdungs- und Risikoanalyse zur Festlegung der Anforderungen und der Sicherheits-Integritätslevel jeder sicherheitstechnischen Funktion;
- d) veranschaulicht er Techniken und Methoden zur Ermittlung der erforderlichen Sicherheits-Integritätslevel;
- e) gibt er einen Rahmen, wie Sicherheits-Integritätslevel ermittelt werden können, gibt aber keine Sicherheits-Integritätslevel für bestimmte Anwendungen vor;
- f) enthält er keine Beispiele, wie man die Anforderungen für andere Methoden zur Risikominderung ermittelt.

1.2 Die [Anhänge B bis F](#) zeigen quantitative und qualitative Ansätze auf und wurden vereinfacht, um die grundlegenden Prinzipien deutlich zu machen. Diese Anhänge verdeutlichen die grundlegenden Ansätze einer Reihe von Methoden, ohne diese zu gewichten.

ANMERKUNG Vor einer Anwendung der in diesen Anhängen enthaltenen Methoden sollten die jeweils angegebenen zugehörigen Quellentexte hinzugezogen werden.

1.3 Bild 1 zeigt den Gesamtrahmen von [IEC 61511-1](#), [IEC 61511-2](#) und IEC 61511-3 und die Rolle, die IEC 61511-3 bei der Erreichung der funktionalen Sicherheit für sicherheitstechnische Systeme spielt.

Siehe [Bild 2](#) als Überblick über Methoden zur Risikominderung.

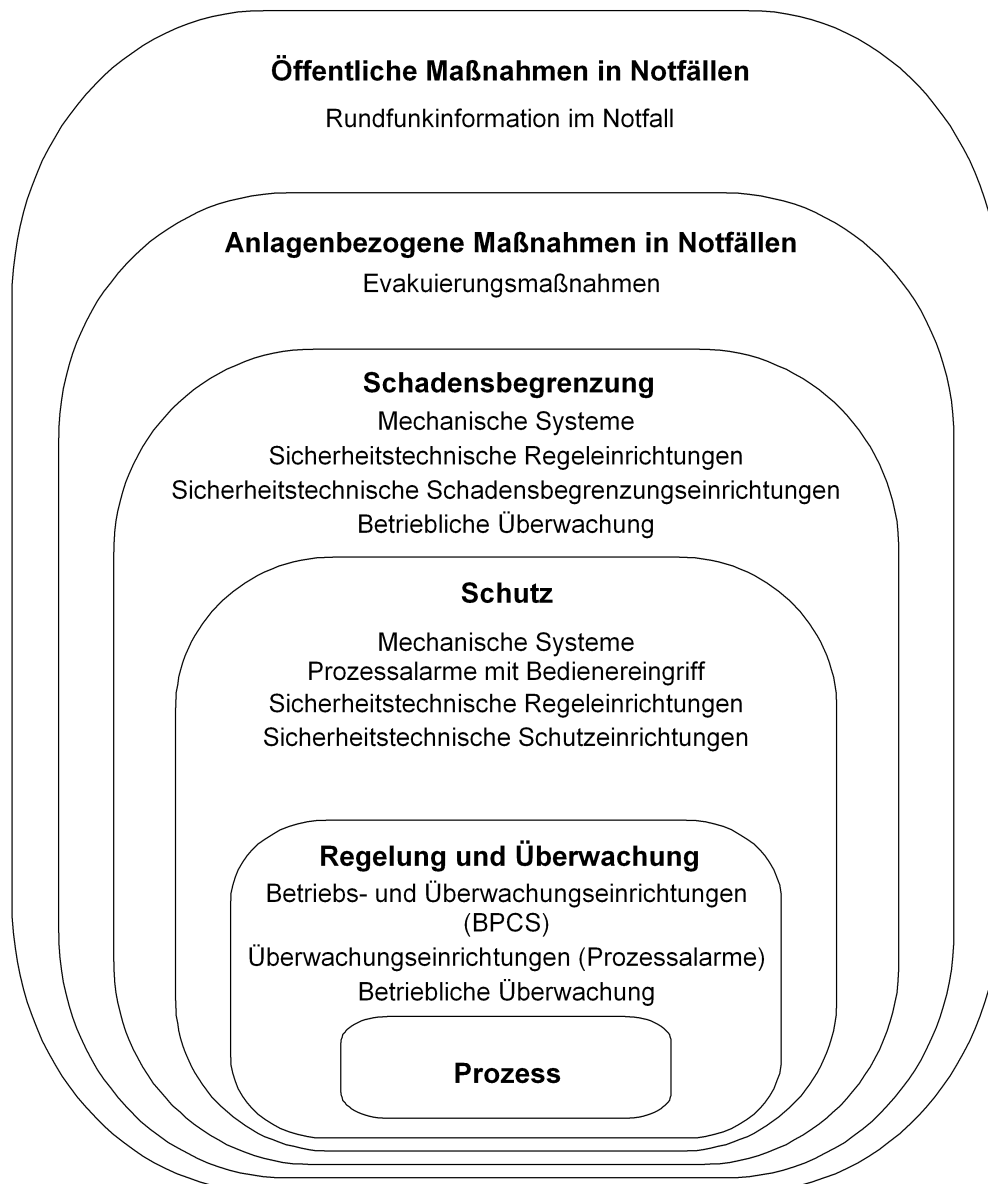


**Bild 2 – Typische Methoden der Risikominderung in prozesstechnischen Anlagen
(z. B. Modell der Schutzebenen)**

2 Definitionen und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Definitionen und Abkürzungen der IEC 61511-1, Abschnitt 3.

3 Risiko und Sicherheitsintegrität – Allgemeine Anleitung

3.1 Allgemeines

In diesem Abschnitt werden die dem Risikobegriff zugrunde liegenden Konzepte und der Zusammenhang zwischen Risiko und Sicherheitsintegrität dargestellt. Dies betrifft alle nachfolgend beschriebenen Methoden der Gefährdungs- und Risikoanalyse.

3.2 Notwendige Risikominderung

Die notwendige Risikominderung ist die Minderung des Risikos, die erreicht werden muss, um das tolerierbare Risiko für eine bestimmte Situation zu erreichen (welches entweder qualitativ¹⁾ oder quantitativ²⁾ angegeben werden darf). Das Konzept der notwendigen Risikominderung ist für die Entwicklung der Spezifikation der Sicherheitsanforderungen zu einer sicherheitstechnischen Funktion von grundlegender Bedeutung (insbesondere der Teil der Anforderungen zur Sicherheitsintegrität in der Spezifikation der Sicherheitsanforderungen). Der Zweck der Festlegung des tolerierbaren Risikos für einen bestimmten gefährlichen Vorfalls ist es, darzulegen, was im Hinblick sowohl auf die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls als auch auf seine besonderen Auswirkungen für sinnvoll gehalten wird. Sicherheitsbezogene Systeme werden entworfen, um die Häufigkeit (oder Wahrscheinlichkeit) des gefährlichen Vorfalls und/oder die Auswirkungen des gefährlichen Vorfalls zu mindern.

Wichtige Faktoren werden die Wahrnehmungen und Ansichten derjenigen sein, die dem gefährlichen Vorfall ausgesetzt sind. Zur Festlegung des tolerierbaren Risikos einer bestimmten Anwendung werden u. a. die folgenden Punkte betrachtet:

- Leitfäden der entsprechenden Behörden, die Sicherheitsregeln erstellen;
- Diskussionen und Übereinkünfte mit den verschiedenen Parteien, die an der Anwendung beteiligt sind;
- Industrienormen und -leitfäden;
- Empfehlungen aus der Industrie, von Spezialisten und aus der Wissenschaft;
- gesetzliche Anforderungen, sowohl allgemeine als auch diejenigen, die sich direkt auf die Anwendung beziehen.

3.3 Die Rolle der sicherheitstechnischen Systeme

Ein sicherheitstechnisches System beinhaltet die erforderlichen sicherheitstechnischen Funktionen, um den Prozess in einen sicheren Zustand zu bringen oder diesen aufrechtzuerhalten, und trägt auf diese Weise zur notwendigen Risikominderung auf das tolerierbare Risiko bei. So kann beispielsweise in der Spezifikation der Anforderungen an die Sicherheitsfunktionen festgelegt sein, dass beim Erreichen der Temperatur *X* ein Ventil *Y* öffnet, um Wasser in einen Behälter zu lassen.

Die notwendige Risikominderung lässt sich durch sicherheitstechnische Systeme (SIS) oder andere Schutzebenen oder eine Kombination von beidem erreichen.

Auch eine Person kann Bestandteil einer Sicherheitsfunktion sein. Beispielsweise könnte eine Person Informationen über den Zustand des Prozesses erhalten und aufgrund dieser Information eine Sicherheitsmaßnahme auslösen. Wenn eine Person Teil einer Sicherheitsfunktion ist, sollten alle Aspekte menschlichen Verhaltens berücksichtigt werden.

Sicherheitstechnische Systeme können entweder in Anforderungsbetriebsart oder in der Betriebsart mit kontinuierlicher Anforderung betrieben werden.

3.4 Sicherheitsintegrität

Die Sicherheitsintegrität setzt sich aus den folgenden beiden Elementen zusammen:

- a) **Sicherheitsintegrität der Hardware:** derjenige Teil der Sicherheitsintegrität, der sich auf zufällige Hardwareausfälle mit gefahrbringender Ausfallart bezieht. Das Erreichen der festgelegten Stufe der Sicherheitsintegrität der Hardware kann mit einer vernünftigen Genauigkeit abgeschätzt werden. Die

¹⁾ Um das tolerierbare Risiko zu erreichen, ist es erforderlich, die notwendige Risikominderung festzusetzen. Die **Anhänge D und E der IEC 61508-5** skizzieren qualitative Methoden, obwohl in den aufgeführten Beispielen die notwendige Risikominderung eher mit eingeschlossen und nicht im Einzelnen aufgeführt wird.

²⁾ Beispielsweise würde für ein gefährliches Ereignis mit bestimmten Auswirkungen typischerweise die höchste Eintrittshäufigkeit pro Jahr angegeben werden.

Anforderungen können daher unter Verwendung der üblichen Regeln für die Kombination von Wahrscheinlichkeiten zwischen den Teilsystemen aufgeteilt werden. Zum Erreichen einer angemessenen Sicherheitsintegrität der Hardware kann die Anwendung redundanter Architekturen notwendig sein.

- b) **Systematische Sicherheitsintegrität:** derjenige Teil der Sicherheitsintegrität, der sich auf systematische Ausfälle mit gefahrbringender Ausfallart bezieht. Obwohl die mittlere Ausfallrate für systematische Ausfälle abgeschätzt werden kann, führen die durch Entwurfsfehler und Ausfälle infolge gemeinsamer Ursache resultierenden Ausfalldaten dazu, dass die Verteilung der Ausfälle schwer vorherzusagen ist. Dies führt zu einer zunehmenden Ungewissheit in den Berechnungen der Ausfallwahrscheinlichkeiten für eine bestimmte Situation (zum Beispiel die Wahrscheinlichkeit eines Ausfalls eines SIS). Daher muss eine Beurteilung der Auswahl der besten Vorgehensweisen diese Ungewissheit verringern. Es ist zu beachten, dass Maßnahmen zur Reduzierung der Wahrscheinlichkeit zufälliger Hardwareausfälle nicht notwendigerweise einen Einfluss auf die Wahrscheinlichkeit eines systematischen Ausfalls haben. Methoden, wie zum Beispiel die Verwendung redundanter Kanäle mit identischer Hardware, die sehr wirksam in der Beherrschung zufälliger Hardwareausfälle sind, haben nur einen geringen Nutzen bei der Reduzierung systematischer Ausfälle.

Die gesamte Risikominderung durch die sicherheitstechnische(n) Funktion(en) und andere Schutzebenen muss so groß sein, dass sichergestellt ist:

- dass die Häufigkeit von Ausfällen der Sicherheitsfunktionen gering genug ist und somit die Häufigkeit des gefährlichen Ereignisses nicht größer ist als für das tolerierbare Risiko zulässig;
- dass die Sicherheitsfunktionen die Auswirkungen eines Ausfalls soweit verändern, dass das Risiko vertretbar bleibt.

Bild 3 veranschaulicht die allgemeinen Konzepte zur Risikominderung. Folgende Annahmen für das Modell wurden getroffen:

- eine prozesstechnische Anlage mit zugehörigem BPCS;
- zugehörige menschliche Faktoren sind vorhanden;
- die Schutzebenen umfassen:
 - 1) mechanische Schutzeinrichtungen,
 - 2) sicherheitstechnische Systeme,
 - 3) mechanische Einrichtungen zur Schadensbegrenzung.

ANMERKUNG **Bild 3** ist ein verallgemeinertes Risikomodell und veranschaulicht die allgemeinen Grundsätze. Bei der Erstellung des Risikomodells für eine spezifische Anwendung muss die besondere Art und Weise berücksichtigt werden, mit der die notwendige Risikominderung durch sicherheitstechnische Systeme und/oder andere Schutzebenen tatsächlich erreicht wird. Das sich dabei ergebende Risikomodell kann sich deshalb vom Modell des **Bildes 3** unterscheiden.

Folgende Risiken sind in den **Bildern 3** und **4** aufgeführt:

- das **prozesstechnische Risiko**, das aus den vorgegebenen gefährlichen Ereignissen des Prozesses, dem BPCS und den damit verbundenen Faktoren menschlichen Verhaltens erwächst. Die Bestimmung dieses Risikos erfolgt ohne Berücksichtigung sicherheitstechnischer Schutzmaßnahmen;
- das **tolerierbare Risiko** (Grenzwert für die Prozesssicherheit), welches in einem gegebenen Zusammenhang beruhend auf den aktuellen Wertvorstellungen der Gesellschaft akzeptiert wird;
- das **Restrisiko**, im Sinne dieser Norm das Risiko gefährlicher Ereignisse, das nach Einrichtung von Schutzebenen verbleibt.

Das prozesstechnische Risiko ergibt sich aus dem Risiko des Prozesses selbst unter Berücksichtigung der Risikominderung, die mit vorhandenen prozessleittechnischen Betriebs- und Überwachungseinrichtungen erreicht wird. Um unverhältnismäßige Annahmen zur Sicherheitsintegrität der prozessleittechnischen Betriebs- und Überwachungseinrichtungen zu vermeiden, werden in dieser Norm Grenzen für solche Annahmen festgelegt.

Als notwendige Risikominderung wird die niedrigste Stufe der Risikominderung bezeichnet, mit der sich das tolerierbare Risiko erreichen lässt. Diese Stufe kann durch eine oder durch eine Kombination mehrerer Methoden zur Risikominderung erreicht werden. In **Bild 3** wird gezeigt, wie, ausgehend von dem

prozesstechnischen Risiko, mit der notwendigen Risikominderung das vorgegebene tolerierbare Risiko erreicht wird.

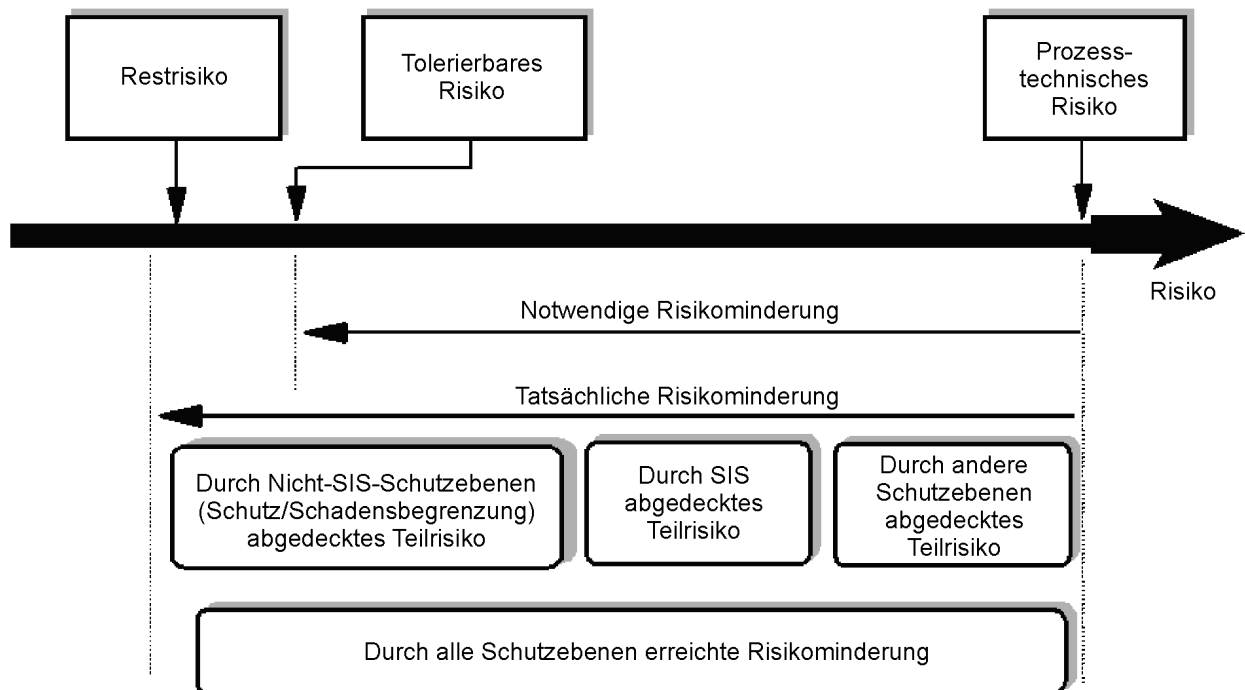


Bild 3 – Risikominderung: Allgemeiner Ansatz

3.5 Risiko und Sicherheitsintegrität

Es ist wichtig, den Unterschied zwischen Risiko und Sicherheitsintegrität klar herauszustellen. Das Risiko ist ein Maß für die Eintrittswahrscheinlichkeit eines bestimmten gefährlichen Ereignisses und dessen Auswirkungen. Es kann für verschiedene Situationen bestimmt werden (prozesstechnisches Risiko, tolerierbares Risiko, Restrisiko, siehe Bild 3). Das tolerierbare Risiko berücksichtigt gesellschaftliche und politische Faktoren. Die Sicherheitsintegrität ist ein Maß für die Wahrscheinlichkeit, mit der die sicherheitstechnischen Funktionen und andere Schutzebenen die geforderten Sicherheitsfunktionen ausführen. Sobald das tolerierbare Risiko festgesetzt und die notwendige Risikominderung abgeschätzt wurde, können die Anforderungen an die Sicherheitsintegrität des SIS aufgestellt werden.

ANMERKUNG Diese Zuordnung kann iterativ erfolgen, um eine den unterschiedlichen Anforderungen entsprechende optimale Lösung zu finden.

Die Rolle der Sicherheitsfunktionen bei der Erreichung der notwendigen Risikominderung ist in den Bildern 3 und 4 veranschaulicht.