

	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; 35.240.50

Ersatz für
DIN EN 61511-3
(VDE 0810-3):2005-05
 Siehe Anwendungsbeginn

**Funktionale Sicherheit –
 PLT-Sicherheitseinrichtungen für die Prozessindustrie –
 Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-
 Integritätslevel
 (IEC 61511-3:2016);
 Deutsche Fassung EN 61511-3:2017**

Functional safety –
 Safety instrumented systems for the process industry sector –
 Part 3: Guidance for the determination of the required safety integrity levels
 (IEC 61511-3:2016);
 German version EN 61511-3:2017

Sécurité fonctionnelle –
 Systèmes instrumentés de sécurité pour le secteur des industries de transformation –
 Partie 3: Conseils pour la détermination des niveaux exigés d'intégrité de sécurité
 (IEC 61511-3:2016);
 Version allemande EN 61511-3:2017

Gesamtumfang 109 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-08-25 angenommene Europäische Norm als DIN-Norm ist 2019-02-01.

Für **DIN EN 61511-3 (VDE 0810-3):2005-05** besteht eine Übergangsfrist bis 2020-04-21.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61511-3 (VDE 0810-3):2013-01.

Für dieses Dokument 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 in DIN und VDE (www.dke.de) zuständig.

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

Das IEC-Komitee hat entschieden, dass der Inhalt dieser Publikation bis zu dem Datum (stability date) unverändert bleiben soll, das auf der IEC-Website unter „<http://webstore.iec.ch>“ zu dieser Publikation angegeben ist. Zu diesem Zeitpunkt wird entsprechend der Entscheidung des Komitees die Publikation

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

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Änderungen

Gegenüber **DIN EN 61511-3 (VDE 0810-3):2005-05** wurden folgende Änderungen vorgenommen:

- a) Terminologie an die überarbeitete Terminologie des neuen Teils 1 dieser Normenreihe angepasst;
- b) Neue Methoden zur Bestimmung des Sicherheits-Integritätslevel in neuen informativen Anhänge aufgenommen;
- c) Gliederung überarbeitet.

Frühere Ausgaben

DIN EN 61511-3 (VDE 0810-3): 2005-05

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

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

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

Eine Information über den Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ist nachstehend wiedergegeben.

Tabelle NA.1

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61025:2007	IEC 61025:2006	DIN EN 61025:2007-08	–
EN 61165:2006	IEC 61165:2006	DIN EN 61165:2007-02	
EN 61511-1:2017	IEC 61511-1:2016	DIN EN 61508-1 (VDE 0803-1) <i>in Vorbereitung</i>	VDE 0803-1
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61508-6:2010	IEC 61508-6:2010	DIN EN 61508-6 (VDE 0803-6):2011-02	VDE 0803-6
–	IEC 61882:2001 <i>ersetzt durch:</i>	–	–
EN 61882:2016	IEC 61882:2016	DIN EN 61882 (VDE 0050-8):2017-02	VDE 0050-8
EN 62551:2012	IEC 62551:2012	DIN EN 62551 (VDE 0050-4):2013-08	VDE 0050-4
–	IEC/TS 62556:2014	–	–
CEN ISO/TR 12489:2016	ISO/TR 12489:2013	–	–

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 61025:2007-08, *Fehlzustandsbaumanalyse (IEC 61025:2006); Deutsche Fassung EN 61025:2007*

DIN EN 61165:2007-02, *Anwendung des Markoff-Verfahrens (IEC 61165:2006); Deutsche Fassung EN 61165:2006*

DIN EN 61508-1 (VDE 0803-1) (in Vorbereitung), *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61508-1:2016); Deutsche Fassung EN 61508-1:2017*

DIN EN 61508-5 (VDE 0803-5):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010*

DIN EN 61508-6 (VDE 0803-6):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2010); Deutsche Fassung EN 61508-6:2010*

DIN EN 61882 (VDE 0050-8):2017-02, *HAZOP-Verfahren (HAZOP-Studien) – Anwendungsleitfaden (IEC 61882:2016); Deutsche Fassung EN 61882:2016*

DIN EN 62551 (VDE 0050-4):2013-08, *Analysemethoden für Zuverlässigkeit – Petrinetze (IEC 62551:2012); Deutsche Fassung EN 62551:2012*

**Funktionale Sicherheit –
PLT-Sicherheitseinrichtungen für die Prozessindustrie –
Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-
Integritätslevel
(IEC 61511-3:2016)**

Functional safety –
Safety instrumented systems for the process
industry sector –
Part 3: Guidance for the determination of the
required safety integrity levels
(IEC 61511-3:2016)

Sécurité fonctionnelle –
Systèmes instrumentés de sécurité pour le
secteur des industries de transformation –
Partie 3: Conseils pour la détermination des
niveaux exigés d'intégrité de sécurité
(IEC 61511-3:2016)

Diese Europäische Norm wurde von CENELEC am 2016-08-25 angenommen. 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 CEN-CENELEC Management Centre 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 CEN-CENELEC Management Centre mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

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



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1 000 Brüssel

© 2017 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61511-3:2017 D

Europäisches Vorwort

Der Text des Dokuments 65A/779/FDIS, zukünftige 2. Ausgabe der IEC 61511-3, erarbeitet vom SC 65A „System aspects“ des IEC/TC 65 „Industrial process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 61511-3:2017 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2017-10-21
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-04-21

Dieses Dokument ersetzt **EN 61511-3:2004**.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CENELEC [und/oder CEN] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Anerkennungsnotiz

Der Text der Internationalen Norm IEC 61511-3:2016 wurde von CENELEC ohne irgendeine Abänderung als Europäische Norm angenommen.

In der offiziellen Fassung sind unter „Literaturhinweise“ zu den aufgelisteten Normen die nachstehenden Anmerkungen einzutragen:

IEC 61025:2006	ANMERKUNG	Harmonisiert als EN 61025:2007.
IEC 61165:2006	ANMERKUNG	Harmonisiert als EN 61165:2006.
IEC 61508-5:2010	ANMERKUNG	Harmonisiert als EN 61508-5:2010 .
IEC 61508-6:2010	ANMERKUNG	Harmonisiert als EN 61508-6:2010 .
IEC 62551:2012	ANMERKUNG	Harmonisiert als EN 62551:2012 .
ISO/TR 12489:2013	ANMERKUNG	Harmonisiert als CEN ISO/TR 12489:2016.

Anhang ZA (normativ)

Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ANMERKUNG 1 Ist eine internationale Publikation durch gemeinsame Abänderungen modifiziert worden, gekennzeichnet durch (mod.), dann gilt die entsprechende EN oder das HD.

ANMERKUNG 2 Die aktuellsten Informationen über die letzten Fassungen der Europäischen Normen, die im vorliegenden Anhang aufgelistet wurden, sind verfügbar unter <www.cenelec.eu>.

<u>Publikation</u>	<u>Jahr</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Jahr</u>
IEC 61511-1	2016	Functional safety – Safety instrumented systems for the process industry sector – Normative (uon) – Part 1: Framework, definitions, system, hardware and software requirements	EN 61511-1	2016

Inhalt

Seite

Europäisches Vorwort.....	2
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	3
Einleitung	10
1 Anwendungsbereich	13
2 Normative Verweisungen	14
3 Begriffe und Abkürzungen	14
Anhang A (informativ) Risiko und Sicherheitsintegrität – Allgemeine Anleitung	15
A.1 Allgemeines	15
A.2 Notwendige Risikominderung	15
A.3 Die Rolle der PLT-Sicherheitseinrichtungen	15
A.4 Risiko und Sicherheitsintegrität	17
A.5 Zuordnung der Sicherheitsanforderungen.....	18
A.6 Gefährliches Ereignis, gefährliche Situation und Schadensereignis.....	18
A.7 Sicherheits-Integritätslevel	19
A.8 Auswahl einer Methode zur Bestimmung der erforderlichen Sicherheits-Integritätslevel	19
Anhang B (informativ) Teilquantitative Methode – Ereignisbaumanalyse	21
B.1 Überblick.....	21
B.2 Übereinstimmung mit IEC 61511-1:2016	21
B.3 Beispiel	21
B.3.1 Allgemeines	21
B.3.2 Zielwert für die Prozesssicherheit	22
B.3.3 Gefährdungsanalyse	23
B.3.4 Teilquantitative Methode der Risikoanalyse.....	24
B.3.5 Risikoanalyse eines bestehenden Prozesses.....	24
B.3.6 Ereignisse, die den Zielwert für die Prozesssicherheit nicht erfüllen	27
B.3.7 Risikominderung mit Hilfe anderer Schutzebenen	27
B.3.8 Risikominderung durch eine PLT-Sicherheitsfunktion	27
Anhang C (informativ) Matrixmethode für die Sicherheitsebenen.....	30
C.1 Überblick.....	30
C.2 Zielwert für die Prozesssicherheit	31
C.3 Gefährdungsanalyse	32
C.4 Risikoanalyse	32
C.5 Matrix der Schutzebenen.....	33
C.6 Allgemeine Vorgehensweise	34
Anhang D (informativ) Teilqualitative Methode: der kalibrierte Risikograph.....	36
D.1 Überblick.....	36
D.2 Aufbau des Risikographen	36

	Seite
D.3 Kalibrierung	37
D.4 Mitglieder und Organisation des für die SIL-Bestimmung eingesetzten Teams	38
D.5 Dokumentation der Ergebnisse der SIL-Bestimmung	39
D.6 Beispiel für eine Kalibrierung auf Basis eines typische Maßstabs	39
D.7 Risikographen für Umweltschäden	42
D.8 Risikograph für Vermögensschäden	44
D.9 Bestimmung des Integritätslevels von PLT-Sicherheitsfunktionen, wenn zu den Auswirkungen eines Versagens mehr als ein Schadenstyp gehört	44
Anhang E (informativ) Qualitative Methode: der Risikograph	45
E.1 Allgemeines	45
E.2 Typischer Einsatz von Funktionen der Prozessleittechnik	45
E.3 Aufbau des Risikographen	46
E.4 Einsatz des Risikographen beim Risiko von Personenschäden	46
E.5 Wichtige Gesichtspunkte bei der Anwendung von Risikographen	48
Anhang F (informativ) Analyse der Schutzebenen (LOPA) (en: Layer of Protection Analysis)	49
F.1 Überblick	49
F.2 Schadensereignis	49
F.3 Schweregrad	50
F.4 Auslösende Ursache	51
F.5 Eintrittswahrscheinlichkeit	51
F.6 Schutzebenen	52
F.7 Zusätzliche Schadensbegrenzungsmaßnahmen	52
F.8 Unabhängige Schutzebenen (IPL)	53
F.9 Vorläufige Ereigniswahrscheinlichkeit	53
F.10 Integritätslevel der PLT-Sicherheitsfunktion	53
F.11 Vermeidenswahrscheinlichkeit für das Ereignis	54
F.12 Gesamtrisiko	54
F.13 Beispiel	54
F.13.1 Allgemeines	54
F.13.2 Schadensereignis und Schweregrad	54
F.13.3 Auslösende Ursache	54
F.13.4 Eintrittswahrscheinlichkeit	55
F.13.5 Auslegung der Schutzebenen	55
F.13.6 PLT-Betriebseinrichtungen (BPCS)	55
F.13.7 Alarme	55
F.13.8 Zusätzliche Schadensbegrenzungsmaßnahmen	55
F.13.9 Unabhängige Schutzebene(n) (IPL)	55
F.13.10 Vorläufige Ereigniswahrscheinlichkeit	56
F.13.11 PLT-Sicherheitseinrichtungen (SIS)	56

	Seite
F.13.12 Nächste PLT-Sicherheitsfunktion.....	56
Anhang G (informativ) Analyse der Schutzebenen unter Verwendung einer Risikomatrix	57
G.1 Überblick.....	57
G.2 Vorgehensweise	58
G.2.1 Allgemeines	58
G.2.2 Schritt 1: Allgemeine Information und Definition der Funktionsgruppen	59
G.2.3 Schritt 2: Beschreibung des gefährlichen Vorfalls.....	60
G.2.4 Schritt 3: Ermittlung der Häufigkeit des auslösenden Ereignisses.....	63
G.2.5 Schritt 4: Bestimmung des Schweregrads der Auswirkung des gefährlichen Vorfalls und des Risikoreduzierungsfaktors	64
G.2.6 Schritt 5: Ermittlung der unabhängigen Schutzebenen und des Risikoreduzierungsfaktors	65
G.2.7 Schritt 6: Ermittlung von Schadensbegrenzungssystemen und des Risikoreduzierungsfaktors	66
G.2.8 Schritt 7: Bestimmung der Risikolücke des CMS.....	67
G.2.9 Schritt 8: Ermittlung der Risikolücke des Szenarios.....	70
G.2.10 Schritt 9: Erstellung von Empfehlungen, sofern erforderlich.....	70
Anhang H (informativ) Qualitativer Ansatz für Risikoeinschätzung und Zuordnung der Sicherheits-Integritätslevel (SIL).....	72
H.1 Überblick.....	72
H.2 Risikoeinschätzung und SIL-Zuordnung	74
H.2.1 Allgemeines	74
H.2.2 Ermittlung/Angabe der Gefährdung.....	74
H.2.3 Risikoeinschätzung.....	74
H.2.4 Auswahl der Auswirkungsparameter (C) (Tabelle H.2).....	75
H.2.5 Eintrittswahrscheinlichkeit dieses Schadens.....	76
H.2.6 Einschätzung der Schadenswahrscheinlichkeit	79
H.2.7 SIL-Zuordnung.....	79
Anhang I (informativ) Erstellen und Kalibrieren eines Risikographen	84
I.1 Überblick.....	84
I.2 Schritte für das Erstellen und Kalibrieren eines Risikographen	84
I.3 Erstellen des Risikographen.....	84
I.4 Parameter des Risikographen.....	85
I.4.1 Auswahl der Parameter	85
I.4.2 Anzahl der Parameter.....	85
I.4.3 Parameterwerte	85
I.4.4 Parameterdefinition	85
I.4.5 Risikograph.....	86
I.4.6 Vertretbare Ereignishäufigkeit jeder Auswirkung	86
I.4.7 Kalibrierung	87
I.4.8 Fertigstellen des Risikographen	88

	Seite
Anhang J (informativ) Mehrfache Sicherheitseinrichtungen.....	89
J.1 Überblick	89
J.2 Angabe systematischer Abhängigkeiten	89
J.3 Teilquantitative Ansätze	92
J.4 Boolesche Ansätze	94
J.5 Zustandsübergang	97
Anhang K (informativ) Konzepte für ALARP und tolerierbares Risiko (ALARP: Prinzip der Verhältnismäßigkeit)	101
K.1 Allgemeines.....	101
K.2 ALARP-Modell.....	101
K.2.1 Überblick	101
K.2.2 Grenzwerte für das tolerierbare Risiko	102
Literaturhinweise	104
Bilder	
Bild 1 – Gesamtrahmen der Reihe IEC 61511	12
Bild 2 – Typische Schutzebenen und Maßnahmen zur Risikominderung.....	14
Bild A.1 – Risikominderung: allgemeiner Ansatz	17
Bild A.2 – Risiko und Konzepte der Sicherheitsintegrität	18
Bild A.3 – Schadensereignis.....	18
Bild A.4 – Zuordnung der Sicherheitsanforderungen zu Nicht-SIS-Schutzebenen und anderen Schutzebenen	20
Bild B.1 – Druckbehälter mit vorhandenen Sicherheitseinrichtungen	22
Bild B.2 – Fehlerbaum für Überdruck im Behälter.....	25
Bild B.3 – Gefährliche Vorfälle bei vorhandenen Sicherheitseinrichtungen.....	26
Bild B.4 – Gefährliche Vorfälle mit einer SIL2-PLT-Sicherheitsfunktion	29
Bild C.1 – Schutzebenen	30
Bild C.2 – Beispiel für eine Matrix der Schutzebenen	34
Bild D.1 – Allgemeiner Risikograph.....	40
Bild D.2 – Risikograph für Umweltschäden	43
Bild E.1 – Risikograph nach VDI/VDE 2180 – Personenschutz und Beziehung zu den SIL	47
Bild F.1 – Dokumentationsblatt zur Analyse der Schutzebenen (LOPA)	50
Bild G.1 – Schutzebenen mit hervorgehobenen proaktiven und reaktiven IPL.....	57
Bild G.2 – In Anhang G verwendeter Arbeitsablauf	59
Bild G.3 – Beispiel für eine Prozessabgrenzung für ein ausgewähltes Szenario	60
Bild G.4 – Akzeptables Sekundärrisiko	68
Bild G.5 – Nicht akzeptables Sekundärrisiko	68
Bild G.6 – Verändertes Risiko der Sekundärauswirkung	70
Bild H.1 – Prozessablauf der SIL-Zuordnung.....	73
Bild H.2 – Parameter für die Risikoeinschätzung.....	75

Bild I.1 – Zu betrachtende Parameter des Risikographen.....	85
Bild I.2 – Darstellung eines Risikographen mit den Parametern aus Bild I.1	86
Bild J.1 – Übliche Berechnungen.....	89
Bild J.2 – Genaue Berechnungen.....	90
Bild J.3 – Redundantes PLT-Sicherheitseinrichtung	92
Bild J.4 – Korrekturkoeffizienten für die Berechnungen der Häufigkeit des gefährlichen Vorfalls, wenn die Wiederholungsprüfungen gleichzeitig durchgeführt werden.....	93
Bild J.5 – Erweiterung des einfachen Beispiels.....	94
Bild J.6 – Fehlerbaummodellierung der mehrfachen PLT-Sicherheitseinrichtung in Bild J.5.....	95
Bild J.7 – Modellierung von Ausfällen infolge gemeinsamer Ursache zwischen SIS ₁ und SIS ₂	96
Bild J.8 – Auswirkung gestaffelter Prüfungen.....	96
Bild J.9 – Effekt einer Teilhubprüfung.....	97
Bild J.10 – Modellierung der Beschaffung der Reparaturressource.....	98
Bild J.11 – Beispiel der Ausgabewerte aus der Monte-Carlo-Simulation.....	99
Bild J.12 – Einfluss von Reparaturen infolge gemeinsam genutzter Reparaturressourcen.....	100
Bild K.1 – Tolerierbares Risiko und ALARP	102

Tabellen

Tabelle B.1 – Ergebnisse der HAZOP-Analyse.....	23
Tabelle C.1 – Häufigkeit gefährlicher Vorfälle (ohne Berücksichtigung von Schutzebenen)	33
Tabelle C.2 – Kriterien zur Bewertung der Auswirkung gefährlicher Vorfälle.....	33
Tabelle D.1 – Beschreibung der Parameter des Risikographen für die Prozessindustrie	37
Tabelle D.2 – Beispiel für eine Kalibrierung des allgemeinen Risikographen	41
Tabelle D.3 – Allgemeine Auswirkungen auf die Umwelt.....	43
Tabelle E.1 – Legende zum Risikographen (siehe Bild E.1)	48
Tabelle F.1 – LOPA-Informationen aus der HAZOP-Studie	50
Tabelle F.2 – Schweregrade von Schadensereignissen	51
Tabelle F.3 – Wahrscheinlichkeit von Ereignissen	51
Tabelle F.4 – Typische PFD _{avg} von Schutzebenen (Schutz und Schadensbegrenzung).....	52
Tabelle G.1 – Ausgewähltes Szenario aus dem HAZOP-Arbeitsblatt.....	61
Tabelle G.2 – Ausgewähltes Szenario aus dem HAZOP-Arbeitsblatt.....	62
Tabelle G.3 – Beispiele für auslösender Ursachen und ihren zugeordnete Häufigkeit.....	64
Tabelle G.4 – Entscheidungstabelle für den Schweregrad der Auswirkung	65
Tabelle G.5 – Matrix für den Risikoreduzierungsfaktor	65
Tabelle G.6 – Beispiele für unabhängige Schutzebenen (IPLs) mit zugeordneten Risikoreduzierungsfaktoren (RRF) und Ausfallwahrscheinlichkeiten bei Anforderung (PFD)	67
Tabelle G.7 – Beispiele für Schadensbegrenzungssysteme (CMS) mit zugeordneten Risikoreduzierungsfaktoren (RRF) und Ausfallwahrscheinlichkeiten bei Anforderung (PFD)	67
Tabelle G.8 – Schritt 7 – LOPA-Arbeitsblatt	69
Tabelle G.9 – Schritt 8 – LOPA-Arbeitsblatt	71
Tabelle H.1 – Verzeichnis der SIF und der zu bewertenden gefährlichen Ereignisse	74

	Seite
Tabelle H.2 – Auswirkungsparameter/Schweregrad	76
Tabelle H.3 – Aufenthaltsparameter/Einwirkungswahrscheinlichkeit (F)	77
Tabelle H.4 – Vermeidungsparameter/Vermeidungswahrscheinlichkeit.....	78
Tabelle H.5 – Parameter der Anforderungsrate (W)	78
Tabelle H.6 – Matrix des Risikographen (Formular der SIL-Zuordnung für PLT- Sicherheitsfunktionen).....	80
Tabelle H.7 – Beispiel für Auswirkungskategorien.....	81
Tabelle K.1 – Beispiel für die Risikoklassifizierung von Ereignissen	103
Tabelle K.2 – Interpretation der Risikoklassen.....	103

Einleitung

PLT-Sicherheitseinrichtungen (SIS) sind seit vielen Jahren für PLT-Sicherheitsfunktionen (SIF) in der Prozessindustrie im Einsatz. Wenn der Einsatz der Prozessleittechnik für PLT-Sicherheitsfunktionen effizient sein soll, dann muss sie bestimmten Mindestanforderungen entsprechen.

Die Reihe IEC 61511 behandelt die Anwendung von PLT-Sicherheitseinrichtungen in der Prozessindustrie. Sie behandelt außerdem die Gefährdungs- und Risikoanalyse des Prozesses, die durchzuführen ist, um die Spezifikation der PLT-Sicherheitseinrichtungen daraus abzuleiten. Die Beiträge anderer Sicherheitseinrichtungen werden nur im Hinblick auf die Anforderungen an die PLT-Sicherheitseinrichtung betrachtet. Diese umfasst dabei alle zur Ausführung einer PLT-Sicherheitsfunktion erforderlichen Geräte vom Sensor bis zum Aktor.

Die Reihe IEC 61511 besteht aus zwei grundlegenden Konzepten: Dem „Sicherheitslebenszyklus einer PLT-Sicherheitseinrichtung“ und der „Sicherheits-Integritätslevel“ (SIL).

Die in der Reihe IEC 61511 betrachteten PLT-Sicherheitseinrichtungen beruhen auf elektrischer/elektronischer/programmierbarer elektronischer Technologie. Wenn andere Technologien für Logiksysteme (Steuerungen) verwendet werden, können die grundlegenden Prinzipien dieser Norm in entsprechender Weise angewendet werden, um sicherzustellen, dass die Anforderungen an die funktionale Sicherheit erfüllt werden. In der Reihe IEC 61511 werden auch die Sensoren und Aktoren von PLT-Sicherheitseinrichtungen betrachtet, unabhängig von der Technologie, in der sie ausgeführt sind. Die Reihe IEC 61511 wurde als sektorspezifische Ausprägung der Reihe IEC 61508 entwickelt. Die Reihe IEC 61511 ist innerhalb des Rahmens der IEC 61508 zugeschnitten auf die Prozessindustrie.

Die Reihe IEC 61511 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 inhärent sicheren Prozesses erreichen. Dies ist jedoch in manchen Fällen nicht möglich oder umsetzbar. 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) beruhen. Um diesen Ansatz zu erleichtern, umfasst die Reihe IEC 61511 Folgendes:

- die Durchführung einer Gefährdungs- und Risiko-Beurteilung, um die übergreifenden Sicherheitsanforderungen festzulegen;
- eine Zuordnung der Sicherheitsanforderungen zu den PLT-Sicherheitseinrichtungen;
- Arbeiten innerhalb eines Betrachtungsrahmens, der alle sicherheitstechnischen Methoden zur Erlangung funktionaler Sicherheit umfasst;
- Beschreibungen der Ausführung bestimmter Tätigkeiten, die sich auf alle Methoden zur Erlangung der funktionalen Sicherheit anwenden lassen, wie z. B. Sicherheits-Management..
- Behandlung aller Phasen innerhalb des Sicherheits-Lebenszyklus vom anfänglichen Konzept, Entwurf, Ausführung, Betrieb und Instandhaltung bis hin zur Außerbetriebnahme;
- bereits bestehenden oder neuen landesspezifischen Normen für die Prozessindustrie wird es ermöglicht, mit dieser Norm harmonisiert zu werden.

Die Reihe IEC 61511 strebt nach einer hohen Übereinstimmung (beispielsweise bezüglich zugrundeliegender Prinzipien, Terminologie, Dokumentation) innerhalb der Prozessindustrie. Dies sollte sowohl Vorteile für die Sicherheit als auch ökonomische Vorteile bringen.

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

IEC 61511-3 gibt Anleitungen zur Ermittlung der erforderlichen Sicherheits-Integritätslevel (SIL) mit Hilfe einer Gefährdungs- und Risikobewertung. Diese geben einen Überblick über das weite Feld von Methoden, die weltweit dafür angewendet werden. Zur Umsetzung einer dieser Methoden sind die vorliegenden Informationen jedoch nicht ausreichend.

Vor dem Fortfahren sollte man sich die Grundsätze und Bestimmung der Sicherheits-Integritätslevel (SIL) in IEC 61511-1:2016 ansehen. Die informativen Anhänge der IEC 61511-3 behandeln das Folgende:

- Anhang A bietet Informationen, die auf alle hier erläuterten Methoden zur Gefährdungs- und Risiko-Beurteilung zutreffen.
- Anhang B bietet einen Überblick über eine teilquantitative Methode zur Ermittlung des erforderlichen Sicherheits-Integritätslevels.
- Anhang C bietet einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels eine Matrix verwendet.
- Anhang D bietet einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels einen teilqualitativen Risikographen verwendet.
- Anhang E bietet einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels einen qualitativen Risikographen verwendet.
- Anhang F bietet einen Überblick über eine Methode, die zur Ermittlung des erforderlichen Sicherheits-Integritätslevels eine Analyse der Schutzebenen vornimmt (LOPA).
- Anhang G bietet eine Analyse der Schutzebenen unter Verwendung einer Risikomatrix.
- Anhang H bietet einen Überblick über einen qualitativen Ansatz für die Risikoeinschätzung und die SIL-Zuordnung;
- Anhang I bietet einen Überblick über die grundlegenden Schritte für die Erstellung und die Kalibrierung eines Risikographen.
- Anhang J bietet einen Überblick über den Einfluss von mehrfachen Sicherheitseinrichtungen auf die Bestimmung des erforderlichen SIL.
- Anhang K bietet einen Überblick über das Konzept des tolerierbaren Risikos und die ALARP-Methode.

Bild 1 zeigt den Gesamtrahmen für IEC 61511-1, IEC 61511-2 und IEC 61511-3 und welche Rolle die Reihe IEC 61511 für PLT-Sicherheitseinrichtungen zum Erreichen funktionaler Sicherheit spielt.

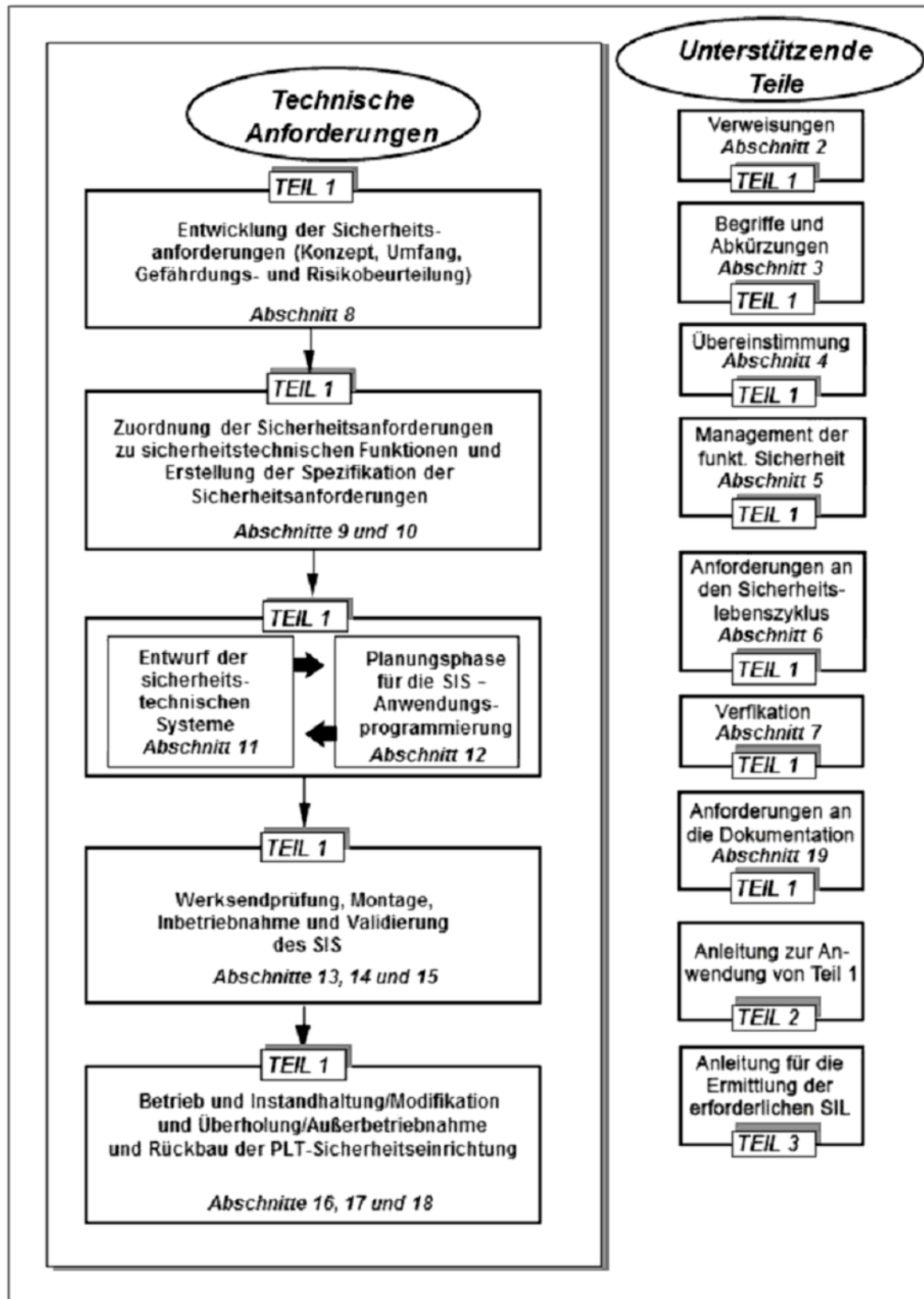


Bild 1 – Gesamtrahmen der Reihe IEC 61511

1 Anwendungsbereich

Dieser Teil der IEC 61511 enthält Informationen über:

- die grundlegenden Konzepte des Risikos und die Beziehung des Risikos zur Sicherheitsintegrität (siehe Abschnitt [A.4](#));
- die Bestimmung des tolerierbaren Risikos (siehe [Anhang K](#));
- verschiedene Methoden zur Bestimmung der SIL für die PLT-Sicherheitsfunktionen (SIF) (siehe [Anhänge B bis K](#));
- den Einfluss von Mehrfach-Sicherheitseinrichtungen auf die Berechnungen, die bestimmen der Fähigkeit, die gewünschte Risikominderung zu erzielen (siehe [Anhang J](#)).

Im Besonderen, dieser Teil der IEC 61511:

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

ANMERKUNG Die Beispiele in den Anhängen dieser Norm zeigen nur, wie die Anforderungen der IEC 61511 in einem speziellen Fall erfüllt werden, und der Anwender sollte sich selbst überzeugen, dass die gewählten Methoden und Techniken für seine Situation geeignet sind.

Die [Anhänge B bis K](#) zeigen quantitative und qualitative Ansätze auf, um die grundlegenden Prinzipien deutlich zu machen. Sie wurden aufgenommen, um die Grundsätze einer Methode zu veranschaulichen, ohne sie vollständig darzustellen.

ANMERKUNG 1 Vor einer Anwendung der in diesen Anhängen enthaltenen Methoden sollten die jeweils angegebenen zugehörigen Quellen hinzugezogen werden.

ANMERKUNG 2 Die in Teil 3 enthaltenen Methoden zur SIL-Ermittlung brauchen nicht für jede Anwendung geeignet zu sein. Insbesondere können für Betriebsarten mit kontinuierlicher Anforderung oder hoher Anforderungsrate spezielle Techniken oder zusätzliche Gesichtspunkte erforderlich sein, die nicht erläutert sind.

ANMERKUNG 3 Die hier angegebenen Methoden können zu nicht-konservativen Ergebnissen führen, wenn ihre zugrundeliegenden Randbedingungen verletzt werden und Gesichtspunkte wie gemeinsame Ursachen, Fehlertoleranz, ganzheitliche Betrachtung der Anwendung, Mangel an Erfahrung mit der angewendeten Methode, Unabhängigkeit der Schutzebenen usw. nicht sorgfältig berücksichtigt werden. Siehe [Anhang J](#).

[Bild 2](#) gibt einen Überblick über typische Schutzebenen und Maßnahmen zur Risikominderung.

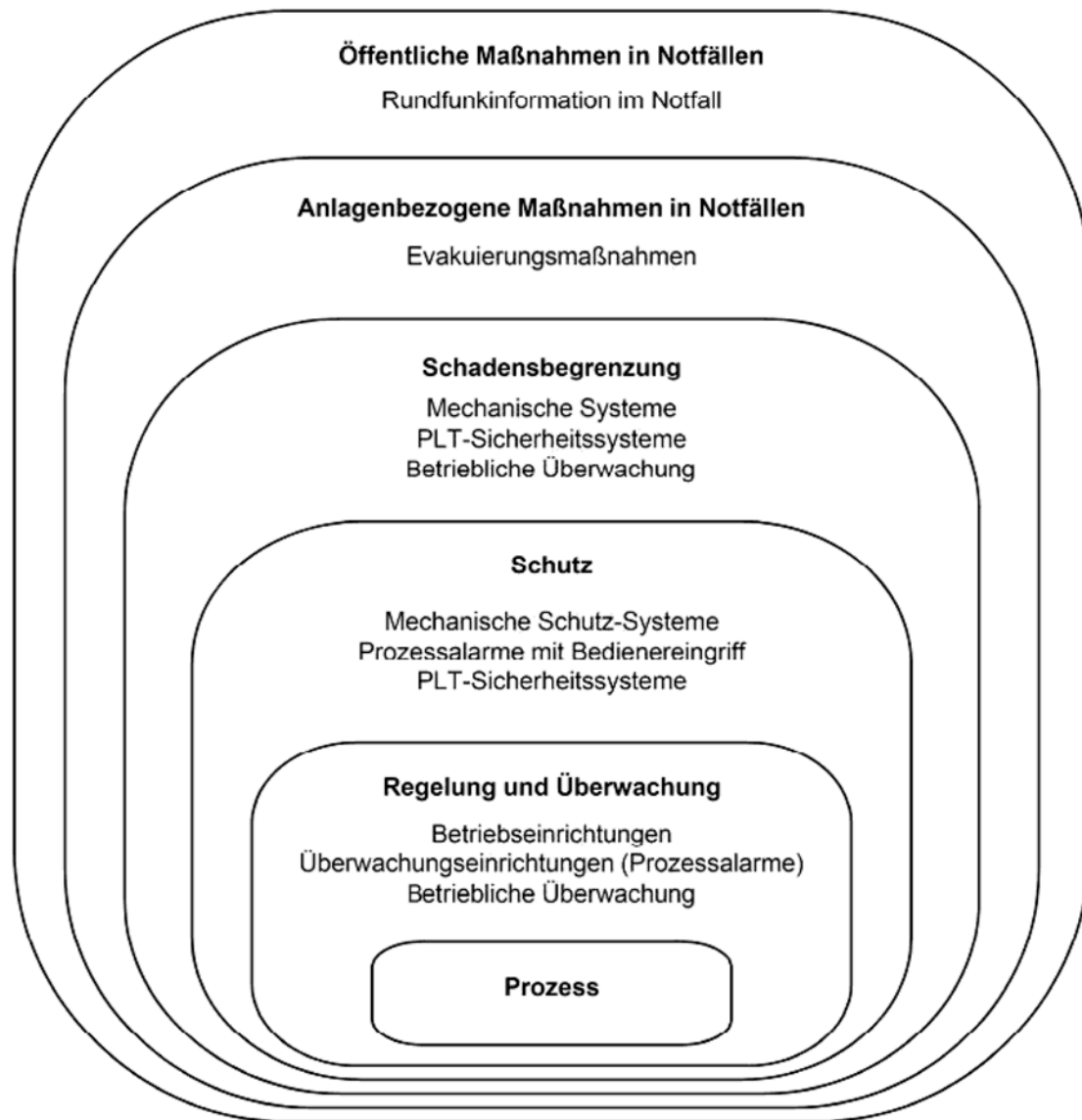


Bild 2 – Typische Schutzebenen und Maßnahmen zur Risikominderung

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 61511-1:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: framework, definitions, system, hardware and application programming requirements*

3 Begriffe und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe und Abkürzungen nach **IEC 61511-1:2016**.

Die Anhänge in diesem Teil 3 sind informativ und nicht normativ. Die Anwendung einer in den Anhängen des Teils 3 beschriebenen Methode garantiert nicht die Übereinstimmung mit den Anforderungen der **IEC 61511-1:2016**.

Anhang A (informativ)

Risiko und Sicherheitsintegrität – Allgemeine Anleitung

A.1 Allgemeines

In Anhang A 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.

A.2 Notwendige Risikominderung

Die notwendige Risikominderung (die entweder qualitativ (siehe Anmerkung 1) oder quantitativ (siehe Anmerkung 2) angegeben werden kann) ist die Minderung des Risikos, die erreicht werden muss, um das tolerierbare Risiko (z. B. den Zielwert für die Prozesssicherheit) für eine bestimmte Situation zu erreichen. Das Konzept der notwendigen Risikominderung ist für die Entwicklung der Spezifikation der Sicherheitsanforderungen (SRS) der PLT-Sicherheitsfunktion von grundlegender Bedeutung (insbesondere die Anforderung der Sicherheitsintegrität). Der Zweck der Festlegung des tolerierbaren Risikos (z. B. des Zielwerts für die Prozesssicherheit) für einen bestimmten gefährlichen Vorfall ist es, darzulegen, was im Hinblick sowohl auf seine Häufigkeit als auch auf seine besonderen Auswirkungen für sinnvoll gehalten wird. Schutzebenen (Bild 2) werden entworfen, um die Häufigkeit des gefährlichen Vorfalls oder seine Auswirkungen zu mindern.

Wichtige Faktoren bei der Bewertung des tolerierbaren Risikos sind auch die Wahrnehmungen und Ansichten derjenigen, die dem gefährlichen Vorfall ausgesetzt sind. Zur Festlegung des tolerierbaren Risikos einer bestimmten Anwendung können eine Anzahl von Eingangsgrößen betrachtet werden. Dazu gehören:

- Leitfäden der entsprechenden Behörden;
- 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;
- allgemeine und auf die spezifische Anwendung bezogene rechtliche und gesetzliche Anforderungen.

ANMERKUNG 1 Um das tolerierbare Risiko zu erreichen, ist es erforderlich, die notwendige Risikominderung festzulegen. IEC 61508-5:2010, Anhänge D und E skizzieren qualitative Methoden, obwohl in den aufgeführten Beispielen die notwendige Risikominderung eher eingeschlossen und nicht im Einzelnen aufgeführt wird.

ANMERKUNG 2 Beispielsweise würde für einen gefährlichen Vorfall mit bestimmten Auswirkungen typischerweise die höchste Eintrittshäufigkeit je Jahr angegeben werden.

A.3 Die Rolle der PLT-Sicherheitseinrichtungen

Eine PLT-Sicherheitseinrichtung (SIS) realisiert die erforderliche(n) PLT-Sicherheitsfunktion(en) (SIFs), um den Prozess in einen sicheren Zustand zu bringen oder diesen aufrechtzuerhalten, und trägt auf diese Weise zur notwendigen Risikominderung bei, um das tolerierbare Risiko zu erreichen. So kann beispielsweise in der Spezifikation der Sicherheitsanforderungen (SRS) 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 eine PLT-Sicherheitseinrichtung oder eine Kombination von mehreren PLT-Sicherheitseinrichtungen oder andere Schutzebenen 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 Sicherheitsmaß-

nahme auslösen. Wenn eine Person Teil einer Sicherheitsfunktion ist, sollten alle Aspekte menschlichen Verhaltens berücksichtigt werden.

Eine PLT-Sicherheitsfunktion kann entweder in der Anforderungsbetriebsart oder in der Betriebsart mit kontinuierlicher Anforderung betrieben werden.

Die Sicherheitsintegrität setzt sich aus den folgenden beiden Elementen zusammen:

- a) **Sicherheitsintegrität der Hardware** – derjenige Teil der Sicherheitsintegrität, der sich auf zufällige Hardwareausfälle mit gefährlicher Ausfallart bezieht. Das Erreichen der festgelegten Stufe der Sicherheitsintegrität der Hardware kann mit einer vernünftigen Genauigkeit abgeschätzt werden und die Anforderungen können daher unter Verwendung der üblichen Regeln für die Kombination von Wahrscheinlichkeiten und unter Berücksichtigung von Ausfällen infolge gemeinsamer Ursache 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 gefährlicher Ausfallart bezieht. Obwohl der Beitrag einiger systematischer Ausfälle abgeschätzt werden kann, führen die Ausfalldaten für Entwurfsfehler und Ausfälle infolge gemeinsamer Ursache dazu, dass die Verteilung der Ausfälle schwer vorherzusagen ist. Dies führt zu einer Zunahme der Unsicherheit für die Berechnungen der Ausfallwahrscheinlichkeiten für eine bestimmte Situation (zum Beispiel die Wahrscheinlichkeit eines Ausfalls einer PLT-Sicherheitseinrichtung). Daher muss die beste Vorgehensweise ausgewählt werden, um diese Ungewissheit zu 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 PLT-Sicherheitsfunktion zusammen mit anderen Schutzebenen muss so groß sein, dass sichergestellt ist:

- dass die Häufigkeit von Vorfällen infolge eines Ausfalls der Sicherheitsfunktionen so gering ist, dass die Häufigkeit gefährlicher Vorfälle nicht größer ist als für das tolerierbare Risiko zulässig, und/oder,
- dass die Sicherheitsfunktionen die Auswirkungen eines Ausfalls soweit verändern, dass das Risiko vertretbar bleibt.

Bild A.1 veranschaulicht die allgemeinen Konzepte zur Risikominderung. Folgende Annahmen für das Modell wurden getroffen:

- Es gibt einen Prozess mit einer zugehörigen PLT-Betriebseinrichtung (BPCS);
- zugehörige menschliche Faktoren sind vorhanden;
- die Schutzebenen umfassen:
 - mechanisches Sicherheitseinrichtungssystem,
 - PLT-Sicherheitseinrichtungen,
 - Nicht-PLT-Sicherheitseinrichtungen,
 - mechanisches Schadensbegrenzungssysteme.

ANMERKUNG 1 **Bild A.1** ist ein verallgemeinertes Risikomodell zur Veranschaulichung der 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 PLT-Sicherheitseinrichtungen und/oder andere Schutzebenen tatsächlich erreicht wird. Das sich dabei ergebende Risikomodell kann sich deshalb vom Modell in **Bild A.1** unterscheiden.

Folgende Risiken sind in den **Bildern A.1** und **A.2** aufgeführt:

- Prozessrisiko – das Risiko, das aus den vorgegebenen gefährlichen Vorfall des Prozesses, der PLT-Betriebseinrichtungen und den damit verbundenen Faktoren menschlichen Verhaltens erwächst; die Bestimmung dieses Risikos erfolgt ohne Berücksichtigung von Sicherheitsmaßnahmen;

- tolerierbares Risiko (Zielwert für die Prozesssicherheit) – das Risiko, welches in einem gegebenen Zusammenhang beruhend auf den aktuellen Wertvorstellungen der Gesellschaft akzeptiert wird;
- verbleibendes Risiko – das Risiko eines gefährlichen Vorfalles nach der Hinzufügung von Schutzebenen.

Das Prozessrisiko ergibt sich aus dem Risiko des Prozesses selbst unter Berücksichtigung der Risikominderung, die mit dem Prozessleitsystem erreicht wird. Um unverhältnismäßige Annahmen zur Sicherheitsintegrität der Betriebseinrichtungen zu verhindern, werden in der Reihe IEC 61511 Grenzen für solche Annahmen festgelegt.

Als notwendige Risikominderung wird die niedrigste Risikominderung bezeichnet, mit der sich das tolerierbare Risiko erreichen lässt. Dieser Wert kann durch eine Methode oder durch eine Kombination mehrerer Methoden zur Risikominderung erreicht werden. In Bild A.1 wird gezeigt, wie ausgehend vom Prozessrisiko mit der notwendigen Risikominderung das vorgegebene tolerierbare Risiko erreicht wird.

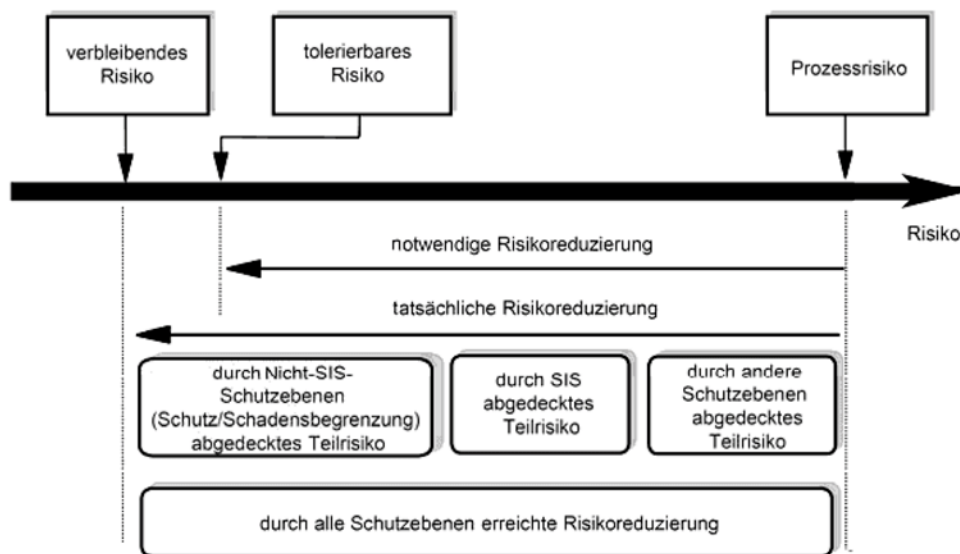


Bild A.1 – Risikominderung: allgemeiner Ansatz

ANMERKUNG 2 In einigen Anwendungen können die Risikoparameter (z. B. Häufigkeit und Wahrscheinlichkeit eines Ausfalls bei Anforderung) nicht einfach wie in Bild A.1 dargestellt kombiniert werden, um den Risiko-Zielwert zu erreichen, ohne die in [Anhang J](#) aufgeführten Faktoren zu berücksichtigen. Der Grund dafür sind Überschneidungen, Ausfälle infolge gemeinsamer Ursache und die übergreifenden Abhängigkeiten zwischen den verschiedenen Schutzebenen.

A.4 Risiko und Sicherheitsintegrität

Es ist wichtig, den Unterschied zwischen Risiko und Sicherheitsintegrität klar herauszustellen. Das Risiko ist ein Maß für die Häufigkeit eines bestimmten gefährlichen Vorfalles und dessen Auswirkungen. Es kann für verschiedene Situationen bestimmt werden (Prozessrisiko, tolerierbares Risiko, verbleibendes Risiko, siehe Bild A.1). Das tolerierbare Risiko berücksichtigt gesellschaftliche und politische Faktoren. Die Sicherheitsintegrität ist ein Maß für die Wahrscheinlichkeit, mit der die PLT-Sicherheitsfunktionen und andere Schutzebenen die festgelegte Risikominderung erzielen. Sobald das tolerierbare Risiko festgesetzt und die notwendige Risikominderung abgeschätzt wurde, können die Anforderungen an die Sicherheitsintegrität der PLT-Sicherheitseinrichtung zugeordnet werden.

ANMERKUNG Diese Zuordnung kann iterativ erfolgen, um eine den unterschiedlichen Anforderungen entsprechende optimale Lösung zu finden. Die Rolle der Sicherheitsfunktionen für das Erreichen der notwendigen Risikominderung ist in den Bildern A.1 und [A.2](#) veranschaulicht.

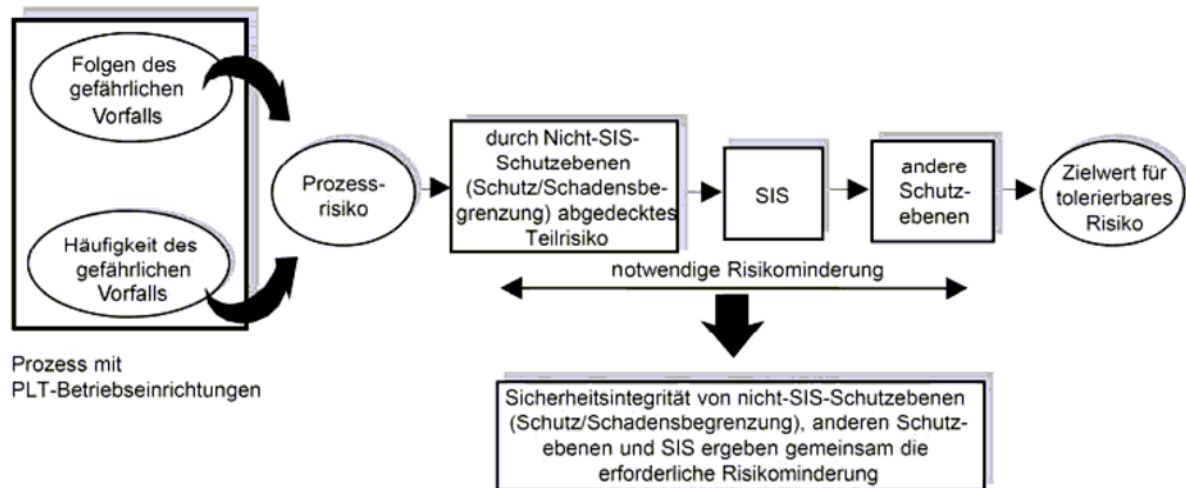


Bild A.2 – Risiko und Konzepte der Sicherheitsintegrität

A.5 Zuordnung der Sicherheitsanforderungen

Die Zuordnung der Sicherheitsanforderungen (sowohl der Sicherheitsfunktionen als auch der Sicherheitsintegrität) zur PLT-Sicherheitseinrichtung und zu anderen Schutzebenen wird in [Bild A.4](#) veranschaulicht. Die Anforderungen für die Zuordnung finden sich in [IEC 61511-1](#)–, [Abschnitt 9](#).

Die Methoden, mit denen die Anforderungen für die Sicherheitsintegrität den PLT-Sicherheitseinrichtungen, sicherheitsbezogenen Systemen anderer Technologien und weiteren Einrichtungen zur Risikominderung zugeordnet werden, hängen im Wesentlichen davon ab, ob die notwendige Risikominderung als Zahlenwert oder aber auf qualitative Weise angegeben wird. Entsprechend werden diese Ansätze auch als „teilquantitative“, „teilqualitative“ bzw. „qualitative“ Methoden bezeichnet (siehe [Anhang B](#) bis [Anhang I](#)).

A.6 Gefährliches Ereignis, gefährliche Situation und Schadensereignis

Die Begriffe „gefährliches Ereignis“ und „gefährliche Situation“ werden in den folgenden Anhängen häufig benutzt. [Bild A.3](#) soll den Unterschied zwischen den Begriffen veranschaulichen, indem die Entwicklung vom gefährlichen Ereignis zu einer gefährlichen Situation durch den Verlust der Regelung bis zum Eintreten eines Schadensereignisses dargestellt wird.

[Bild A.3](#) verwendet Personenschäden, es kann aber genauso für Umwelt- oder Sachschäden angewendet werden.

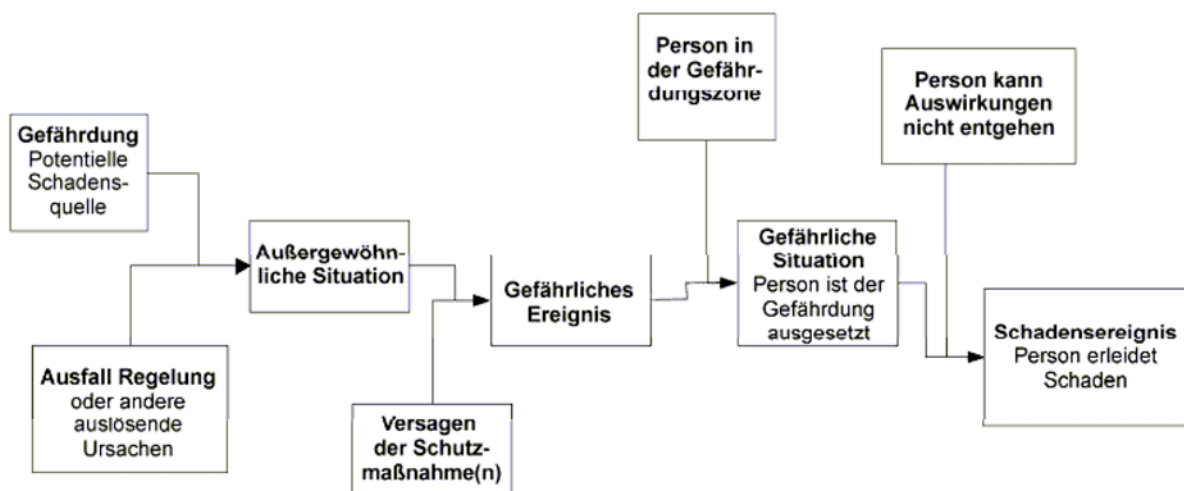


Bild A.3 – Schadensereignis

Bild A.3 zeigt, wie der Verlust einer Regelung oder eine beliebige andere Auslöseursache zu einer außergewöhnlichen Situation führen und zu einer Anforderung von Sicherheitsmaßnahmen wie Sicherheitsalarmen, PLT-Sicherheitseinrichtungen, Entlastungsventilen usw. führen kann. Ein gefährliches Ereignis entsteht, wenn eine Anforderung eintritt und die entsprechenden Sicherheitsmaßnahmen ausgefallen sind und nicht wie vorgesehen arbeiten. Ein gefährliches Ereignis an sich verursacht nicht notwendigerweise einen Schaden, sollte(n) sich aber eine oder mehrere Personen in der Gefährdungszone befinden und damit dem gefährlichen Ereignis ausgesetzt sein, führt dies zu einer gefährlichen Situation. Falls die Person(en) den gefährlichen Auswirkungen des Ereignisses nicht entkommen kann (können), wird dies als ein gefährliches Ereignis mit Personenschaden bezeichnet.

A.7 Sicherheits-Integritätslevel

In **IEC 61511-1:2016** werden vier Sicherheits-Integritätslevel festgelegt, wobei SIL 4 das höchste Niveau und SIL 1 das niedrigste Niveau darstellt.

Die Ausfallgrenzwerte für diese vier Sicherheits-Integritätslevel sind in **IEC 61511-1**–, **Tabellen 4** und **5** angegeben. Es werden jeweils zwei Werte aufgeführt, wobei der eine für PLT-Sicherheitseinrichtungen in der Anforderungsbetriebsart gilt und der andere für PLT-Sicherheitseinrichtungen in der Betriebsart mit kontinuierlicher Anforderung/mit hoher Anforderungsrate.

ANMERKUNG Für PLT-Sicherheitseinrichtungen in der Anforderungsbetriebsart mit niedriger Anforderungsrate wird als betreffender Ausfallgrenzwert die mittlere Wahrscheinlichkeit, dass die Funktion bei Anforderung ihrer planmäßigen Aufgabe ausfällt, verwendet. Für PLT-Sicherheitseinrichtungen in der Betriebsart mit kontinuierlicher Anforderung/ hoher Anforderungsrate wird als betreffender Ausfallgrenzwert die mittlere Häufigkeit eines gefährlichen Ausfalls (siehe **IEC 61511-1:2016**, **3.2.83** und **Tabelle 5**) angegeben.

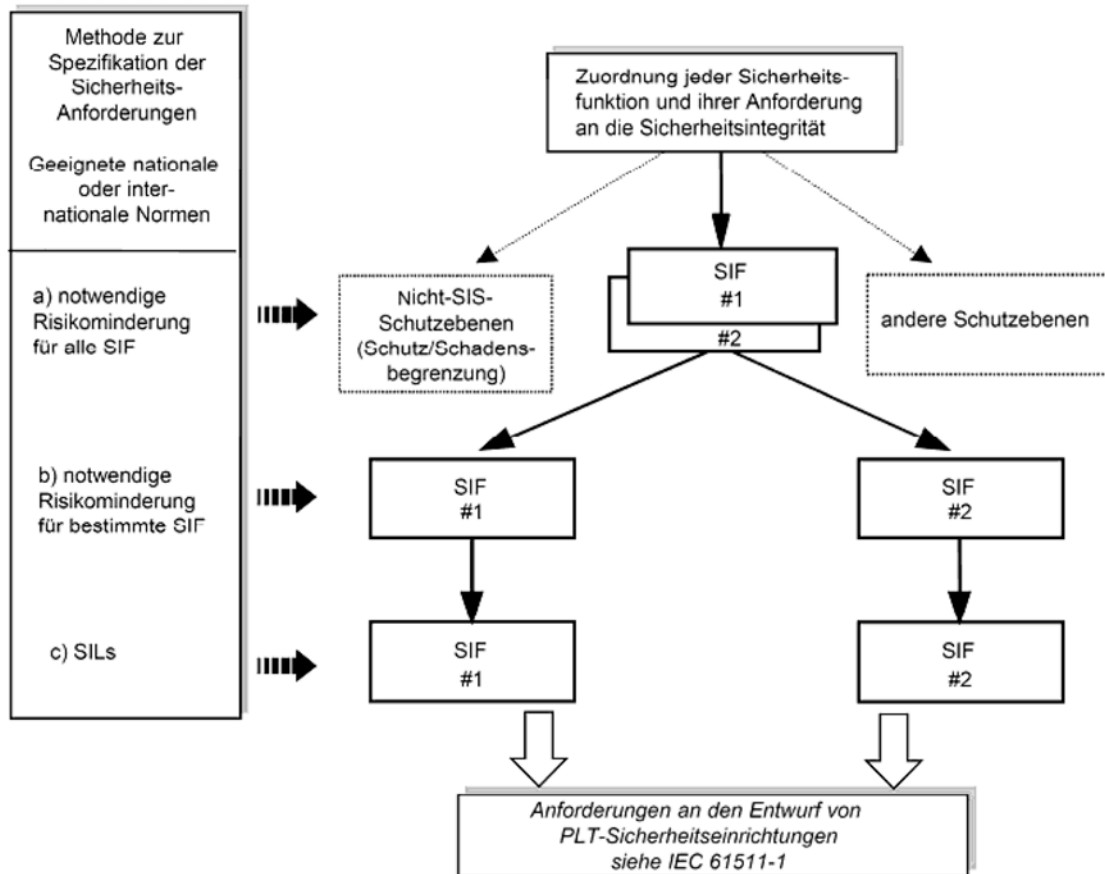
A.8 Auswahl einer Methode zur Bestimmung der erforderlichen Sicherheits-Integritätslevel

Es gibt eine Reihe von Möglichkeiten, den erforderlichen Sicherheits-Integritätslevel für eine bestimmte Anwendung festzulegen. **Anhang B** bis **Anhang I** informieren über eine Reihe von Methoden, die in der Praxis angewendet werden. Welche Methode für eine bestimmte Anwendung ausgewählt wird, hängt von vielen Faktoren ab, beispielsweise:

- der Komplexität der Anwendung;
- Richtlinien von Behörden;
- der Art des Risikos und der notwendigen Risikominderung;
- der Erfahrung und den Fähigkeiten der mit dieser Arbeit betrauten Personen;
- der Kenntnis der für das Risiko relevanten Parameter (siehe **Bild A.4**);
- der Kenntnis über aktuell im Einsatz befindliche PLT-Sicherheitseinrichtungen in den unterschiedlichen Anwendungen, beispielsweise aus Beschreibungen in Industriestandards und Praxisberichten.

In einigen Anwendungen können mehrere Methoden angewendet werden. Eine qualitative Methode kann verwendet werden, um in einem ersten Durchgang den erforderlichen SIL für alle PLT-Sicherheitsfunktionen zu ermitteln. Diejenigen Funktionen, denen mit dieser Methode SIL 3 oder SIL 4 zugeordnet wurde, sollten dann unter Anwendung einer quantitativen Methode näher betrachtet werden, um ein besseres Verständnis für ihre erforderliche Sicherheitsintegrität zu gewinnen.

Es ist entscheidend, dass unabhängig von der (den) für die Anwendung ausgewählten Methode(n) für die Bewertung die Risikokriterien des Standorts zugrunde gelegt werden sollten.



ANMERKUNG Anforderungen bezüglich der Sicherheitsintegrität werden vor der Zuordnung für jede Sicherheitsfunktion definiert (siehe IEC 61511-1:2016, Abschnitt 9).

Bild A.4 – Zuordnung der Sicherheitsanforderungen zu Nicht-SIS-Schutzebenen und anderen Schutzebenen

Anhang B (informativ)

Teilquantitative Methode – Ereignisbaumanalyse

B.1 Überblick

Anhang B erläutert, wie sich die Sicherheits-Integritätslevel über einen teilquantitativen Ansatz festlegen lassen. Ein teilquantitativer Ansatz nutzt sowohl qualitative als auch quantitative Methoden und ist dann besonders nützlich, wenn das tolerierbare Risiko als numerischer Wert angegeben werden soll (z. B. dass eine bestimmte Auswirkung nicht häufiger als einmal in 100 Jahren eintreten soll).

Anhang B ist nicht als endgültige Beschreibung der Methode, sondern als Erläuterung der allgemeinen Grundsätze vorgesehen. Er beruht auf einer Methode, die detailliert in der folgenden Literatur beschrieben ist:

CCPS/AIChE, *Guidelines for Hazard Evaluation Procedures*, Third Edition, Wiley-Interscience, New York (2008) [3].

B.2 Übereinstimmung mit IEC 61511-1:2016

Das wesentliche Ziel von Anhang B besteht darin, ein Vorgehen zu beschreiben, um die benötigten PLT-Sicherheitsfunktionen (SIF) zu ermitteln und ihre SIL-Werte zu bestimmen. Um diesen Anforderungen zu genügen, sind folgende grundlegende Schritte notwendig:

- a) Festlegung des Zielwerts für die Prozesssicherheit (tolerierbares Risiko);
- b) Ermittlung des bestehenden Risikos für jedes einzelne gefährliche Ereignis anhand einer Gefährdungs- und Risikoanalyse;
- c) Ermittlung der erforderlichen Sicherheitsfunktion(en) für jedes einzelne gefährliche Ereignis;
- d) Zuordnung der Sicherheitsfunktion(en) zu Schutzebenen;

ANMERKUNG Es wird davon ausgegangen, dass Schutzebenen unabhängig voneinander sind. Der Zuordnungsprozess kann sicherstellen, dass Ausfälle infolge gemeinsamer Ursache, Ausfälle infolge gemeinsamer Ausfallart und systematische Ausfälle verglichen mit den Gesamtanforderungen an die Risikominderung ausreichend gering sind.

- e) Prüfung, ob eine PLT-Sicherheitsfunktion (SIF) notwendig ist;
- f) Festlegung des erforderlichen SIL der SIF.

In Schritt a) wird der Zielwert für die Prozesssicherheit festgelegt. Schritt b) befasst sich mit der Risikoanalyse des Prozesses und Schritt c) mit der Festlegung der sich aus der Risikoanalyse ergebenden erforderlichen Sicherheitsfunktionen einschließlich ihrer für das Erreichen des Zielwerts für die Prozesssicherheit erforderlichen Risikominderung. Nachdem diesen Sicherheitsfunktionen in Schritt d) Schutzebenen zugeordnet worden sind, wird deutlich, ob eine PLT-Sicherheitsfunktion erforderlich ist (Schritt e)) und welches SIL diese erfüllen muss (Schritt f)).

Anhang B schlägt eine teilquantitative Methode zur Risikobewertung vor, um die Ziele der IEC 61511-1:2016, **Abschnitt 8** zu erreichen. Das Vorgehen wird an einem einfachen Beispiel veranschaulicht.

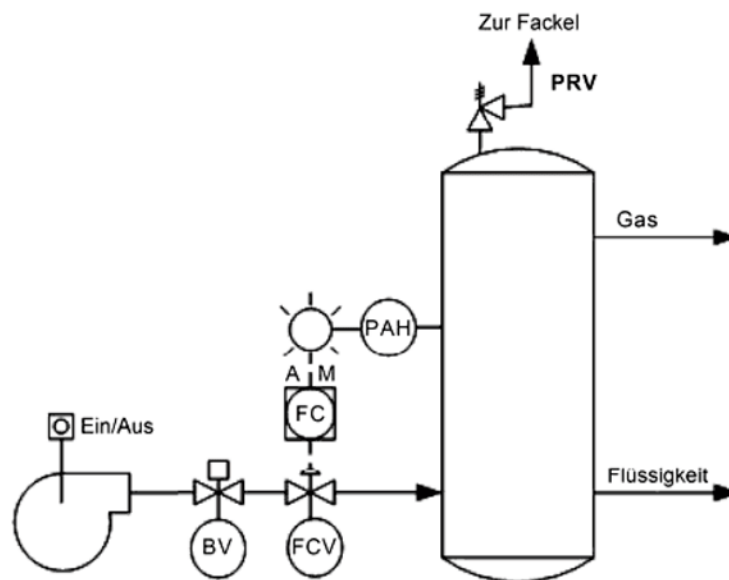
B.3 Beispiel

B.3.1 Allgemeines

Es wird ein Prozess mit einem Druckbehälter mit einem Pumpenzulauf und zwei Abläufen (flüssig und gasförmig) betrachtet, der eine Mischung aus Gas und einer flüchtigen brennbaren Flüssigkeit und die

dazugehörige Prozessleittechnik umfasst (siehe Bild B.1). Der Prozess wird durch eine PLT-Betriebs-einrichtung gesteuert, die das Signal des Durchflussgebers erfasst und das Ventil regelt. Es stehen zwei technische Einrichtungen zur Verfügung: a) ein unabhängiger Druckmessumformer, der bei Hochdruck einen Alarm auslöst und damit den Bediener veranlasst, durch geeignete Maßnahmen den Zulauf zu unterbrechen, und b) im Falle, dass der Bediener nicht reagiert, eine Nicht-PLT-Schutzebene in Form eines Druckentlastungsventils gegen die durch den Druckanstieg im Druckbehälter ausgelösten Gefährdungen. Die vom Druckentlastungsventil freigesetzten Stoffe werden in einen Entspannungsbehälter geleitet, der die Gase an eine Fackel abgibt. Im Beispiel wird angenommen, dass es sich bei der Fackel um eine zugelassene Einrichtung handelt, die ordnungsgemäß geplant, gebaut und betrieben wird; deshalb werden mögliche Ausfälle des Fackelsystems in diesem Beispiel nicht berücksichtigt.

ANMERKUNG Als technische Einrichtungen werden all jene Systeme bezeichnet, die auf eine Anforderung vom Prozess antworten können, einschließlich anderer Sicherheitseinrichtungen der Prozessleittechnik und zugehöriger Bedienertätigkeiten.



Legende

- FC Durchflussregler
- FCV Durchflussregelventil
- PAH Hochdruckalarm
- BV Absperrventil
- PRV Druckentlastungsventil

Bild B.1 – Druckbehälter mit vorhandenen Sicherheitseinrichtungen

B.3.2 Zielwert für die Prozesssicherheit

Eine grundlegende Voraussetzung für die erfolgreiche Beherrschung industrieller Risiken ist die knappe und klare Festlegung eines gewünschten Zielwerts für die Prozesssicherheit (oder ein tolerierbares Risiko). Diese Festlegung kann unter Beachtung nationaler und Internationaler Normen und Vorschriften, unternehmenseigener Sicherheitsrichtlinien und von Vorgaben anderer beteiligter Stellen – wie beispielsweise der Öffentlichkeit, der örtlichen Rechtsprechung und von Versicherungsgesellschaften – unterstützt durch anerkannte Regeln der Technik erfolgen. Der Zielwert für die Prozesssicherheit wird für einen Prozess, ein Unternehmen oder einen Industriezweig festgelegt. Er sollte nicht verallgemeinert werden, solange dies nicht in gesetzlichen Regelungen oder Normen geschieht. Für das Anschauungsbeispiel wird angenommen, dass als Zielwert für die Prozesssicherheit die mittlere Eintrittshäufigkeit für eine Entspannung aus dem Druckbehälter in die Atmosphäre von weniger als 10^{-4} je Jahr festgelegt worden ist.

B.3.3 Gefährdungsanalyse

Es sollte eine Gefährdungsanalyse durchgeführt werden, um Gefährdungen, mögliche Abweichungen im Prozessablauf und deren Ursachen, verfügbare technische Einrichtungen, auslösende Ereignisse und mögliche gefährliche Ereignisse (Unfälle) zu ermitteln. Dazu dienen verschiedene qualitative Methoden:

- Sicherheits-Prüfungen;
- Checklisten;
- Was-wäre-wenn-Analysen;
- HAZOP-Studien;
- Fehlermöglichkeits- und Einflussanalyse (FMEA) (en: failure mode and effects analysis);
- Ursache-Wirkungs-Analyse.

Eine weitverbreitete Methode ist die HAZOP-Analyse (en: Hazard and Operability analysis). Die HAZOP-Analyse (oder -Studie) ermittelt und bewertet Gefahrenquellen in einer Anlage, aber auch Probleme mit der Bedienbarkeit, welche die geplante Produktivität der Anlage in Frage stellen.

Als zweiter Schritt wird eine HAZOP-Analyse für das in [Bild B.1](#) gezeigte Anschauungsbeispiel durchgeführt. In der Analyse werden diejenigen gefährlichen Ereignisse bewertet, die zu einer Freisetzung von Stoffen in die Umwelt führen können. In Tabelle B.1 wird zur Veranschaulichung der HAZOP-Ergebnisse eine gekürzte Liste aufgezeigt.

Als Ergebnis der HAZOP-Studie wurde erkannt, dass ein Überdruck im Behälter zu einer Freisetzung des brennbaren Stoffs in die Umgebung führen kann. Dies ist ein möglicher Auslöser für ein gefährliches Ereignis, je nachdem, wie die verfügbaren technischen Einrichtungen darauf ansprechen. Wenn eine vollständige HAZOP-Analyse für dieses Verfahren durchgeführt worden wäre, hätten sich auch weitere auslösende Ereignisse gefunden, die zu einer unerwünschten Freisetzung führen können, als da sind: Leckage an Geräten, Bruch von Rohrleitungen und äußere Einwirkungen, beispielsweise ein Brand. Für dieses Anschauungsbeispiel wird die Überdruckbedingung im Behälter untersucht.

Tabelle B.1 – Ergebnisse der HAZOP-Analyse

Gegenstand	Abweichungen	Ursachen	Auswirkungen	Sicherheits-einrichtungen	Maßnahmen
Behälter	hoher Durchfluss	Versagen der Durchflussregelung	Hoher Durchfluss führt zu Druckanstieg (siehe B.3.3 Anmerkung).		
	hoher Druck	1) Versagen der Durchflussregelung 2) Brand in der Umgebung	Zerstörung des Behälters und Freisetzung in die Umgebung	1) Hochdruckalarm 2) Flutungssystem 3) Druckentlastungs-ventil	Bewertung der Entwurfsbedingungen für die Freisetzung über des Druckentlastungsventil in die Umgebung
	niedriger/kein Durchfluss	Versagen der Durchflussregelung	keine maßgeblichen Folgen		
	Rückströmung		keine maßgeblichen Folgen		

ANMERKUNG In diesem Beispiel wird angenommen, dass im Behälter Überdruck entstehen kann, da die nachfolgenden Einrichtungen nicht in der Lage sind, den vollen Gasdurchfluss aus dem Behälter aufzunehmen, wenn dessen Zulauf zu hoch ist.

B.3.4 Teilquantitative Methode der Risikoanalyse

Ein Schätzwert für das Prozessrisiko wird anhand einer teilquantitativen Risikoanalyse ermittelt, welche die mit möglichen Unfällen oder gefährlichen Ereignissen im Prozess verbundenen Risiken benennt und quantifiziert. Die Ergebnisse können zur Festlegung von erforderlichen Sicherheitsfunktionen und deren zugehörigen SIL-Werten herangezogen werden, um so das Prozessrisiko auf ein vertretbares Maß zu verringern. Die Ermittlung des Prozessrisikos mit einer teilquantitativen Methode kann in folgende Hauptschritte unterteilt werden. Die ersten vier dieser Schritte können während der HAZOP-Studie durchgeführt werden.

- a) Ermittlung der Gefährdungen im Prozess;
- b) Ermittlung auslösender Ereignisse;
- c) Entwicklung von Szenarien für gefährliche Ereignisse für jedes auslösende Ereignis;
- d) Ermittlung der Zusammensetzung der Schutzebenen;

ANMERKUNG 1 Zum Schutz eines Prozesses werden Sicherheitsfunktionen den Schutzebenen zugeordnet, die PLT-Sicherheitseinrichtungen und andere Maßnahmen zur Risikominderung umfassen (siehe Bild B.2).

ANMERKUNG 2 Dieser Schritt gilt für das obige Beispiel, da es sich um einen vorhandenen Prozess mit bestehenden Schutzebenen handelt.

- e) Ermittlung der Eintrittshäufigkeit der auslösenden Ereignisse und der Zuverlässigkeit vorhandener Sicherheitseinrichtungen aufgrund von Erfahrungswerten oder Modellberechnungen (z. B. Ereignisbaumanalyse, Fehlermöglichkeits- und Einflussanalyse (FMEA) oder Fehlerbaumanalyse);
- f) Quantifizierung der Eintrittshäufigkeit für die bedeutenden gefährlichen Ereignisse;
- g) Bewertung der Auswirkungen aller bedeutenden gefährlichen Ereignisse;
- h) Zusammenfassung der Ergebnisse (Auswirkungen und Häufigkeit eines Unfalls) zum Risiko, das mit jedem gefährlichen Ereignis verbunden ist.

Zu den wesentlichen Ergebnissen von Interesse zählen folgende Punkte:

- ein besseres und gründlicheres Verständnis der mit dem Prozess verbundenen Gefährdungen und Risiken;
- Kenntnis des Prozessrisikos;
- der Beitrag bestehender Sicherheitsfunktionen zur gesamten Risikominderung;
- die Ermittlung aller Sicherheitsfunktionen, die notwendig sind, um das Prozessrisiko auf ein vertretbares Maß zu mindern;
- ein Vergleich des abgeschätzten Prozessrisikos mit dem Zielrisiko.

Die teilquantitative Methode ist aufwändig, aber weist auch Vorteile auf, die in den qualitativen Ansätzen nicht vorhanden sind. Die Methode hängt sehr stark vom Sachverstand ab, den das Team für die Ermittlung der Gefährdungen mitbringt; sie bietet eine Methode zur Handhabung von bestehenden Sicherheitseinrichtungen anderer Technologie; sie verwendet einen formalen Rahmen zur Dokumentation aller Tätigkeiten, die letztlich zu den Ergebnissen geführt haben, und sie stellt ein System für das Management im Lebenszyklus bereit.

Für das Anschauungsbeispiel wurde durch die HAZOP-Studie ein gefährliches Ereignis – Überdruck – ermittelt, welches möglicherweise zu einer Freisetzung von Stoffen in die Umwelt führen könnte. Es ist anzumerken, dass der in B.3.4 gewählte Ansatz eine Kombination aus der quantitativen Bestimmung der Häufigkeit eines gefährlichen Ereignisses und einer qualitativen Bewertung seiner Auswirkungen darstellt. Dieser Ansatz veranschaulicht das systematische Vorgehen, das zur Ermittlung gefährlicher Vorfälle und PLT-Sicherheitsfunktionen befolgt werden sollte.

B.3.5 Risikoanalyse eines bestehenden Prozesses

Der nächste Schritt besteht darin, diejenigen Faktoren zu ermitteln, die zur Entwicklung eines auslösenden Ereignisses beitragen können. Hierzu zeigt Bild B.2 einen einfachen Fehlerbaum mit einigen Ereignissen, die zu einem Überdruck im Behälter beitragen können. Das Hauptereignis, der Überdruck im Behälter, wird

verursacht durch einen Ausfall einer PLT-Betriebseinrichtung (z. B. Durchflussregelung) oder durch einen Brand in der Umgebung (siehe [Tabelle B.1](#)).

Mit der Aufstellung des Fehlerbaums werden die Auswirkungen eines Ausfalls der PLT-Betriebseinrichtung auf den Prozess verdeutlicht, und die Häufigkeit eines Brandes in der Umgebung erweist sich im Vergleich dazu als vernachlässigbar. Die PLT-Betriebseinrichtung führt keinerlei Sicherheitsfunktionen aus. Ihr Ausfall führt jedoch zu einer höheren Anforderungsrate an die PLT-Sicherheitseinrichtung. Eine zuverlässige PLT-Betriebseinrichtung würde daher weniger oft Anforderungen an die PLT-Sicherheitseinrichtung verursachen.

Der Fehlerbaum lässt sich quantifizieren, und für dieses Beispiel wird eine Eintrittshäufigkeit für die Überdruckbedingung in der Größenordnung von 10^{-1} je Jahr angenommen. Es ist zu beachten, dass davon ausgegangen wird, dass jede in Bild B.2 dargestellte Ursache unabhängig von anderen Ursachen ist (d. h. keine Überschneidung) und die Ausfallrate in Ereignissen je Jahr angegeben wird.

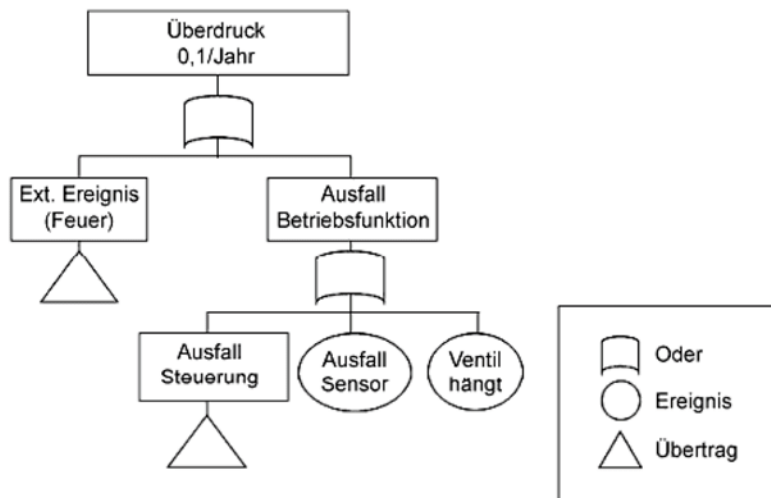


Bild B.2 – Fehlerbaum für Überdruck im Behälter

ANMERKUNG 1 Der Fehlerbaum in Bild B.2 beinhaltet keine Schutzmaßnahmen.

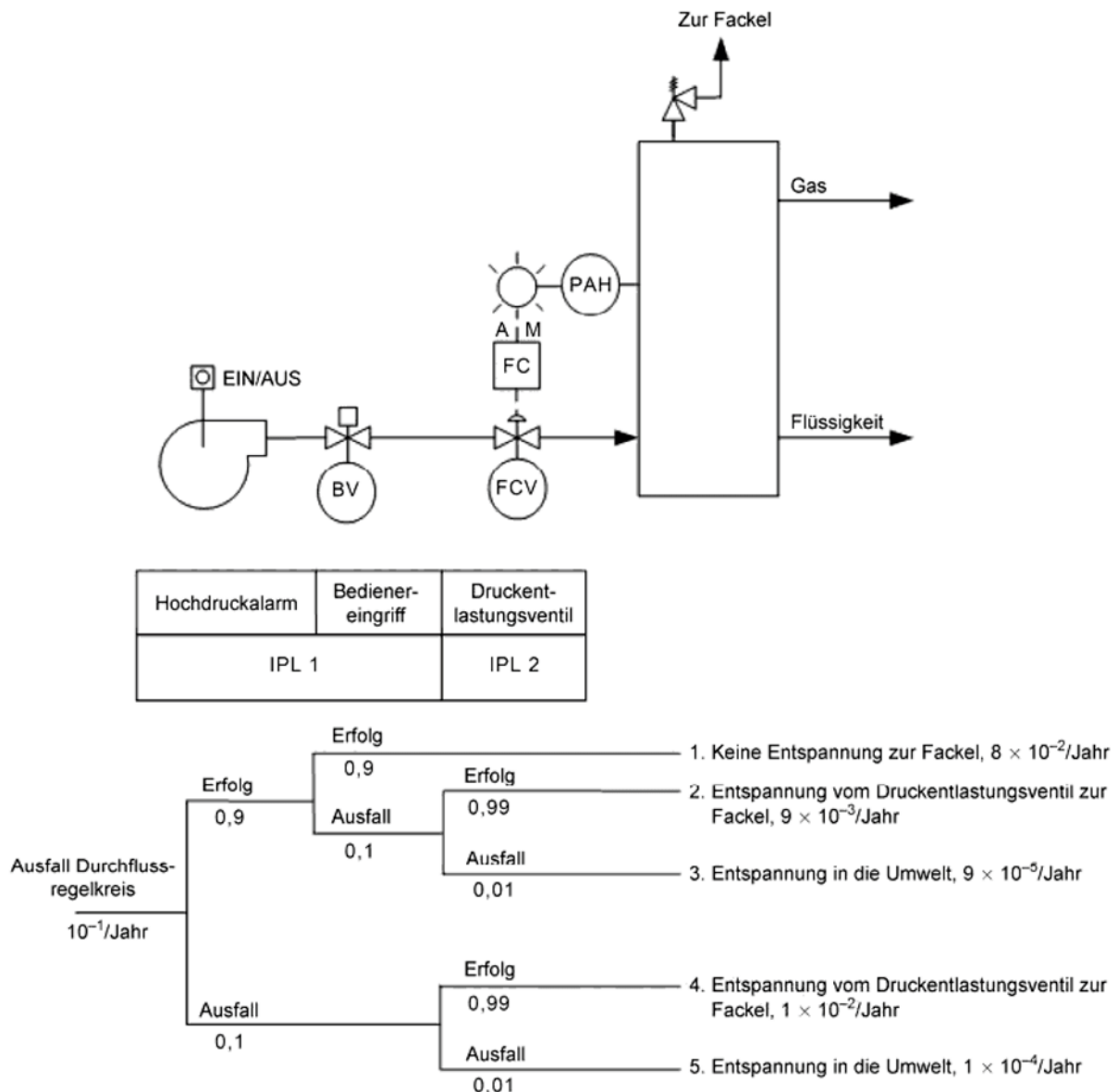
Sobald die Eintrittshäufigkeit des auslösenden Ereignisses festliegt, wird die erfolgreiche oder nicht erfolgreiche Reaktion der Sicherheitseinrichtungen auf die Abweichung vom Normalbetrieb in Form eines Ereignisbaums dargestellt. Zuverlässigkeitsdaten für die Leistungsfähigkeit der Sicherheitseinrichtungen können gesammelten Felddaten, veröffentlichten Datensammlungen oder modellgestützten Vorhersagen zur Zuverlässigkeit entnommen werden.

Für dieses Beispiel wurden die Zuverlässigkeitsdaten geschätzt und beziehen sich nicht auf veröffentlichte oder vorhergesagte Werte für die Systemleistung. [Bild B.3](#) zeigt mögliche Ergebnisszenarien, die sich im Anschluss an einen Überdruck im Behälter abspielen könnten. Als Ergebnisse aus dieser Ereignismodellierung ergeben sich a) die Eintrittshäufigkeit für jede Ereignisfolge und b) die qualitativen Auswirkungen im Hinblick auf die Folgen des Ereignisses.

In [Bild B.3](#) werden fünf solcher Ergebnisszenarien aufgeführt, jedes mit Angabe der Eintrittshäufigkeit und einer qualitativen Folge. Ergebnisszenario 1 mit Bedienereingriff nach einem Hochdruckalarm tritt mit einer Häufigkeit von 8×10^{-2} je Jahr ein und führt zu einer Drosselung der Fertigung ohne Freisetzung. Das ist eine annehmbare Entwurfsbedingung für den Prozess und der Bediener wird auf eine angemessene Reaktion zum Erzielen der Risikominderung hin geschult und überprüft.

Weiterhin treten die Ergebnisszenarien 2 und 4 mit einer Freisetzung von Stoffen zur Fackel mit einer kombinierten Häufigkeit von $1,9 \times 10^{-2}$ je Jahr ($9 \times 10^{-3} + 1 \times 10^{-2}$) ein und werden ebenfalls als eine Entwurfsbedingung für den Prozess berücksichtigt. Die verbleibenden Ergebnisszenarien 3 und 5 weisen eine kombinierte Eintrittshäufigkeit von $1,9 \times 10^{-4}$ je Jahr ($9 \times 10^{-5} + 1 \times 10^{-4}$) auf und führen zu einer Zerstörung des Behälters und einer Freisetzung von Stoffen in die Umwelt (siehe Anmerkung 2).

Es sollte angemerkt werden, dass diese Analyse nicht die Möglichkeit von Ausfällen infolge gemeinsamer Ursache des Hochdruckalarms und des BPCS-Durchflusssensors berücksichtigt. Solche Ausfälle infolge gemeinsamer Ursache können zu einem signifikanten Anstieg der Eintrittshäufigkeit für das Ergebnisszenario 3 führen und so das Gesamtrisiko erhöhen.



ANMERKUNG Ergebnisse auf die erste Stelle gerundet.

Bild B.3 – Gefährliche Vorfälle bei vorhandenen Sicherheitseinrichtungen

ANMERKUNG 2 In einigen Anwendungen können die Häufigkeit und die Wahrscheinlichkeit eines Ausfalls bei Anforderung nicht multipliziert werden, wie in Bild B.3 dargestellt. Der Grund dafür sind Überschneidungen, Ausfälle infolge gemeinsamer Ursache und die umfassenden Abhängigkeiten zwischen den verschiedenen Schutzebenen. Siehe [Anhang J](#).

ANMERKUNG 3 In Bild B.3 wird vorausgesetzt, dass die Ereignisse voneinander unabhängig sind. Da außerdem die Häufigkeitswerte nur geschätzt sind, nähert sich die Summe der Eintrittshäufigkeiten über alle Fälle derjenigen für das auslösende Ereignis (0,1 je Jahr).

B.3.6 Ereignisse, die den Zielwert für die Prozesssicherheit nicht erfüllen

Wie bereits festgestellt wurde, legen anlagenspezifische Richtlinien den Zielwert für die Prozesssicherheit wie folgt fest: keine Freisetzung von Stoffen in die Umwelt mit einer Eintrittshäufigkeit von mehr als 10^{-4} in einem Jahr. Die gesamte Häufigkeit von Freisetzungen in die Umgebung beträgt 9×10^{-5} (Ergebnisszenario 3) + $1,0 \times 10^{-4}$ (Szenario 5) = $1,9 \times 10^{-4}$ je Jahr, was größer ist als der Zielwert für die Prozesssicherheit. Aufgrund der Daten der Eintrittshäufigkeit der gefährlichen Vorfälle und deren Auswirkungen aus Bild B.3 ist eine weitere Risikominderung notwendig, um die Ergebnisszenarien 3 und 5 unter den Zielwert für die Prozesssicherheit zu bringen.

B.3.7 Risikominderung mit Hilfe anderer Schutzebenen

Zunächst sollten Schutzebenen anderer Technologien berücksichtigt werden, bevor auf PLT-Sicherheitsfunktionen in einer PLT-Sicherheitseinrichtung zurückgegriffen wird. In Tabelle B.1 ist ein Flutungssystem als Sicherheitssystem aufgeführt, welches aber die Zerstörung des Behälters oder eine Freisetzung in die Umwelt nicht verhindert.

Da der Zweck der Analyse die Minderung des Risikos einer Freisetzung von Stoffen in die Umwelt ist, kann davon ausgegangen werden, dass das Flutungssystem keine annehmbare Maßnahme zur Verringerung des Risikos einer Zerstörung des Behälters oder einer Freisetzung in die Umwelt darstellt. Das Flutungssystem mindert das Risiko für das Personal und für die Eskalation des Ereignisses, das in diesem Beispiel nicht bewertet wird.

B.3.8 Risikominderung durch eine PLT-Sicherheitsfunktion

Der Zielwert für die Prozesssicherheit kann nicht mit Schutzebenen anderer Technologien erreicht werden. Um die Gesamthäufigkeit von Freisetzungen in die Atmosphäre zu reduzieren, ist eine neue PLT-Sicherheitsfunktion mit SIL 2 erforderlich, um den Zielwert für die Prozesssicherheit zu erfüllen. Die neue PLT-Sicherheitsfunktion ist in Bild B.4 dargestellt.

An dieser Stelle ist ein Entwurf der SIF im Einzelnen nicht notwendig. Ein Grundkonzept des SIF-Entwurfs ist ausreichend. In diesem Schritt wird überprüft, ob mit einer neuen SIF mit SIL 2 die erforderliche Risikominderung und der Zielwert für die Prozesssicherheit erreicht werden. Der genaue Entwurf der SIF erfolgt dann, nachdem der Zielwert für die Prozesssicherheit für die SIF festgelegt worden ist. In diesem Beispiel nutzt die neue SIF zwei für Sicherheitsaufgaben vorgesehene Drucksensoren in einer 1oo2-Anordnung (in Bild B.4 nicht dargestellt), die Signale an ein Logiksystem senden. Der Ausgang des Logiksystems regelt das Absperrventil und die Pumpe.

ANMERKUNG 1oo2 bedeutet, dass jeweils einer der Drucksensoren die Abschaltung des Prozesses auslösen kann.

Mit der neuen SIF mit SIL 2 wird die Häufigkeit von Freisetzungen aufgrund von Überdruck im Druckbehälter verringert. Bild B.4 zeigt die neue Schutzebene und alle möglichen Unfallszenarien. Wie dieses Bild zeigt, kann die Häufigkeit einer Freisetzung aus diesem Behälter auf 10^{-4} je Jahr oder weniger verringert werden, und der Zielwert für die Prozesssicherheit kann erreicht werden, sofern nachgewiesen werden kann, dass die PLT-Sicherheitsfunktion die Anforderungen für SIL 2 einhält.

In Bild B.4 sind sieben Ergebnisszenarien jeweils mit einer Eintrittshäufigkeit und einer qualitativen Aussage zur Auswirkung angegeben. Die Häufigkeit von Ergebnisszenario 1 wurde bereits erläutert. Der Bedienergriff führt zu einer gedrosselten Fertigung mit einer Häufigkeit von 8×10^{-2} pro Jahr.

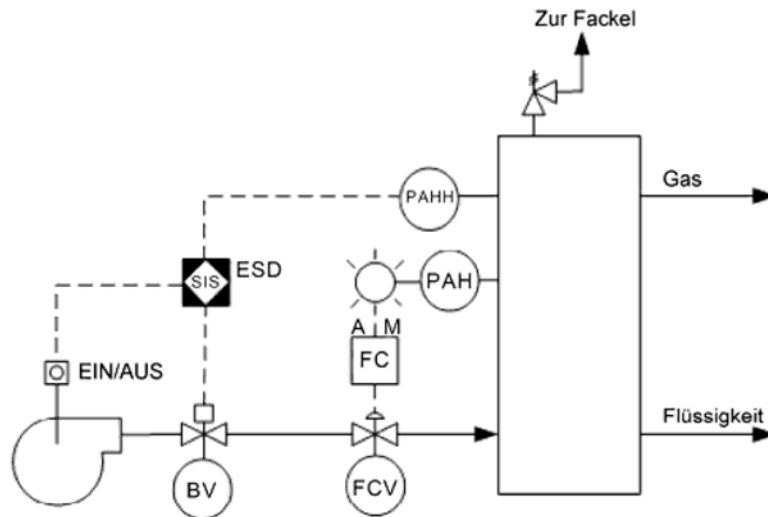
In diesem Entwurfsfall führt ein erfolgreiches Ansprechen der PLT-Sicherheitseinrichtung zu einer Abschaltung des Prozesses, dies tritt mit einer Häufigkeit von $1,9 \times 10^{-2}$ je Jahr ein. Die PLT-Sicherheitseinrichtung verringert die Prozessanforderungsrate an das Druckentlastungsventil. Die Häufigkeit des Ergebnisszenarios 3 mit einer Freisetzung aus dem Druckentlastungsventil an die Fackel wird um zwei Größenordnungen gegenüber dem vorangehenden Fall auf 9×10^{-5} je Jahr herabgesetzt. Ergebnisszenario 4, der gefährliche Vorfall mit einer Freisetzung von Stoffen in die Umgebung, weist eine Eintrittshäufigkeit von 9×10^{-7} je Jahr auf.

Ereignisszenario 5 führt infolge der Abschaltung des Prozesses durch die PLT-Sicherheitseinrichtung nicht zu einer Freisetzung und tritt mit einer Häufigkeit von 1×10^{-2} je Jahr ein. Wenn die PLT-Sicherheitseinrichtung versagt, stellt das Druckentlastungsventil die nächste Sicherheitsfunktion zur Verfügung, wie im Ereignisszenario 6 dargestellt, und öffnet zur Fackel. Die Öffnung des Druckentlastungsventils tritt mit einer Häufigkeit von 1×10^{-4} je Jahr ein. Die Gesamthäufigkeit von Freisetzungen zur Fackel wird durch die Szenarien 3 und 6 bestimmt, die mit einer Gesamthäufigkeit von $9 \times 10^{-5} + 1 \times 10^{-4}$ bzw. $1,9 \times 10^{-4}$ auftreten. Freisetzungen zur Fackel sind eine zulässige Entwurfsbedingung für den Prozess. Ereignisszenario 7 behandelt den Ausfall aller Sicherheitsfunktionen und tritt mit 1×10^{-6} je Jahr ein.

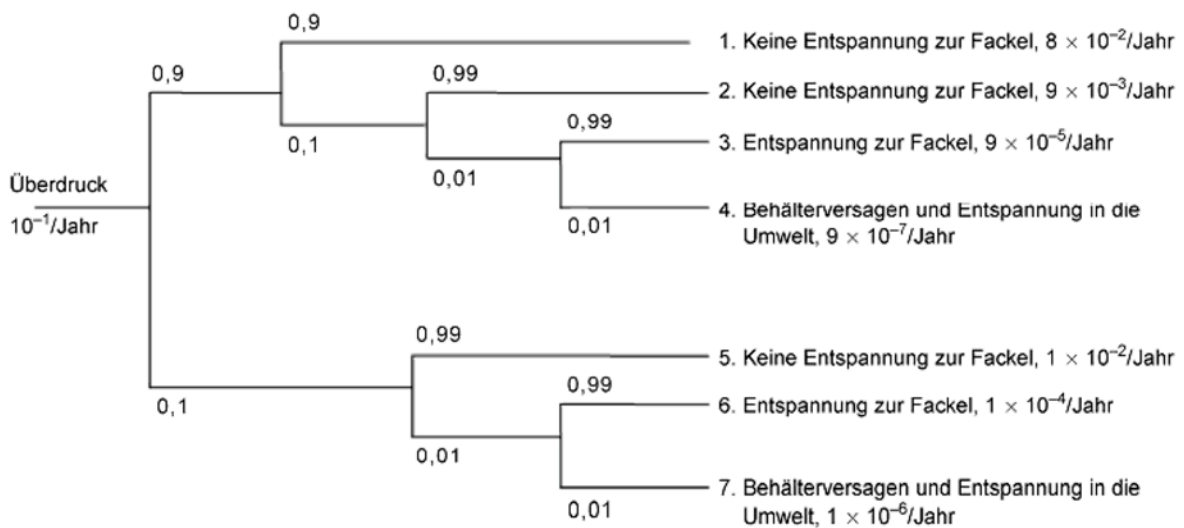
Die Gesamthäufigkeit für ein Behälterversagen mit Freisetzungen in die Umgebung (Summe der Häufigkeiten der Szenarien 4 und 7) hat sich auf $1,9 \times 10^{-6}$ je Jahr verringert und liegt damit unter dem Zielwert für die Prozesssicherheit von 10^{-4} je Jahr.

Es sollte angemerkt werden, dass diese Ereignisbaumanalyse nicht die Möglichkeit von Ausfällen infolge gemeinsamer Ursache und der umfassenden Abhängigkeiten zwischen dem Hochdruckalarm und der SIF mit SIL 2 berücksichtigt. Es kann außerdem die Möglichkeit eines Ausfalls infolge gemeinsamer Ursache und der umfassenden Abhängigkeiten zwischen den Sicherheitsfunktionen und dem Ausfall des Durchflusssensors einer PLT-Betriebseinrichtung bestehen.

Solche Ausfälle infolge gemeinsamer Ursache können zu einem signifikanten Anstieg der Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktionen bei Anforderung führen und so das Gesamtrisiko erheblich erhöhen.



Hochdruckalarm	Bediener-eingriff	Sicherheitseinrichtung SIL 2	Druckentlastungsventil
IPL 1		IPL 2	IPL 3



ANMERKUNG Ergebnisse auf die erste Stelle gerundet.

Bild B.4 – Gefährliche Vorfälle mit einer SIL2-PLT-Sicherheitsfunktion