

DIN EN 746-11

ICS 25.180.01

Einsprüche bis 2020-03-31

Entwurf

**Industrielle Thermoprozessanlagen und dazugehörige
Prozesskomponenten –
Sicherheitsanforderungen –
Teil 11: Schutzsysteme;
Deutsche und Englische Fassung prEN 746-11:2020**

Industrial furnaces and associated processing equipment –
Safety –

Part 11: Protective systems;
German and English version prEN 746-11:2020

Fours industriels et équipements associés –
Sécurité –

Partie 11: Systèmes de protection;
Version allemande et anglaise prEN 746-11:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2020-01-31 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nam@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Maschinenbau (NAM), 60498 Frankfurt am Main, Postfach 71 08 64, Lyoner Str. 18, 60528 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 158 Seiten

DIN-Normenausschuss Maschinenbau (NAM)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

Die nationalen Interessen bei der Erarbeitung werden vom Arbeitsausschuss NA 060-03-04 AA „Schutzsysteme“ im Fachbereich „Thermoprozesstechnik“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von Thermoprozessanlagen sowie der Berufsgenossenschaften sind an der Erarbeitung beteiligt.

Dieser Norm-Entwurf konkretisiert einschlägige Anforderungen von Anhang I der EU-Maschinenrichtlinie 2006/42/EG an erstmals im Europäischen Wirtschaftsraum (EWR) in Verkehr gebrachte Maschinen, um den Nachweis der Übereinstimmung mit diesen Anforderungen zu erleichtern.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

**Industrielle Thermoprozessanlagen und dazugehörige
Prozesskomponenten — Sicherheitsanforderungen — Teil 11:
Schutzsysteme; Deutsche und Englische Fassung prEN 746-11:2020**

Fours industriels et équipements associés — Sécurité — Partie 11 : Systèmes de protection; Version allemande et anglaise prEN 746-11:2020

Industrial furnaces and associated processing equipment — Safety — Part 11: Protective systems; German and English version prEN 746-11:2020

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Inhalt

	Seite
Europäisches Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Anforderungen an die Gestaltung von Anlageteilen in einem Schutzsystem	10
4.1 Allgemeines	10
4.2 Anforderungen an Schutzsysteme	11
4.2.1 Allgemeines	11
4.2.2 Verfahren A	14
4.2.3 Verfahren B	15
4.2.4 Verfahren C	16
4.2.5 Verfahren D	20
4.3 Fehlerbetrachtung für den festverdrahteten Teil von Schutzsystemen	21
4.4 Ausfall von Versorgungseinrichtungen	21
4.5 Rücksetzen/Entriegelung	22
Anhang A (informativ) Erläuterung der Techniken und Maßnahmen zur Vermeidung systematischer Fehler	23
A.1 Allgemeines	23
A.2 Kompetenzen	23
A.3 Vermeidung systematischer Fehler	24
Anhang B (informativ) Beispiele für Techniken zur Vermeidung von Fehlern durch die externe Verkabelung	25
Anhang C (informativ) Beispiele für die Bestimmung des Sicherheits-Integritätslevels (SIL) mittels des Risikograph-Verfahrens	29
C.1 Allgemeines	29
C.2 Beispiele für die Bestimmung des erforderlichen SIL/PL	30
C.2.1 Beispiel 1 – Tabelle C.1	30
C.2.2 Beispiel 2 – Tabelle C.2	30
C.2.3 Risikoeinschätzung und SIL-Zuweisung in Übereinstimmung mit Anhang A von EN 62061:2005 (d. h. Tabelle C.1)	40
C.2.4 Benutzer-Richtlinie für den Risikograph in Übereinstimmung mit EN61511-3:2017 (d. h. Tabelle C.2)	44
Anhang D (informativ) Beispiel für eine erweiterte Risikobeurteilung für eine sicherheitstechnische Funktion mittels des Verfahrens nach EN 61511	50
D.1 Allgemeines	50
D.2 Konzeptbeschreibung der gesteuerten Ausrüstung	50
D.3 Gefährdungs- und Risikobeurteilung	50
D.3.1 Allgemeines	50
D.3.2 Auslösende Ereignisse	51
D.3.3 Gefährdung — Prozessabweichung – unzureichende Verbrennungsluft	51
D.4 Konsequenzen	51
D.5 Beispiel eines Ereignisbaums	51
D.6 Sicherheitsanforderungsspezifikation des Schutzsystems	52

D.6.1	Allgemeine Anforderungen	52
D.6.2	Funktionale Anforderungen an Sicherheitssensoren	54
D.6.3	Anforderungen an das Logiksystem, einschließlich Alarm, externer Vergleich und HMI	55
D.6.4	Anforderungen an den Aktor	56
D.6.5	Anforderungen an manuelle Eingriffe	57
D.6.6	Anforderungen an den Anlauf	57
Anhang E (informativ) Schematische Beispieldiagramme eines Schutzsystems.....		58
Anhang F (normativ) Festverdrahtung für Schutzsysteme.....		68
F.1	Allgemeines	68
F.2	Schutz vor Fehlern des Logiksystems	68
F.3	Maßnahmen zur Vermeidung von Fehlern	69
F.4	Hardwareauslegung	69
F.4.1	Allgemeine Anforderungen an die Hardware	69
F.4.2	Festverdrahteter Teil eines Schutzsystems.....	69
Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und den grundlegenden Anforderungen der abzudeckenden Richtlinie 2006/42/EG		79
Literaturhinweise.....		80

Europäisches Vorwort

Dieses Dokument (prEN 746-11:2020) wurde vom Technischen Komitee CEN/TC 186 „Industrielle Thermoprozessanlagen - Sicherheit“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Der Inhalt von prEN 746-11:2020 basiert auf Teilen von EN 746-2:2009 und ISO 13577-4:2016.

Dieses Dokument wurde im Rahmen eines Mandats erarbeitet, das die Europäische Kommission und die Europäische Freihandelszone CEN erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinien.

Zum Zusammenhang mit EU-Richtlinien siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Einleitung

Dieser Teil von EN 746 wurde entwickelt, um Anforderungen an ein Schutzsystem festzulegen, bei dem es sich um eine sicherheitsbezogene elektrische Steuerung (SRECS) einer industriellen Thermoprozessanlage und zugehöriger Einrichtungen (TPE) handelt.

Obligatorische sicherheitsbezogene Steuerungen von TPE werden in EN 746-1, EN 746-2 und EN 746-3 festgelegt.

Es ist vorgesehen, dass die Hersteller von TPE bei der Auslegung der TPE eine Auswahl zwischen den vier Verfahren treffen, die in diesem Teil von EN 746 festgelegt werden.

Dieser Teil von EN 746 soll mit den anderen Teilen von EN 746 und im Rahmen der Grundlagen von EN ISO 12100 verwendet. Allerdings gibt es Fälle, in denen eine Risikobeurteilung nach EN 61511 (alle Teile) für die Auslegung eines TPE-Schutzsystems geeigneter ist.

Dieses Dokument ist eine Typ-C-Norm, wie in EN ISO 12100 angegeben.

Auf die betroffenen Maschinen und das Ausmaß, in dem Gefährdungen, Gefährdungssituationen oder -ereignisse erfasst werden, wird im Anwendungsbereich dieses Teils von EN 746 hingewiesen.

Wenn die Festlegungen in dieser Typ-C-Norm von den Festlegungen in Typ-A- oder Typ-B-Normen abweichen, haben die Festlegungen in dieser Typ-C-Norm bei Maschinen, die nach den Festlegungen dieser Typ-C-Norm gestaltet und gebaut wurden, Vorrang gegenüber den Festlegungen in anderen Normen.

EN 61511 (alle Teile) bietet die Option eines Schutzsystems mit geringer Anforderungsrate. EN 62061:2005 oder EN ISO 13849-1:2015 nehmen stets Anwendungen mit hohen Anforderungen an.

Daher gestattet dieser Teil von EN 746 eine erweiterte Risikobeurteilung für SRECS, in der alternativ eine Risikobeurteilung nach EN 61511 (alle Teile) gewählt werden kann.

1 Anwendungsbereich

Dieser Teil von EN 746 legt die Anforderungen an Schutzsysteme, die in Industrieöfen und zugehörigen Prozessanlagen (TPE) verwendet werden, fest.

Die funktionalen Anforderungen, die für Schutzsysteme gelten, werden in den anderen Teilen der Normenreihe EN 746 festgelegt.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes normativ 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).

prEN ISO 13574:—¹, *Industrieöfen und zugehörige Prozesseinrichtungen — Terminologie*

EN 298:2012, *Feuerungsautomaten für Brenner und Brennstoffgeräte für gasförmige oder flüssige Brennstoffe*

EN ISO 13849-1:2015, *Sicherheit von Maschinen — Sicherheitsbezogene Teile von Steuerungen — Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015)*

EN 14597:2012, *Temperaturregleinrichtungen und Temperaturbegrenzer für wärmeerzeugende Anlagen*

EN IEC 60947-4-1:2019, *Low-voltage switchgear and controlgear — Part 4-1: Contactors and motor-starters - Electromechanical contactors and motor-starters (IEC 60947-4-1:2018)*

EN 60947-5-1:2017, *Niederspannungsschaltgeräte — Teil 5-1: Steuergeräte und Schaltelemente — Elektromechanische Steuergeräte (IEC 60947-5-1:2016)*

EN 60204-1:2018, *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen (IEC 60204-1:2016)*

EN 60730-2-5:2015, *Automatische elektrische Regel- und Steuergeräte — Teil 2-5: Besondere Anforderungen an automatische elektrische Brenner-Steuerungs- und Überwachungssysteme (IEC 60730-2-5:2013)*

EN 61508 (alle Teile), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (IEC 61508)*

EN 61131-3:2013, *Speicherprogrammierbare Steuerungen — Teil 3: Programmiersprachen (IEC 61131-3:2013)*

EN 61511 (alle Teile), *Funktionale Sicherheit — PLT-Sicherheitseinrichtungen für die Prozessindustrie (IEC 61511 (alle Teile))*

EN 62061:2005², *Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener, elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005)*

¹ In Vorbereitung.

² Dieses Dokument ist derzeit von den Änderungen EN 62061:2005/A1:2013 und EN 62061:2005/A2:2015 betroffen.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach prEN ISO 13574 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken zur Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1

Aktor

Teil eines Schutzsystems, der die Eingriffe in den Prozess ausführt, um einen sicheren Zustand zu erreichen oder zu erhalten

Anmerkung 1 zum Begriff: Beispiele sind Ventile, Schalter und Motoren einschließlich ihrer Hilfsaggregate (wie ein Magnetventil und der Antrieb, wenn es bzw. er Teil der Sicherheitsfunktion ist).

[QUELLE: EN 61511-1:2017, 3.2.24, geändert: „einer PLT-Betriebs- oder PLT-Sicherheitseinrichtung“ wurde in der Definition zu „Schutzsystem“ geändert.]

3.2

Flammenwächter

Einrichtung, mit der das Vorhandensein einer Flamme festgestellt und signalisiert wird

Anmerkung 1 zum Begriff: Sie kann aus einem Flammenfühler, einem Verstärker und einem Relais für die Signalübertragung bestehen.

[QUELLE: prEN ISO 13574:—, 2.65, geändert: Der zweite Satz der ursprünglichen Definition wurde in die Anmerkung übertragen.]

3.3

Feuerungsautomat

Schutzsystem, das mindestens aus einem Programmiergerät und allen Elementen eines Flammenwächters besteht

Anmerkung 1 zum Begriff: Die verschiedenen Funktionsteile eines Feuerungsautomaten können in einem oder mehreren Gehäusen angeordnet sein.

[QUELLE: prEN ISO 13574:—, 2.5, geändert: Der zweite Satz der ursprünglichen Definition wurde in die Anmerkung übertragen.]

3.4

Funktionssicherheit

Fähigkeit eines Schutzsystems oder sonstiger Einrichtungen, Risiken zu verringern und Maßnahmen durchzuführen, die für das Erreichen oder Beibehalten eines sicheren Zustands für das Verfahren und die zugehörige Ausrüstung erforderlich sind

[QUELLE: prEN ISO 13574:—, 2.73]

3.5

Logikfunktion

Funktion, die die Umwandlung der Eingangsinformation (bereitgestellt durch eine oder mehrere Eingangsfunktionen oder Sensoren) zur Ausgangsinformation (verwendet durch eine oder mehrere Ausgangsfunktionen oder Aktoren) durchführt

Anmerkung 1 zum Begriff: Logikfunktionen werden vom Logiksystem eines Schutzsystems durchgeführt.

[QUELLE: EN 61511-1:2017, 3.2.39, geändert — in der Beschreibung wurde „Eingangsfunktionen“ zu „Eingangsinformationen und Sensoren“ und „Ausgangsfunktionen“ zu „Ausgangsfunktionen oder Aktoren“ geändert, der zweite Satz der ursprünglichen Beschreibung wurde entfernt und die Anmerkung wurde hinzugefügt.]

3.6

Logiksystem

Teil eines Schutzsystems, der eine oder mehrere Logikfunktionen ausführt

Anmerkung 1 zum Begriff: Beispiele sind elektrische Systeme, elektronische Systeme, programmierbare elektronische Systeme, pneumatische Systeme und hydraulische Systeme. Sensoren und Aktoren sind nicht Teil des Logiksystems.

[QUELLE: EN 61511-1:2017, 03.02.1940, geändert: „eines BPCS oder einer SIS“ wurde in der Definition zu „eines Schutzsystems“ geändert und Anmerkung 1 der ursprünglichen Definition wurde entfernt.]

3.7

manuelle Rücksetzung

Handlung, die nach Abschaltung einer Sicherheitseinrichtung (z. B. Feuerungsautomat) von Hand durch das aufsichtführende Bedienungspersonal durchgeführt wird

[QUELLE: prEN ISO 13574:—, 2.107]

3.8

Performance Level

PL

diskreter Level, der die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen

[QUELLE: EN ISO 13849-1:2015, 3.1.23]

3.9

Produktnorm

Normen für Produkte und Komponenten, die EN 746 (alle Teile) mit Ausnahme dieses von Teil EN 746 aufgeführt sind

[QUELLE: prEN ISO 13574:—, 2.135, geändert: „EN 746-4“ wurde in der Definition zu „diesem Teil von EN 746“ geändert.]

3.10

speicherprogrammierbare Steuerung

SPS

elektronische Einrichtung zur Steuerung der logischen Abfolge der Ereignisse

[QUELLE: prEN ISO 13574:—, 2.125]

3.11

Schutzsystem

instrumentiertes System, das zur Implementierung einer oder mehrerer sicherheitsbezogener Funktion(en) eingesetzt wird und aus einer Kombination von Sensor(en), Logic Solver(n) und Stellgliedern (Bild 2 enthält ein Beispiel)

Anmerkung 1 zum Begriff: Sowohl sicherheitsbezogene Steuer- und/oder Schutzfunktionen können eingeschlossen sein.

[QUELLE: prEN ISO 13574:—, 2.138]

3.12

Sicherheitsbus

Ein Bussystem und/oder Protokoll für digitale Netzwerkkommunikation zwischen Sicherheitskomponenten, um einen sicheren Zustand des Schutzsystems gemäß EN 61508 (alle Teile) oder EN 60730-2-5:2015 zu erreichen oder beizubehalten

[QUELLE: prEN ISO 13574:—, 2.164]

3.13

Sicherheitseinrichtung

Einrichtung, die entweder allein oder als Teil eines Schutzsystems zur Durchführung von Schutzfunktionen verwendet wird

Anmerkung 1 zum Begriff: Beispiele sind Sensoren, Begrenzer, Flammenwächter, Feuerungsautomaten, Logiksysteme, Aktoren und automatische Absperrventile.

3.14

Sicherheits-Integritätslevel

SIL

diskrete Stufe (eine von vier möglichen) zur Spezifizierung der Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe und der Sicherheits-Integritätslevel 1 die niedrigste ist

Anmerkung 1 zum Begriff: Die Ziel-Ausfallmaßnahmen werden in EN 61508-1:2010, Tabellen 2 und 3, festgelegt.

Anmerkung 2 zum Begriff: Ein Sicherheits-Integritätslevel (SIL) ist keine Eigenschaft eines Systems, Teilsystems, Elementes oder einer Einrichtung. Die korrekte Interpretation des Ausdrucks „SIL-*n*-sicherheitsbezogenes System“ (wobei *n* 1, 2, 3 oder 4 ist) ist, dass das System potenziell in der Lage ist, Sicherheitsfunktionen mit einem Sicherheits-Integritätslevel von bis zu *n* zu unterstützen.

[QUELLE: EN ISO 13849-1:2015, 3.1.33]

3.15

Sensor

Einrichtung, die auf Basis einer Prozessvariable ein Signal erzeugt

BEISPIEL Sender, Aufnehmer, Prozessschalter und Positionsschalter

3.16

System für Dauerbetrieb

System, bei dem die Betriebsstellung ohne Unterbrechung für mehr als 24 h vorgesehen ist

[QUELLE: EN 60730-2-5:2015, 2.5.101]

3.17

System für intermittierenden Betrieb

System, bei dem die Betriebsstellung für weniger als 24 h vorgesehen ist

[QUELLE: EN 60730-2-5:2015, 2.5.102]

3.18

systematische Fähigkeit

Gemessenes (auf einer Skala zwischen SC1 und SC4 ausgedrücktes) Vertrauen, dass die systematische Sicherheitsintegrität eines Elementes die Anforderungen des spezifischen Sicherheits-Integritätslevels hinsichtlich der spezifizierten Sicherheitsfunktion des Elementes erfüllt, wenn das Element gemäß den im konformen Sicherheitshandbuch gegebenen Anweisungen verwendet wird

Anmerkung 1 zum Begriff: Die systematische Fähigkeit wird in Bezug auf die Anforderungen zur Vermeidung und Steuerungssystematischer Fehler (siehe EN 61508-2:2010 und EN 61508-3:2010) festgelegt.

Anmerkung 2 zum Begriff: Was unter dem entsprechenden Ausfallmechanismus zu verstehen ist, hängt von der Natur des Elementes ab. Handelt es sich z.B. um ein reines Softwareelement, müssen nur Software-Ausfallmechanismen berücksichtigt werden. Umfasst das Element jedoch Hard- und Software, ist es notwendig, systematische Hard- und Software-Ausfallmechanismen zu beachten.

Anmerkung 3 zum Begriff: Die systematische Fähigkeit SC_N eines Elements hinsichtlich der spezifizierten Sicherheitsfunktion des Elementes bedeutet, dass die systematische Sicherheitsintegrität des SIL_N erfüllt wird, wenn das Element gemäß den im konformen Sicherheitshandbuch gegebenen Anweisungen verwendet wird.

[QUELLE: prEN ISO 13574:—, 2.183]

4 Anforderungen an die Gestaltung von Anlageteilen in einem Schutzsystem

4.1 Allgemeines

Die elektrische Ausrüstung muss den Anforderungen gemäß EN 60204-1 entsprechen und die Gefährdungen berücksichtigen, welche in der geforderten Risikobeurteilung während der Konstruktionsphase identifiziert wurden. Die elektrische Ausrüstung muss gegen Beschädigung geschützt werden. Insbesondere muss sie gegen Beschädigungen während des Dauerbetriebs widerstandsfähig sein.

Einrichtungen müssen in Übereinstimmung mit den Anweisungen des Herstellers, einschließlich Sicherheitshandbücher, verwendet werden. Jegliche Einrichtung, die außerhalb ihrer veröffentlichten technischen Spezifikation verwendet wird, muss auf ihre Eignung für den vorgesehenen Anwendungszweck geprüft und validiert werden.

Einrichtungen eines Schutzsystems müssen den Umgebungsbedingungen widerstehen und ihre vorgesehene Funktion erfüllen.

Sensoren (z. B. Druckgeber, Temperaturmessumformer, Durchflussgeber), die im Schutzsystem verwendet werden, müssen vom Prozessleitsystem unabhängig sein.

Bild 1 dient der Verdeutlichung der Beziehung zwischen den verschiedenen Komponenten der TPE und zugehörigen Einrichtungen, dem Heizsystem, der Prozessleittechnik/Bedienebene und dem Schutzsystem.

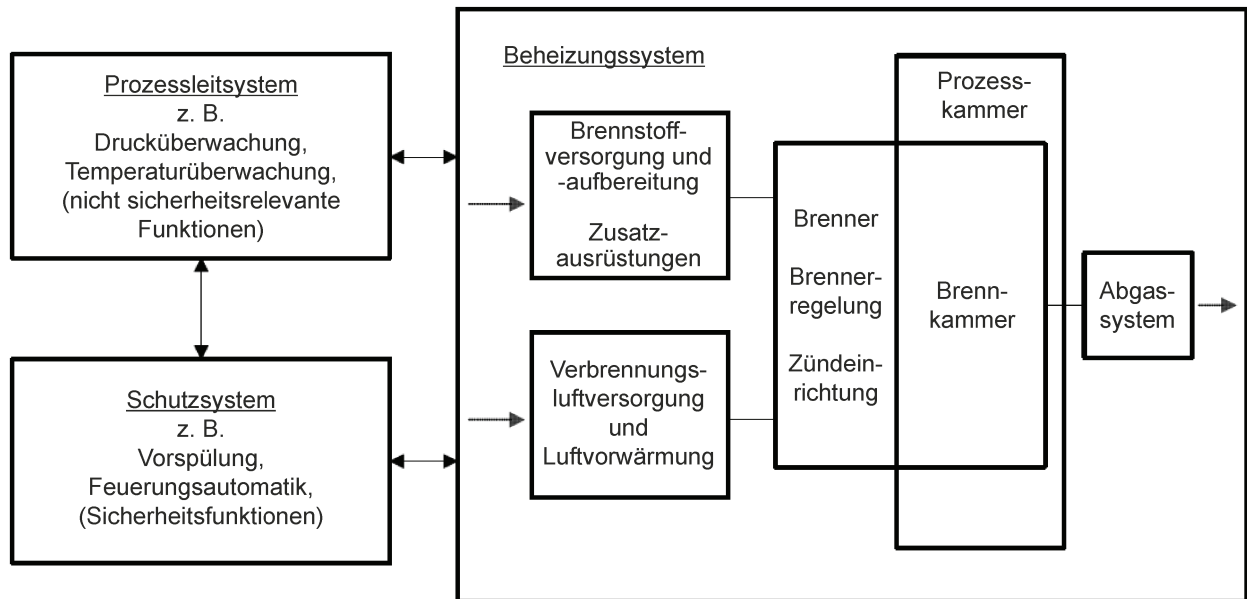


Bild 1 — Blockdiagramm der Steuer- und Schutzsysteme

Es muss eine Reihe geeigneter Techniken und Maßnahmen angewendet werden, die darauf ausgelegt sind, die Einführung von Fehlern bei der Auslegung und Entwicklung der Hard- und Software des Schutzsystems zu verhindern (siehe Anhang A).

Ausfälle aufgrund von Kurzschlüssen in externen Verdrahtungen müssen vermieden werden (siehe Anhang B).

Anforderungen an Prüfung und Prüfungsintervalle für Schutzsysteme müssen in der Betriebsanleitung festgelegt werden. Außer nach den Vorgaben von Verfahren D muss die Prüfung aller Sicherheitsfunktionen mindestens jährlich durchgeführt werden. Verfahren D muss angewendet werden, wenn die Prüfung aller Sicherheitsfunktionen seltener als einmal jährlich durchgeführt wird.

Siehe Anhang C und D für Beispiele für SIL/PL-Bestimmungen.

4.2 Anforderungen an Schutzsysteme

4.2.1 Allgemeines

Jedes oder eine Kombination der vier (4) Verfahren muss zur Implementierung eines Schutzsystems für die in EN 746 (alle Teile) festgelegten Anforderungen an eine Sicherheitsfunktion bzw. an Sicherheitsfunktionen angewendet werden. Jedoch darf für eine bestimmte Sicherheitsfunktion nur ein Verfahren verwendet werden. Es gibt die folgenden vier Verfahren:

- Verfahren A, wie in 4.2.1 festgelegt;
- Verfahren B, wie in 4.2.2 festgelegt;
- Verfahren C, wie in 4.2.3 festgelegt;
- Verfahren D, wie in 4.2.4 festgelegt.

Bild 2 zeigt die grundlegende Konfiguration eines Schutzsystems.

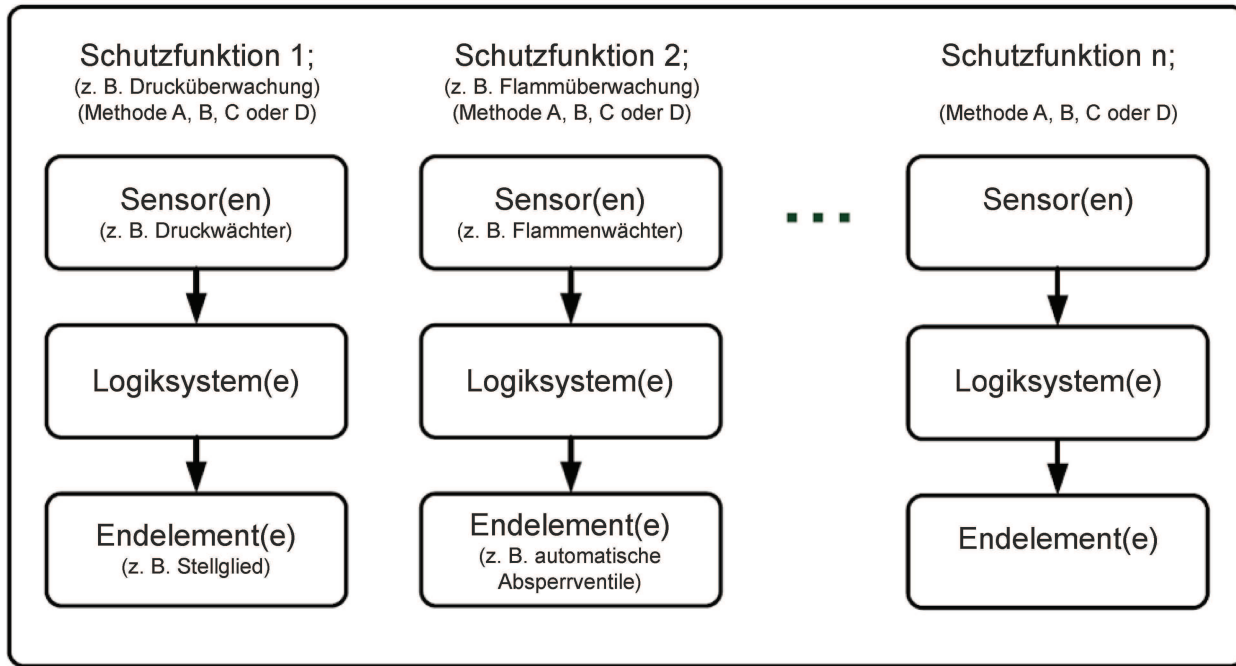


Bild 2 — Grundlegende Konfiguration eines Schutzsystems

Bild 3 zeigt die grundlegenden Eigenschaften der einzelnen Verfahren.

ANMERKUNG 1 Software-Verbindungen sind Verbindungen zwischen Software-Funktionsbausteinen, Sicherheits-SPS-Eingangsfunktionen und Sicherheits-SPS-Ausgangsfunktionen. Sie ähneln festverdrahteten Verbindungen zwischen Einrichtungen.

ANMERKUNG 2 Die Sicherheitsfunktionssoftware ist entweder eine Software-Funktionsbaustein oder ein Programm zur Ausführung von Sicherheitslogikfunktionen (z. B. Vorspülung, Feuerungsautomat).

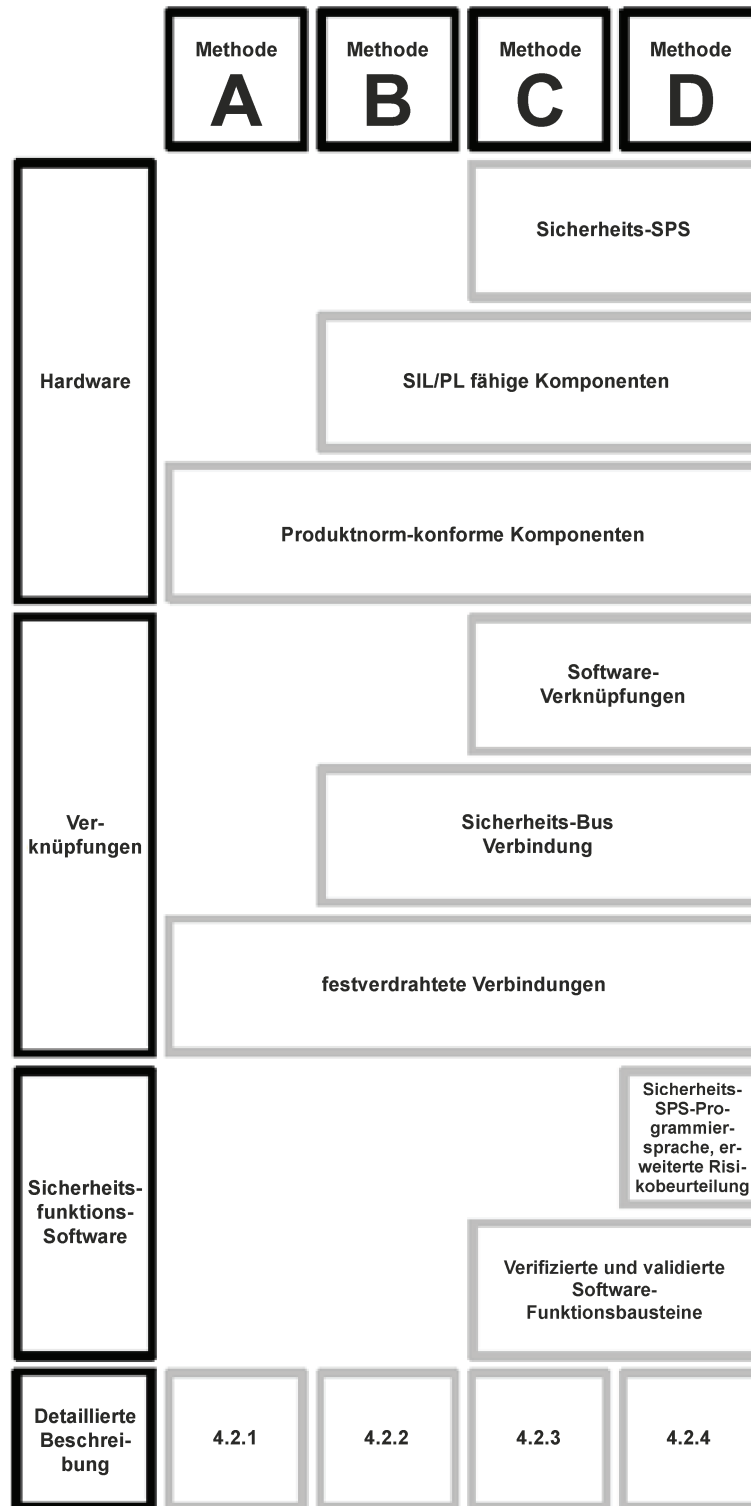


Bild 3 — Überblick über die Verfahren

Anhang E enthält schematische Beispieldiagramme für die verschiedenen Verfahren.

4.2.2 Verfahren A

Verfahren A muss ein festverdrahtetes System sein, in dem alle Einrichtungen (d. h. Sensoren, Logiksysteme und Aktoren, wie in Bild 4 beschrieben) den einschlägigen Produktnormen gemäß EN 746 (alle Teile) und EN 14597:2012 entsprechen.

Die Anforderungen nach EN 61508 (alle Teile), EN 61511 (alle Teile), EN 62061:2005 und EN ISO 13849-1:2015 gelten nicht für diese Art von Schutzsystem.

Die folgenden Anforderungen an die Hartverlötung müssen erfüllt sein:

- alle Logiksysteme müssen durch die Einrichtungen und über die direkten Verbindungen zwischen den Einrichtungen versorgt werden;
- Verbindungen durch Datenkommunikationsbusse sind unzulässig;
- Einrichtungen mit festen Programmsprachen, die die entsprechenden Produktnormen erfüllen, sind zulässig;
- die Hartverlötung muss Anhang F entsprechen

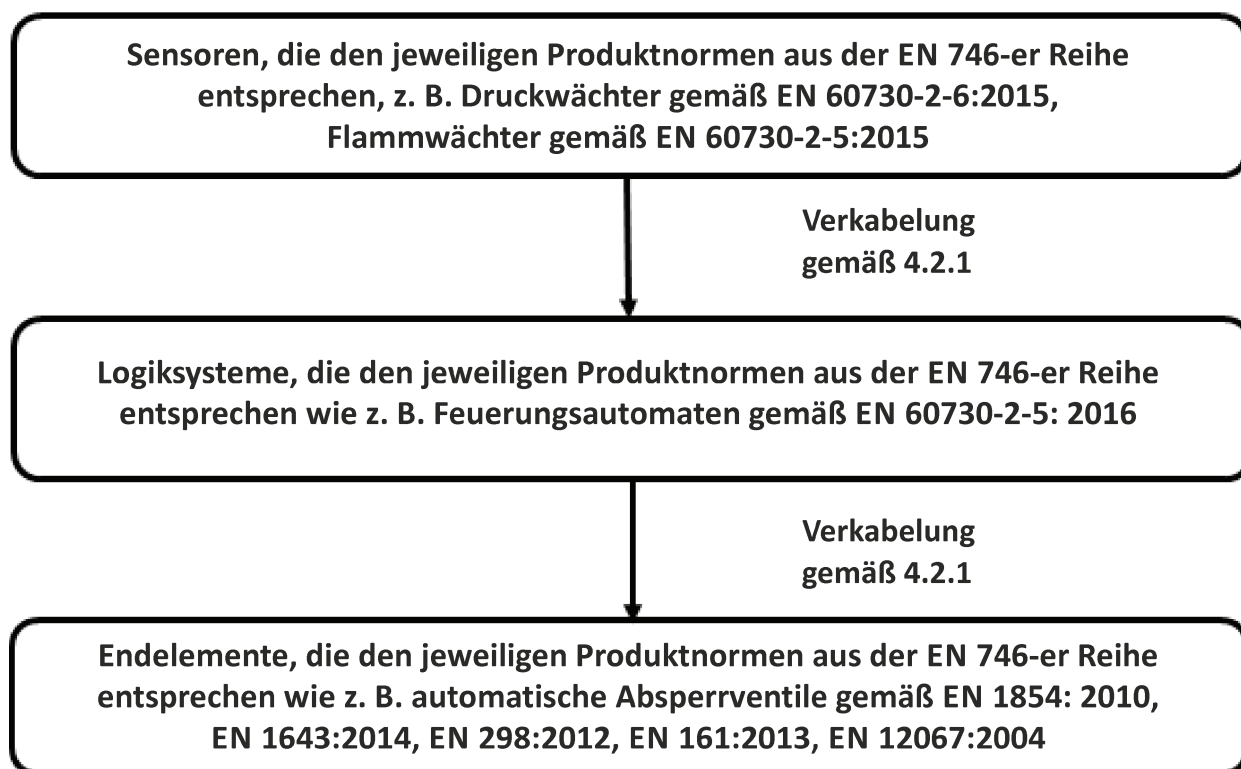


Bild 4 — Hardwarekonfiguration von Verfahren A

ANMERKUNG Die in 4.2.1 verwendeten Sicherheitseinrichtungen entsprechen spezifischen Sicherheitsanforderungen, die auf den Anwendungsbereich und die funktionellen Anforderungen an diese Einrichtungen abgestimmt sind, wie sie in den entsprechenden Produktnormen für Sicherheitseinrichtungen gefordert werden, z. B. Feuerungsautomaten, Ventilprüfsysteme, Druckmessgeräte, automatische Absperrventile. Selbst ohne zusätzliche SIL/PL-Zertifizierung dieser Sicherheitseinrichtungen entsprechen die Sicherheitsanforderungen an die Anwendung der Sicherheitseinrichtungen den entsprechenden Produktnormen. Eine Implementierung des Schutzsystems nach 4.2.1 ist eines von verschiedenen alternativen Verfahren.

4.2.3 Verfahren B

Verfahren B muss eine Kombination aus Einrichtungen, die den einschlägigen Produktnormen entsprechen, und/oder SIL/PL-fähigen Geräten, für die keine relevante Produktnorm existiert, sein. Sicherheits-SPS sind ausgenommen (siehe Bild 5).

Die folgenden Anforderungen an die Hartverlötung müssen erfüllt sein:

- alle Logiksysteme müssen durch die Einrichtungen und über die direkten Verbindungen zwischen den Einrichtungen versorgt werden;
- Einrichtungen mit festen Programmsprachen, die die entsprechenden Produktnormen erfüllen, sind zulässig;
- Verbindungen dürfen festverdrahtet oder durch einen Sicherheitsbus geleitet sein;
- die Hartverlötung muss Anhang F entsprechen.

Für Einrichtungen, die nicht von Produktnormen abgedeckt werden, müssen die folgenden Anforderungen erfüllt werden:

- die Einrichtung muss nach EN 61508 (alle Teile), EN 62061:2005 oder EN 61511 (alle Teile) SIL-3-fähig oder nach EN ISO 13849-1:2015 PL-e-fähig sein;
- Eine Zertifizierung für die SIL/PL-Fähigkeit muss für die gesamte Einrichtung, einschließlich Hard- und Software, gelten.

ANMERKUNG 1 Die Überprüfung und Validierung der SIL/PL-Zertifizierung für Einrichtungen erfolgt in der Regel durch eine notifizierte Stelle, ein akkreditiertes nationales Prüflabor oder durch eine Organisation nach EN ISO/IEC 17025:2005.

Einrichtungen mit einer geringeren Kapazität als SIL 3/PL e sind zulässig, sofern die SIL/PL-Anforderungen an Schleife (Sicherheitsfunktion) bestimmt und berechnet wurden.

Wenn der SIL durch vorherige Verwendung bestimmt wird (d. h. im Gebrauch nachgewiesen), müssen die Anforderungen der EN 61511 (alle Teile) erfüllt werden.

Alle Anforderungen im Sicherheitshandbuch für die Einrichtung, wie etwa das Prüfungsintervall, müssen eingehalten werden.

ANMERKUNG 2 Siehe Anhang C für Beispiele für die SIL/PL-Bestimmung.

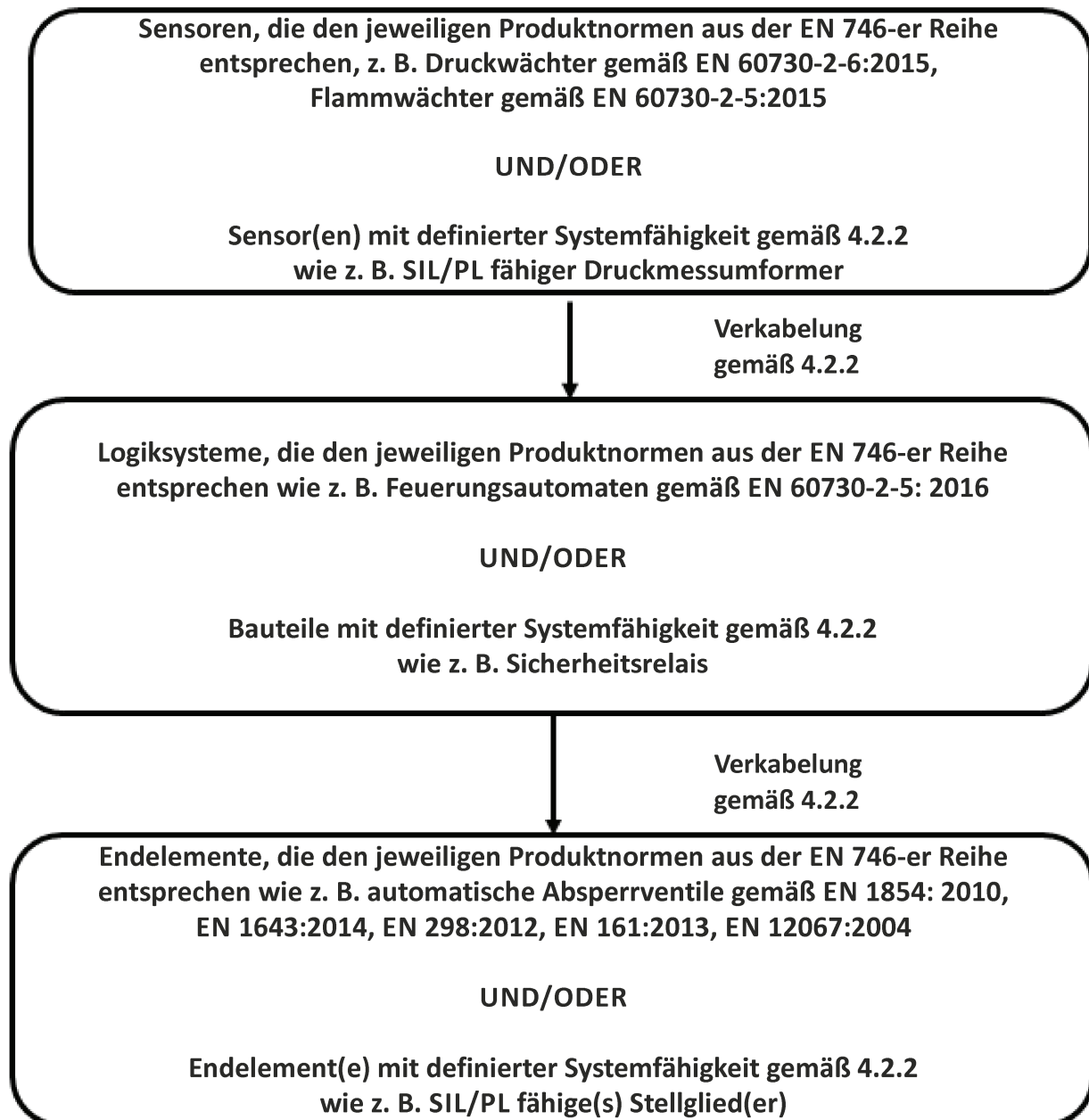


Bild 5 — Hardwarekonfiguration von Verfahren B

4.2.4 Verfahren C

4.2.4.1 Allgemeines

Verfahren C muss eine Kombination aus Einrichtungen, die den einschlägigen Produktnormen entsprechen, und/oder SIL/PL-fähigen Geräten, für die keine relevante Produktnorm existiert, und/oder Sicherheits-SPS sein.

Die folgenden Anforderungen an die Hartverlötung müssen erfüllt sein:

- alle Logiksysteme müssen durch die Einrichtungen und über die direkten Verbindungen zwischen den Einrichtungen versorgt werden;
- Einrichtungen mit festen Programmsprachen, die die entsprechenden Produktnormen erfüllen, sind zulässig;
- Verbindungen dürfen festverdrahtet, durch einen Sicherheitsbus geleitet oder Softwareverbindungen sein;
- die Hartverlötung muss Anhang F entsprechen.

Sicherheitsfunktionssoftware ist nur in Form von geprüfter und validierter SIL-3-fähiger Software-Funktionsbausteine (siehe Bild 6) zulässig.

Sicherheitsfunktionen sind innerhalb einer sicherheitsbewerteten Einrichtung (z. B. einer Sicherheits-SPS) oder innerhalb einer externen Einrichtung, die unter die entsprechende Produktnorm fällt, zulässig.

Für Einrichtungen (Sicherheits-SPS, Zeitsteuergeräte usw.), die NICHT von Produktnormen abgedeckt werden, müssen die folgenden Anforderungen erfüllt werden:

- die Einrichtungen müssen nach EN 61508 (alle Teile), EN 62061:2005 oder EN 61511 (alle Teile) SIL-3-fähig oder nach EN ISO 13849-1:2015 PL-e-fähig sein;
- wenn eine programmierbare Einrichtung eine Sicherheitsfunktion implementiert, die ganz oder teilweise in einer relevanten Produktnorm behandelt wird, muss die Softwarefunktion im Hinblick auf die anwendbaren Anforderungen in der betreffenden Produktnorm überprüft und validiert werden, einschließlich, aber nicht beschränkt auf die Abläufe und Zeitabläufe der Produktnorm;
- Softwareverbindungen in einer programmierbaren Einrichtung müssen durch eine Funktionsprüfung verifiziert werden;
- Software-Programmiersprachen für SPS müssen EN 61131-1:2013 entsprechen;
- Software muss gegen unautorisierte und unbeabsichtigte Änderungen gesperrt und gesichert werden.

ANMERKUNG 1 Die Überprüfung und Validierung der SIL/PL-Zertifizierung erfolgt in der Regel durch eine notifizierte Stelle, ein akkreditiertes nationales Prüflabor oder durch eine Organisation nach EN ISO/IEC 17025:2005.

Einrichtungen mit einer geringeren Kapazität als SIL 3/PL e sind zulässig, sofern die SIL/PL-Anforderungen an Schleife (Sicherheitsfunktion) bestimmt und berechnet wurden.

Wenn der SIL durch vorherige Verwendung bestimmt wird (d. h. im Gebrauch nachgewiesen), müssen die Anforderungen der EN 61511 (alle Teile) erfüllt werden.

Alle Anforderungen im Sicherheitshandbuch für die Einrichtung, wie etwa das Prüfungsintervall, müssen eingehalten werden.

ANMERKUNG 2 Siehe Anhang C für Beispiele für die SIL/PL-Bestimmung.

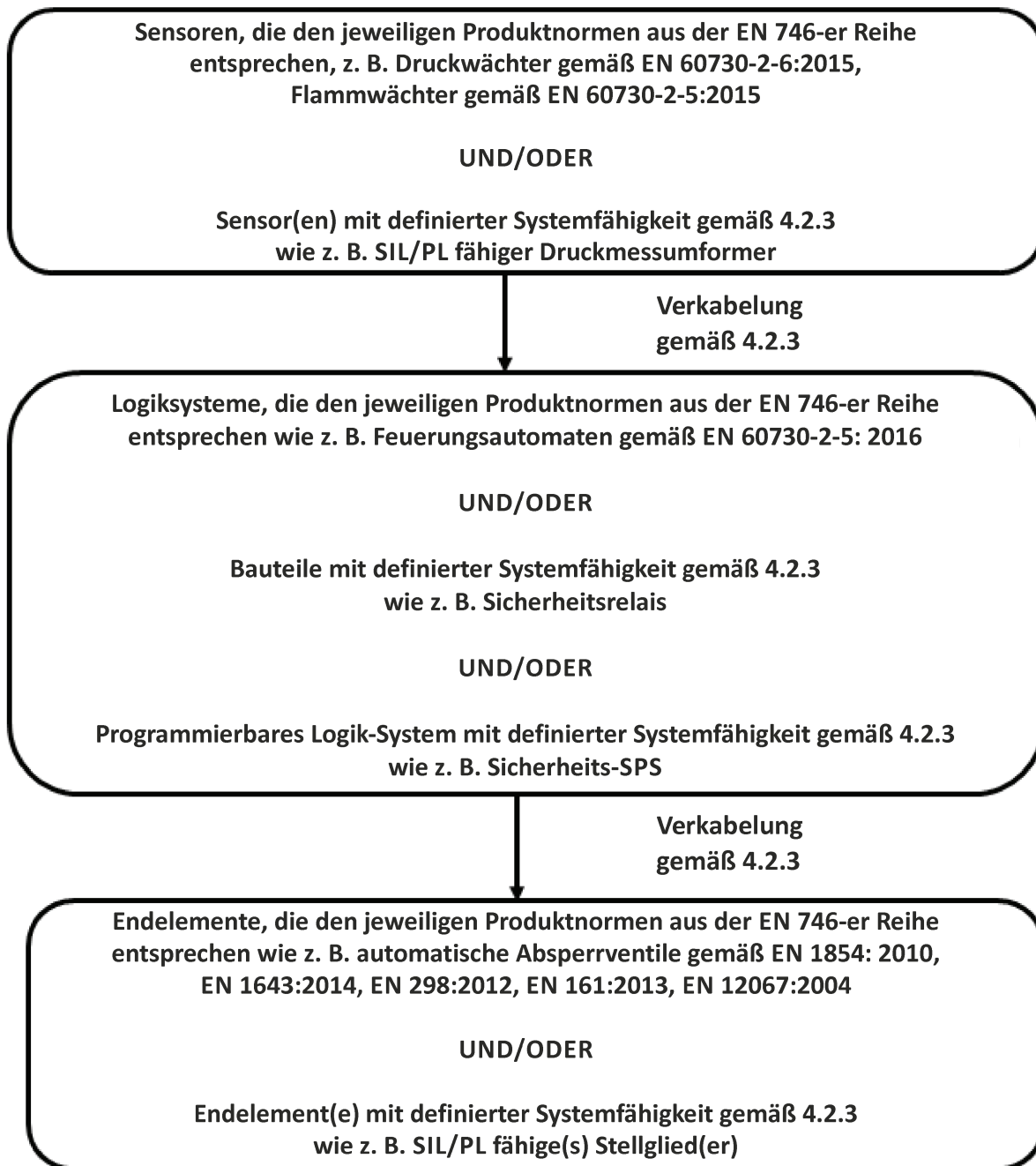


Bild 6 — Hardwarekonfiguration von Verfahren C

4.2.4.2 Anforderungen an Anwendungssoftware

4.2.4.1.1 Gemäß dem geforderten Sicherheits-Integritätslevel müssen die gewählte programmierbare Schutzeinrichtung und ihre Software die Sicherheitsintegritätsanforderungen der jeweiligen Anwendung erfüllen:

- Korrektheit der Funktionalität;
- Sequenzierung und zeitbezogene Informationen;
- zeitliche Beschränkungen;
- Gleichlauf (Softwareunterbrechungen sollten vermieden werden);
- Datenstrukturen und -eigenschaften;
- Planungsannahmen und -abhängigkeiten;
- Prüfbarkeit.

4.2.4.1.2 Der Nachweis der unter 4.2.4.1.1 aufgeführten Punkte muss durch Prüfungs- und Validierungsschritte gemäß den Auslegungs- und Entwicklungsphasen innerhalb des Lebenszyklus der Software erbracht werden, einschließlich

- Validität der Softwareanforderungsspezifikation und
- Vollständigkeit, Einheitlichkeit, Verständlichkeit und Klarheit der Dokumentation und Programme.

Die Darstellungen der Anwendungsauslegung müssen auf einer Notation (z. B. Funktionsdiagramm) beruhen, die eindeutig definiert ist oder auf eindeutig definierte Merkmale beschränkt ist; soweit durchführbar, muss die Anwendungsauslegung den sicherheitsbezogenen Teil der Software minimieren. Soll die Software sowohl Sicherheits- als auch Nicht-Sicherheitsfunktionen implementieren, so muss die gesamte Software als sicherheitsrelevant behandelt werden, es sei denn, dass eine angemessene Unabhängigkeit zwischen den Funktionen in der Anwendungsauslegung nachgewiesen werden kann. Soll die Software Sicherheitsfunktionen mit unterschiedlichen Sicherheits-Integritätslevels implementieren, so muss die gesamte Software als dem höchsten Sicherheits-Integritätslevel zugehörig behandelt werden, es sei denn, in der Anwendungsauslegung kann eine angemessene Unabhängigkeit zwischen den Sicherheitsfunktionen der verschiedenen Sicherheits-Integritätslevel nachgewiesen werden. Die Rechtfertigung der Unabhängigkeit muss in der relevanten Auslegungsdokumentation aufgezeichnet werden.

Sollen im Betrieb bewährte Softwaremodule als Teil der Anwendungssoftware verwendet werden, müssen sie eindeutig gekennzeichnet und dokumentiert werden. Die Eignung der Software zur Erfüllung der Anforderungen einer bestimmten Anwendung muss gerechtfertigt werden. Die Eignung muss auf dem Nachweis eines zufriedenstellenden Betriebs in einer ähnlichen Anwendung oder der Durchführung der gleichen Prüfungs- und Validierungsverfahren, die für jede neu entwickelte Software erwartet werden, beruhen. Bei im Betrieb erprobten Softwaremodulen kann der Umfang der Prüfungen auf die für eine ordnungsgemäße Implementierung erforderlichen Prüfungen beschränkt werden. Einschränkungen aus der bisherigen Softwareumgebung (z. B. Betriebssystem und Compilerabhängigkeiten) sollten bewertet werden. Je nach Art der Softwareentwicklung kann die Verantwortung für die Einhaltung von 4.2.4.1 vom Lieferanten allein, vom Anwender allein oder von beidem getragen werden. Die Aufteilung der Verantwortung muss aufgezeichnet werden. Die vorgeschlagene Softwarearchitektur muss auf einer Aufteilung in Einrichtungen/Teilsysteme, die als Teil der Systemsoftware und der anlagenspezifischen Anwendungssoftware identifiziert werden können, beruhen.

Die folgenden Angaben müssen bereitgestellt werden:

- ob sie neu, bestehend oder proprietär sind;
- ob sie zuvor verifiziert wurden und wenn ja, ihre Verifizierungsbedingungen;
- ob jedes Teilsystem/jede Einrichtung sicherheitsbezogen ist oder nicht;
- das Sicherheits-Integritätslevel des Teilsystems/der Einrichtung;
- Bestimmung, Bewertung und Einzelheiten zur Bedeutung aller Hardware-/Softwareinteraktionen;
- eine Notation, die zur Darstellung der Architektur verwendet wird, die eindeutig definiert ist oder auf eindeutig definierte Merkmale beschränkt ist;
- Identifizierung der Auslegungsmerkmale, die zur Aufrechterhaltung der Sicherheitsintegrität aller Daten verwendet werden (dazu gehören Eingangs-Ausgangs-Daten der Anlage, Kommunikationsdaten, Daten der Bedienerschnittstelle, Wartungsdaten und interne Datenbankdaten).

4.2.5 Verfahren D

Verfahren D muss alle Anforderungen nach EN 61508 (alle Teile), EN 62061:2005, EN 61511 (alle Teile) oder EN ISO 13849-1:2015 erfüllen (siehe Bild 7).

ANMERKUNG 1 Siehe Anhang D für das Verfahren in Übereinstimmung mit EN 61511 (alle Teile).

Verfahren D muss auch die folgenden Anforderungen erfüllen:

- a) der Flammenwächter muss EN 60730-2-5:2009 oder EN 298:2012 erfüllen;
- b) alle Anforderungen der SPS und aller Sicherheitseinrichtungen müssen in Übereinstimmung mit allen Anweisungen im Produktsicherheitshandbuch des Herstellers der Einrichtung angewendet werden, einschließlich der Abstimmungs- und Prüffrequenzanforderungen;
- c) jede Anforderung an die funktionale Sicherheit, wie sie in EN 746 (alle Teile) festgelegt ist, muss gemäß den Normen, z. B. EN 61511 (alle Teile), EN ISO 13849-1:2015 und EN 62061:2005, auf ihren Bedarf hin bewertet und mit dem erforderlichen SIL für jede Funktion umgesetzt werden. Sicherheitsfunktionen des sicherheitsbezogenen Systems, wie z. B. Feuerungsautomat, Ventilprüfung, Luft-Brennstoff-Verbundregler usw., müssen den Sicherheitsanforderungen der einschlägigen Produktnormen entsprechen;

ANMERKUNG 2 Eine erweiterte Risikobeurteilung in Verfahren D kann Vorrang vor den Sicherheitsanforderungen in EN 746 (alle Teile) haben. Aufgrund der Art der erweiterten Risikobeurteilung im Rahmen von Verfahren D wird die allgemeine Sicherheit nicht verringert und erfüllt oder übertrifft die vorgesehenen Anforderungen von EN 746 (alle Teile).

- d) Verbindungen dürfen festverdrahtet, durch einen Sicherheitsbus geleitet oder Softwareverbindungen sein;
- e) die Hartverlötung muss Anhang F entsprechen.

ANMERKUNG 3 Die Überprüfung und Validierung der SIL/PL-Zertifizierung erfolgt der Regel durch eine notifizierte Stelle, ein akkreditiertes nationales Prüflabor oder durch eine Organisation nach EN ISO/IEC 17025:2005.

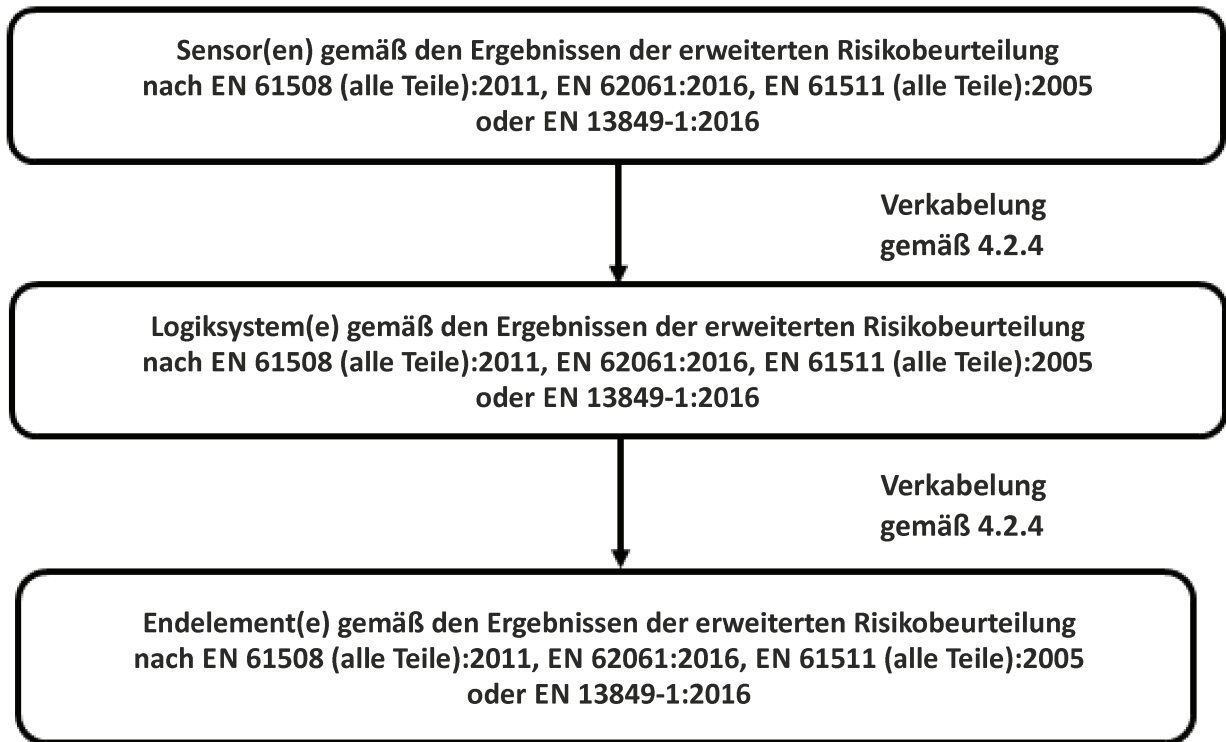


Bild 7 — Hardwarekonfiguration von Verfahren D

4.3 Fehlerbetrachtung für den festverdrahteten Teil von Schutzsystemen

Das Schutzsystem muss so ausgelegt sein, dass die nach EN 746 (alle Teile) erforderlichen Einrichtungen wie folgt verwendet werden müssen:

- a) Wenn Relais in Sicherheitsfunktionen eingesetzt werden, müssen die Kontakte überwacht und zwangsgeführt werden, und der an alle Kontakte angelegte Strom darf höchstens 60 % der Nennleistung der Kontakte betragen. Steuerrelais für die Sicherheit müssen EN 60947-5-1:2017 oder der geforderten SIL/PL-Anforderung entsprechen. Leistungsrelais für die Sicherheit mit oder ohne Spiegelkontakte müssen EN IEC 60947-4-1:2019 oder der geforderten SIL/PL-Anforderung entsprechen.
- b) Die Einrichtungen müssen in Übereinstimmung mit den Anweisungen des Herstellers verdrahtet werden.
- c) Wenn bei den Verfahren B und C Zeitsteuergeräte, die nicht, wie in allen anderen Teilen von EN 746 festgelegt, den einschlägigen Produktnormen entsprechen, in Sicherheitsfunktionen verwendet werden, müssen sie eine systematische Fähigkeit von SC 3 (SIL-3-fähig) aufweisen. Die Einstellungen von einstellbaren Zeitsteuergeräten müssen verriegelt oder versiegelt sein.
- d) Es muss ein Überstromschutz vorgesehen werden, um den Strom im Sicherheitskreis auf unter 60 % der niedrigsten Einrichtungskontaktleistung zu begrenzen.
- e) Anhang F enthält zusätzliche Anforderungen.

4.4 Ausfall von Versorgungseinrichtungen

Der Ausfall von Versorgungseinrichtungen (z. B. Strom, Instrumentenluft) für die TPE muss einen sicheren Zustand (z. B. Verriegelung) auslösen. Jeder Neu-Start darf nur durch einen manuellen Eingriff ausgelöst werden. Anlauf und Zündung müssen prEN 746-2:—, 4.2.7 oder 4.3.7, entsprechen.

4.5 Rücksetzen/Entriegelung

Sofern nach Verfahren gestattet, muss an Einrichtungen, die eine Sicherheitsfunktion erfüllen, muss das Rücksetzen nach einer Störabschaltung manuell nach Beseitigung des Fehlers durchgeführt werden (siehe prEN ISO 13574:—, 2.107).

Eine Rücksetzung darf eine Sicherheitsfunktion nicht außer Kraft setzen.

Die Auslegung muss Maßnahmen zur Verhinderung unbeabsichtigter und permanenter Rücksetzungen umfassen.

Die Auslegung muss Maßnahmen zur Verhinderung des unbeabsichtigten Anlaufs der TPE umfassen.

Die Betriebsanleitung muss eine Anforderung beinhalten, dass der Bediener vor dem Auslösen einer Rücksetzung den sicheren Betrieb gewährleistet.

Die maximale Anzahl der Rücksetzungen innerhalb eines bestimmten Zeitraums muss auf der Grundlage der Risikobeurteilung begrenzt und in der Betriebsanleitung angegeben werden.

Wenn die manuelle Rücksetzung ohne Sicht auf die TPE ausgelöst wird, muss ein sicherer Betrieb durch den Rücksetzungsvorgang gewährleistet sein und der aktuelle Status und die relevanten Informationen des kontrollierten Prozesses müssen für den Benutzer sichtbar sein.

Anhang A (informativ)

Erläuterung der Techniken und Maßnahmen zur Vermeidung systematischer Fehler

A.1 Allgemeines

Zufällige Fehler haben physikalische Ursachen (z. B. extreme Temperaturen, Korrosion, Verschleiß) und statistische Informationen können für eine Risikoanalyse herangezogen werden. Systematische Fehler ergeben sich jedoch aus menschlichem Fehlverhalten in den Spezifikationen und der Auslegung des Schutzsystems. Systematische Fehler können verborgen sein, bis bestimmte Bedingungen auftreten, und werden unter Umständen lange nicht entdeckt. Diese spezifischen Bedingungen führen dazu, dass alle Einrichtungen, die aus diesem System hergestellt wurden, in gleicher Weise ausfallen. Daher ist es wichtig, systematischen Fehlern direkt vom Anfang eines Projektes vorzubeugen.

A.2 Kompetenzen

Da systematische Fehler menschlicher Natur sind, müssen die Personen und ihre Organisation, die an der Auslegung und Entwicklung von Schutzsystemen beteiligt sind, die entsprechenden Kompetenzen für die Aktivitäten, für die sie verantwortlich sind, aufweisen. Jede Person, Abteilung, Organisation oder andere Einheit muss identifiziert und über die ihnen zugewiesenen Verantwortlichkeiten informiert werden (gegebenenfalls einschließlich Genehmigungsbehörden oder Sicherheitsbehörden). Die folgenden Punkte müssen bei der Bestimmung der Kompetenzen für die Auslegung des Schutzsystems behandelt werden:

- a) Ingenieurwissen, Schulung und Erfahrung im Hinblick auf
 - 1) die Prozessanwendung,
 - 2) die jeweilige verwendete Technologie (z. B. Elektrik, Elektronik, Programmierung) und
 - 3) die Sensoren und Aktoren;
- b) Sicherheitstechnikwissen (z. B. Prozesssicherheitsanalyse);
- c) Kenntnisse der gesetzlichen und regulatorischen funktionalen Sicherheitsanforderungen;
- d) angemessene Management- und Führungskompetenzen, die für die jeweilige Rolle in Auslegung geeignet sind;
- e) Kenntnis der potenziellen Konsequenzen eines Ereignisses;
- f) Eignung für die Neuheit und Komplexität der Anwendung und der Technologie.

Weitere Informationen zu Kompetenzen können EN 61511-1:2017 entnommen werden.

A.3 Vermeidung systematischer Fehler

Im Folgenden wird eine Zusammenfassung typischer Aktivitäten geliefert, die für die Vermeidung systematischer Fehler während der Auslegungsphase erforderlich sind. Weitere Einzelheiten können EN 61508-2:2010 entnommen werden.

Es ist ein Auslegungsverfahren mit Merkmalen, die Folgendes ermöglichen, auszuwählen:

- a) Transparenz, Modularität und andere Merkmale, die Komplexität beeinflussen;
- b) eindeutiger und präziser Ausdruck von
 - 1) Funktionalität,
 - 2) Teilsystem- und Elementschnittstellen,
 - 3) Sequenzierung und zeitbezogenen Informationen, und
 - 4) Gleichlauf und Synchronisation;
- c) eindeutige und präzise Dokumentation und Kommunikation von Informationen;
- d) Prüfung und Validierung.

Es sind Merkmale zu nutzen, die das Schutzsystem gegen systematische und zufällige Fehler sowie verbleibende Auslegungsfehler in der Hardware, Software und im Datenkommunikationsprozess schützen.

Während der Auslegung sind die Aktivitäten, die beim Entwickler durchgeführt werden können, von denen zu unterscheiden und zu bestimmen, für die Zutritt zum Standort des Benutzers erforderlich ist.

Wartungsanforderungen müssen während der Auslegungsphase formal festgehalten werden, um sicherzustellen, dass die Anforderungen an die Sicherheitsintegrität der Schutzsysteme über den Lebenszyklus kontinuierlich erfüllt werden.

Es sind die menschlichen Fähigkeiten und Einschränkungen sowie die Aktivitäten, die Bedienungspersonen und Wartungspersonal zugewiesen sind, einschließlich ihres wahrscheinlichen Schulungsniveaus oder ihrer Kenntnisse, zu berücksichtigen.

Die Integrationsprüfungen für das Schutzsystem und die Prüfplandokumentation, einschließlich der folgenden Punkte, sind zu planen:

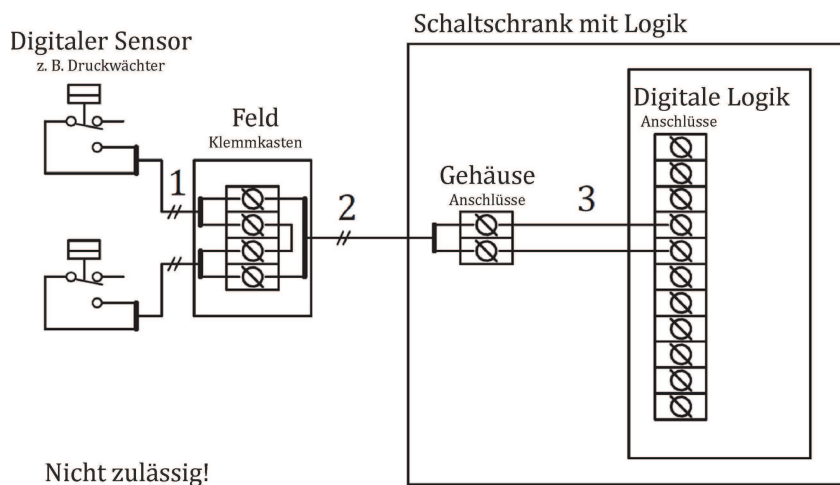
- die Arten der durchzuführenden Prüfungen und die zu befolgenden Verfahren;
- die Prüfungsumgebung, Werkzeuge, Konfiguration und Programme;
- die Kriterien für bestanden/nicht bestanden.

Wo anwendbar, sind automatische Prüfwerkzeuge und integrierte Entwicklungswerkzeuge zu verwenden.

Anhang B (informativ)

Beispiele für Techniken zur Vermeidung von Fehlern durch die externe Verkabelung

Bild B.1 zeigt, wie ein möglicher Kurzschluss an Kabel 2 das Schutzsystem außer Kraft setzt. Bei der normalen Sicherheitsfunktion würde ein geöffneter Zustand der Druckschalterkontakte dazu führen, dass das Logiksystem eine Aktion durch den Aktor ausführt, um das System in einen sicheren Zustand zu bringen. Bei einem Kurzschluss an Kabel 2 wird der offene Zustand bei beiden Schaltern nicht entdeckt.



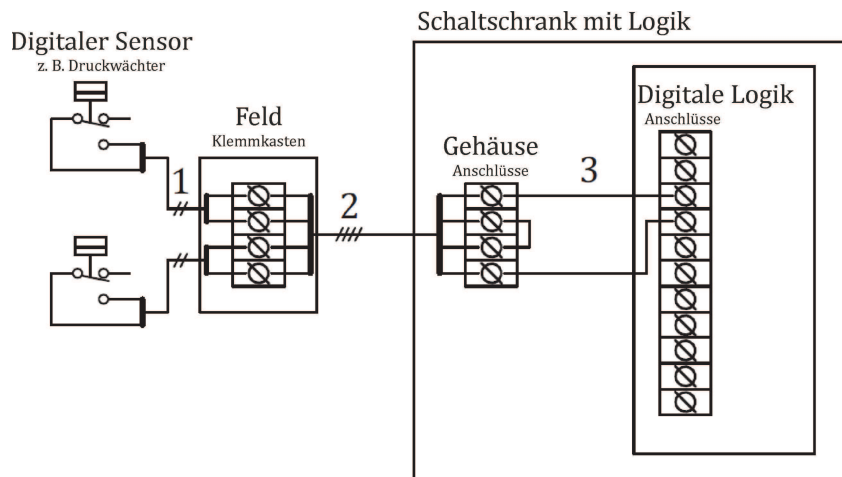
Legende

- 1 Kabel 1
- 2 Kabel 2
- 3 Kabel 3

Bild B.1 — Falsche externe Verkabelungsmethode

ACHTUNG — Bild B.1 zeigt ein FALSCHES Beispiel für eine externe Verkabelungsmethode.

Bild B.2 zeigt eine Technik, die bei Verwendung der Schutzsystemverfahren A und B ein ausreichendes Schutzniveau für die Sicherheitsfunktion bieten kann. Alle Leiter werden über Kabelkanäle oder Leitungen, die einen ausreichenden Schutz vor mechanischen und thermischen Schäden bieten, in das Hauptgehäuse zurückgeführt. Die Drahtverbindungen werden auch innerhalb des Hauptgehäuses des Logiksystems des Schutzsystems hergestellt.

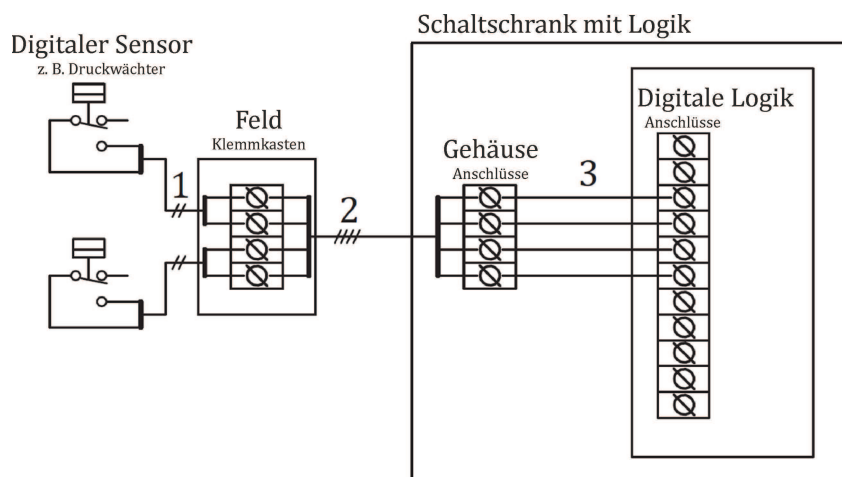


Legende

- 1 Kabel 1
- 2 Kabel 2
- 3 Kabel 3

Bild B.2 — Geschützte Verkabelung

Bild B.3 zeigt eine minimale Variation von Bild B.2, wobei die Schutzsystemeinrichtung jeden Leiter von den Sensoren aufnimmt und bei Verwendung eines der Schutzsystemverfahren, A, B, C oder D, ein ausreichendes Schutzniveau für die Sicherheitsfunktion bieten kann.

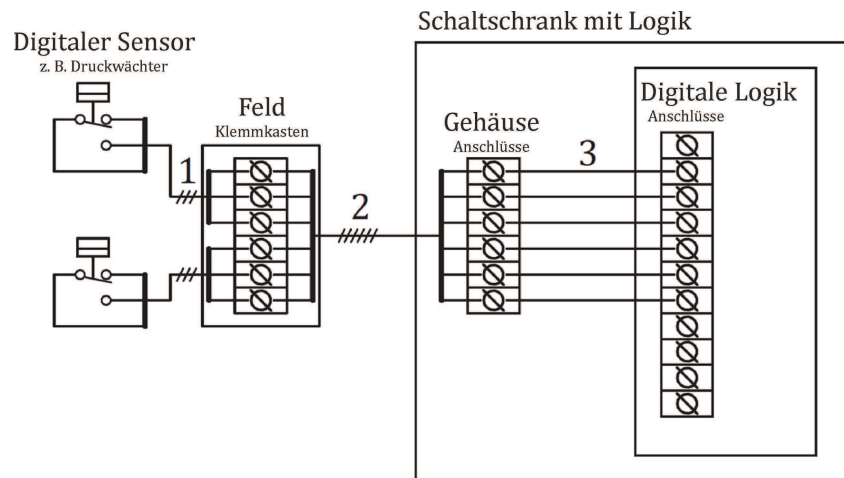


Legende

- 1 Kabel 1
- 2 Kabel 2
- 3 Kabel 3

Bild B.3 — Geschützte Verkabelung, alle Leiter durchgehend geführt

Bild B.4 zeigt eine Technik, bei der beide Zustände des Sensorschalters durch das Schutzsystem überwacht werden und dessen Logiksystem den unzulässigen Zustand erkennt, der durch einen Kurzschluss in der Feldverdrahtung verursacht wird. Diese Technik ist geeignet, wenn eines der Schutzsystemverfahren, A, B, C oder D, verwendet wird.

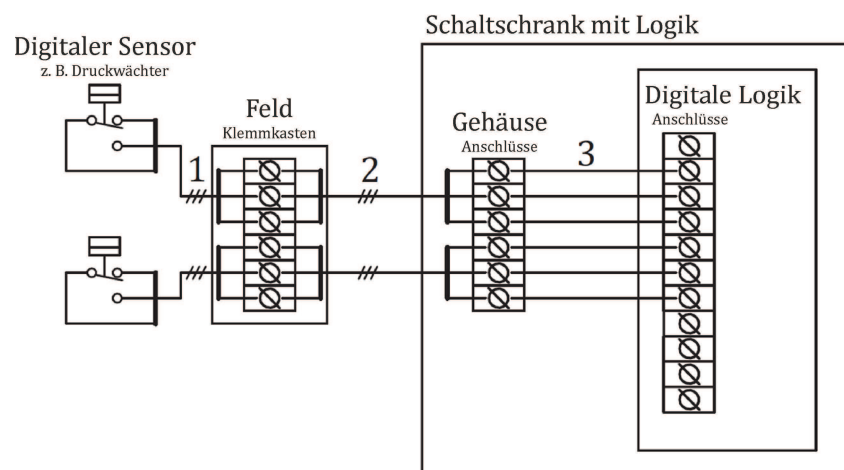


Legende

- 1 Kabel 1
- 2 Kabel 2
- 3 Kabel 3

Bild B.4 — Überwachung der beiden Zustände

Bild B.5 zeigt eine Variation von Bild B.4, wobei ein einzelnes Kabel 2 mit 6 Leitern durch zwei Kabel mit 3 Leitern ersetzt werden kann.

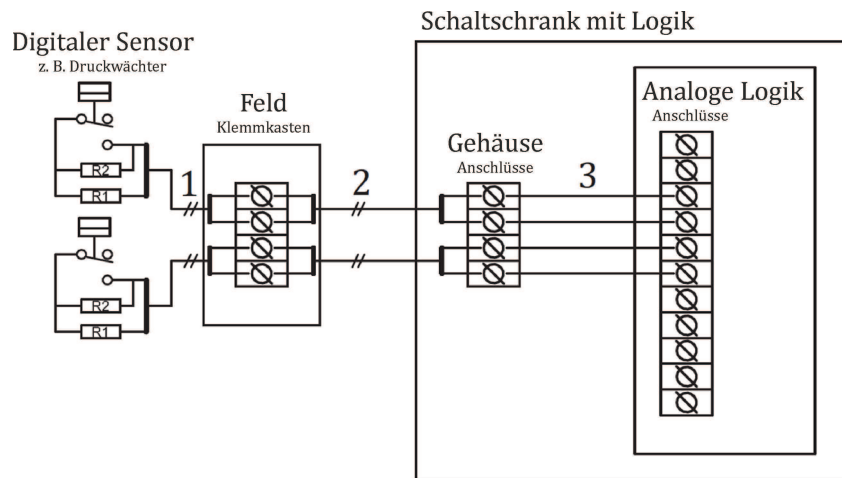


Legende

- 1 Kabel 1
- 2 Kabel 2
- 3 Kabel 3

Bild B.5 — Überwachung der beiden Zustände, mehrere Kabel

Abbildung B.6 zeigt eine Technik mit analogen Signalen für die Schaltzustände und das Logiksystem des Schutzsystems erkennt den unzulässigen Zustand durch einen Kurzschluss in der Feldverdrahtung (der analoge Pegel liegt außerhalb der zulässigen Bänder für den hohen oder niedrigen Zustand). Diese Technik ist geeignet, wenn eines der Schutzsystemverfahren, A, B, C oder D, verwendet wird.



Legende

- 1 Kabel 1
- 2 Kabel 2
- 3 Kabel 3

Bild B.6 — Überwachung durch analogen Wert

Anhang C (informativ)

Beispiele für die Bestimmung des Sicherheits-Integritätslevels (SIL) mittels des Risikograph-Verfahrens

C.1 Allgemeines

Verschiedene Internationale Normen können zur Bestimmung des erforderlichen SIL/PL herangezogen werden. Für maschinelle Anlagen wurde EN 62061:2005 zur Bestimmung des SIL entwickelt während EN 61511 (alle Teile) zur Bestimmung des erforderlichen SIL in der Prozessindustrie entwickelt wurde. Risikograph-Verfahren für die Bestimmungen des Sicherheits-Integritätslevels (SIL) werden in den beiden Europäischen Normen [EN 62061 und EN 61511 (alle Teile)] angegeben. Zudem deckt EN ISO 13849-1:2015 die Bestimmung des Performance Level (PL) ab und enthält auch ein Verfahren zur Bestimmung eines PL aus einem SIL (EN ISO 13849-1:2015, Tabelle 4).

Für jede Gefährdung des Industrieofens und der zugehörigen Prozessanlagen (TPE) muss eine Gefahren- und Risikoanalyse durchgeführt werden. Bei der Beschreibung der Gefährdung muss auch stets die Ursache für die Gefährdungssituation angegeben werden. So kann beispielsweise eine Explosion im Ofen durch eine Vielzahl von Ursachen, wie Überhitzung, Überdruck, unzureichendes Brennstoff-Luft-Verhältnis usw., verursacht werden. Jeder dieser Ursachen wird dann mindestens eine sicherheitsbezogene Funktion zugeordnet, die dann das daraus resultierende Risiko reduzieren muss.

Das erforderliche SIL/PL für jede sicherheitsbezogene Funktion hängt von verschiedenen Parametern ab:

- Folgen des Gefährdungsereignisses (Parameter Se gemäß Anhang A von EN 62061:2005, Parameter C gemäß EN 61511-3:2017); das Szenario der ungünstigsten Möglichkeiten muss berücksichtigt werden;
- Häufigkeit und Dauer der im Gefährdungsbereich verbrachten Zeit (Parameter Fr gemäß Anhang A von EN 62061:2005, Parameter F gemäß EN 61511-3:2017); der Faktor der verbrachten Zeit muss auf der Grundlage der am stärksten gefährdeten Person und nicht des Durchschnitts aller Personen bestimmt werden. Somit wird sichergestellt, dass das Risiko nicht über alle Personen gemittelt wird;
- Möglichkeit der Verhinderung oder Vermeidung des Gefährdungsereignisses (Parameter Av gemäß Anhang A von EN 62061:2005, Parameter P gemäß EN 61511-3:2017);
- Eintrittswahrscheinlichkeit des Gefährdungsereignisses oder der Anforderungsrate (Parameter Pr gemäß Anhang A von EN 62061:2005, Parameter W gemäß EN 61511-3:2017).

Der Parameter Av gemäß Anhang A von EN 62061:2005 und der Parameter P gemäß EN 61511-3:2017 können unter Berücksichtigung von Aspekten der TPE-Auslegung und ihrer vorgesehenen Anwendung geschätzt werden, was dazu beitragen kann, den Schaden durch eine Gefahr zu vermeiden oder zu begrenzen. Zu diesen Aspekten gehören beispielsweise die Geschwindigkeit des Auftretens des Gefährdungsereignisses (plötzlich, schnell oder langsam), die räumliche Möglichkeit, sich von der Gefährdung zurückzuziehen, die Art der Einrichtung oder des Systems und die Möglichkeit der Erkennung einer Gefährdung. Der geringste Wert sollte nur verwendet werden, wenn

- das Risiko offensichtlich ist, bevor es sich vollständig entfaltet,
- die Zeit, die nach der Erkennung bis zum vollständigen Eintreten der Gefährdung vergeht, definitiv ausreicht, um die erforderlichen Aufgaben durchzuführen und

- unabhängige Einrichtungen vorhanden sind, durch die das Risiko vom Bediener verhindert werden kann, oder
- es für alle Personen möglich ist, aus dem Gefährdungsbereich zu fliehen.

Der Parameter Pr nach Anhang A von EN 62061:2005 und der Parameter W nach EN 61511-3:2017 umfassen die Wahrscheinlichkeit des Auftretens des gefährlichen Prozesszustandes ohne die zu klassifizierende sicherheitsbezogene Funktion. Maßnahmen, die komplett unabhängig von der Sicherheitsfunktion zur Vermeidung dieses speziellen Risikos sind, können bei der Verringerung dieses Parameters berücksichtigt werden.

Die Ergebnisse der SIL/PL-Bestimmung müssen mit den getroffenen Entscheidungen und Rechtfertigungen schriftlich dokumentiert werden.

C.2 Beispiele für die Bestimmung des erforderlichen SIL/PL

C.2.1 Beispiel 1 – Tabelle C.1

Tabelle C.1 zeigt einen Vergleich der SIL/PL-Bestimmung in verschiedenen Risikoumgebungen nach Anhang A von EN 62061:2005 / EN ISO 13849-1:2015, Tabelle 4.

C.2.2 Beispiel 2 – Tabelle C.2

Tabelle C.2 zeigt einen Vergleich der SIL/PL-Bestimmung in verschiedenen Risikoumgebungen; Beispiel der SIL-Bestimmung nach EN 61511-3:2017.

**Tabelle C.1 — Vergleich der SIL/PL-Bestimmung in verschiedenen Risikoumgebungen nach EN 62061:2005 und
EN ISO 13849-1:2015, Tabelle 4**

Risikobeurteilung und Sicherheitsmaßnahmen										Dokumentennr.: Teil von:			
Projekt: Beispiel einer typischen SIL-Bestimmung													
Herausgegeben von:													
Datum:													
Überarbeitet:													
Schwarze Fläche = Sicherheitsmaßnahmen erforderlich Graue Fläche = Sicherheitsmaßnahmen empfohlen													
	Konsequenzen	Schweregrad	Klasse Cl					Häufigkeit und		Wahrscheinlichkeit der Gefährdung		Vermeidung	
		Se	3—4	5—7	8—10	11—13	14—15	Dauer, Fr		Ereignis, Pr		Av	
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 Stunde	5	Sehr hoch	5		
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3		> 1 Stunde - <= Tag	5	Wahrscheinlich	4		
Heilbar, ärztliche Behandlung	2			OM	SIL 1	SIL 2		> 1 Tag - <= 2 Wochen	4	Möglich	3	Unmöglich	5
Heilbar, erste Hilfe	1				OM	SIL 1		> 2 Wochen - <= 1 Jahr	3	Selten	2	Möglich	3
								> 1 Jahr	2	Vernachlässigbar	1	Wahrscheinlich	1

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen		Wahrscheinlichkeit des Eintretens			Klasse	Unversehrtheit		Erläuterungen
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Ein Temperaturfühler in Kombination mit einem Logiksystem überwacht die Prozesstemperatur. Wenn die Temperatur über ein sicheres Niveau steigt, muss sie in einen sicheren Zustand gebracht werden.		4	3	2	3	8	2 ^a	d	Umgebung mit geringerem Risiko Geringfügige Konsequenzen für wenige Personen, die gute Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.2.6/4.3.2.8, Automatische Absperrventile Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Ein Temperaturfühler in Kombination mit einem Logiksystem überwacht die Prozesstemperatur. Wenn die Temperatur über ein sicheres Niveau steigt, muss sie in einen sicheren Zustand gebracht werden.		4	5	2	3	10	2	d	Umgebung mit mittlerem Risiko Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.2.6/4.3.2.8, Automatische Absperrventile Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Ein Temperaturfühler in Kombination mit einem Logiksystem überwacht die Prozesstemperatur. Wenn die Temperatur über ein sicheres Niveau steigt, muss sie in einen sicheren Zustand gebracht werden.		4	5	3	3	11	3	e	Umgebung mit höherem Risiko Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können prEN 746-2:—, 4.2.2.6/4.3.2.8, Automatische Absperrventile Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen		Wahrscheinlichkeit des Eintretens			Klasse	Unversehrtheit		Erläuterungen
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
12	Verbrennungsluftdruck/-strom zu gering	Druckschalter, Druckgeber oder Durchflussmesser überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Druck/Strom unter ein sicheres Niveau fällt.		4	5	2	1	8	2	d	Umgebung mit geringerem Risiko Geringfügige Konsequenzen für wenige Personen, die gute Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.2/4.3.3.2, Strömungs- und Druckwächter für Verbrennungsluft Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
12	Verbrennungsluftdruck/-strom zu gering	Druckschalter, Druckgeber oder Durchflussmesser überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Druck/Strom unter ein sicheres Niveau fällt.		4	5	2	3	10	2	d	Umgebung mit mittlerem Risiko Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.2/4.3.3.2, Strömungs- und Druckwächter für Verbrennungsluft Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen		Wahrscheinlichkeit des Eintretens			Klasse	Unversehrtheit		Erläuterungen
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
12	Verbrennungsluftdruck/-strom zu gering	Druckschalter, Druckgeber oder Durchflussmesser überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Druck/Strom unter ein sicheres Niveau fällt.		4	5	3	3	11	3	e	Umgebung mit höherem Risiko Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können prEN 746-2:—, 4.2.3.2/4.3.3.2, Strömungs- und Druckwächter für Verbrennungsluft Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
13	Luft-/Gasregler außerhalb des sicheren Betriebsbereiches	Der korrekte Luft-/Gasregler wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Reglersensor kombiniert mit einem Logiksystem muss den Regler auf ein sicheres Niveau bringen.		4	2	3	5	10	2	d	Umgebung mit geringerem Risiko Geringfügige Konsequenzen für wenige Personen, die gute Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.3/4.3.3.3: Luft-Brennstoff-Verhältnis, Gefährdung: Explosion, Feuer, Vergiftung.
13	Luft-/Gasregler außerhalb des sicheren Betriebsbereiches	Der korrekte Luft-/Gasregler wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Reglersensor kombiniert mit einem Logiksystem muss den Regler auf ein sicheres Niveau bringen.		4	5	4	5	14	3	e	Umgebung mit mittlerem Risiko Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.3/4.3.3.3: Luft-Brennstoff-Verhältnis Gefährdungen: Explosion, Feuer, Vergiftung

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen		Wahrscheinlichkeit des Eintretens			Klasse	Unversehrtheit		Erläuterungen
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
13	Luft-/Gasregler außerhalb des sicheren Betriebsbereiches	Der korrekte Luft-/Gasregler wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Reglersensor kombiniert mit einem Logiksystem muss den Regler auf ein sicheres Niveau bringen.		4	5	5	5	15	3	e	Umgebung mit höherem Risiko Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.3/4.3.3.3: Luft-Brennstoff-Verhältnis Gefährdungen: Explosion, Feuer, Vergiftung
ANMERKUNG C.2.3 enthält eine Anleitung zu diesem Risikograph.											

Tabelle C.2 — Vergleich der SIL/PL-Bestimmung in verschiedenen Risikoumgebungen nach EN 61511

Projekt:		Beispiel einer typischen SIL-Bestimmung							Prozess:														
Heraus- gegeben von:									SIF:														
Datum:									Anlage:														
Überarbeitet									Risiko:														
Konsequenzparameter		Risikograph-Matrix							Belegungsparameter			Vermeidungsparameter			Anforderungsdatenparameter								
		Wahrscheinlichkeitssumme (F+P+W)							Häufigkeit der Präsenz von Menschen im Gefährdungsbereich. Eine begrenzte Belegung darf bei der Auswahl der Konsequenzkategorie nicht in Anspruch genommen worden sein!			Wahrscheinlichkeit der Vermeidung des Gefährdungsereignisses, wenn die SIF auf Anforderung ausfällt . Impliziert unabhängige Anlagen, die „abschalten“ sollen, so dass die Gefährdung vermieden oder alle Personen in einen sicheren Bereich fliehen können. Zu erfüllende Bedingungen: •Anlagen, die den Bediener alarmieren, dass die SIS ausgefallen ist •Unabhängige Anlagen, die den Prozess in einen sicheren Zustand versetzen •Die Zeit zwischen der Alarmierung des Bedieners und dem Gefährdungsereignis beträgt > 1 Stunde			Geschätzte SIF-Anforderungsrate			W					
															W ₉	Oft	> 1 / Jahr	9					
Schweregrad		C	1-2	3-4	5-6	7-8	9-10	11-12							W ₈			Häufig	1/1-3 Jahre	8			
C _F	Katastrophal	F	a	SIL 1	SIL 2	SIL 3	SIL 4	b							W ₇			Wahr-scheinlich	1/3-10 Jahre	7			
C _E	Umfangreich	E	OK	a	SIL 1	SIL 2	SIL 3	SIL 4							Expositionsrate		F	W ₆			Wahr-scheinlich	1/10-30 Jahre	6
C _D	Ernst	D	OK	OK	a	SIL 1	SIL 2	SIL 3							F _D	Dauer-belastung	100 %	2	W ₅			Gelegentlich	1/30-100 Jahre
C _C	Beträchtlich	C	OK	OK	OK	a	SIL 1	SIL 2	F _C	Häufig	10 % – 100 %	2	Vermeidungswahrscheinlichkeit		P	W ₄			Gering	1/100-300 Jahre	4		
C _B	Geringfügig	B	OK	OK	OK	OK	a	SIL 1	F _B	Gelegent-lich	1 % – 10 %	1	P _B	Vermeidungsbedingung nicht erfüllt		1	W ₃			Unwahr-scheinlich	1/300-1 000 Jahre	3	
C _A	Vernach-lässigbar	A	OK	OK	OK	OK	OK	a	F _A	Selten	<1%	0	P _A	Alle Vermeidungsbedin-gungen sind erfüllt		0	W ₂			Unglaublich	1/1 000-10 000 Jahre	2	

SIF	Gefährdungs- ereignis	Sicherheitstechnische Funktion (SIF)	Konsequenzen		Einfluss		Bedarf	Wahr- schein- lichkeit	Unver- sehrtheit		Gefährdungsbeschreibung und Kommentare
Nr.	Beschreibung	Beschreibung	Schaden	C	F	P	W	Summe	SIL	SIL	
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Ein Temperaturfühler in Kombination mit einem Logiksystem überwacht die Prozesstemperatur.	H	D	1	0	6	7	1	1	Erhebliche Konsequenzen für wenige Personen, die nicht rechtzeitig fliehen können prEN 746-2:—, 4.2.2.6/4.3.2.8: Automatische Absperrventile Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
		E	B	1	0	7		—			
		F	D			7		1			
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Ein Temperaturfühler in Kombination mit einem Logiksystem überwacht die Prozesstemperatur. Wenn die Temperatur über ein sicheres Niveau steigt, muss sie in einen sicheren Zustand gebracht werden.	H	D	2	1	6	9	2	2	Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.2.6/4.3.2.8: Automatische Absperrventile Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
			E	B	1	1		8	—		
			F	D				8	2		
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Ein Temperaturfühler in Kombination mit einem Logiksystem überwacht die Prozesstemperatur. Wenn die Temperatur über ein sicheres Niveau steigt, muss sie in einen sicheren Zustand gebracht werden.	H	D	2	1	7	10	2	2	Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können prEN 746-2:—, 4.2.2.6/4.3.2.8: Automatische Absperrventile Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
			E	B	1	1		9	a		
			F	D				9	2		

SIF	Gefährdungs- ereignis	Sicherheitstechnische Funktion (SIF)	Konsequenzen		Einfluss		Bedarf	Wahr- schein- lichkeit	Unver- sehrtheit		Gefährdungsbeschreibung und Kommentare
Nr.	Beschreibung	Beschreibung	Schaden	C	F	P	W	Summe	SIL	SIL	
12	Verbrennungsluft- druck/-strom zu gering	Druckschalter, Druckgeber oder Durchflussmesser überwacht den Luft- druck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Druck/Strom unter ein sicheres Niveau fällt.	H	D	1	0	6	7	1	2	Geringfügige Konsequenzen für wenige Personen, die gute Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.2/4.3.3.2: Strömungs- und Druckwächter für Verbrennungsluft Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
			E	B	1	0		7	—		
			F	E				7	2		
12	Verbrennungsluft- druck/-strom zu gering	Druckschalter, Druckgeber oder Durchflussmesser überwacht den Luft- druck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Druck/Strom unter ein sicheres Niveau fällt.	H	D	2	1	6	9	2	2	Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.2/4.3.3.2: Strömungs- und Druckwächter für Verbrennungsluft Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
			E	B	1	1		8	—		
			F	E				8	2		
12	Verbrennungsluft- druck/-strom zu gering	Druckschalter, Druckgeber oder Durchflussmesser überwacht den Luft- druck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Druck/Strom unter ein sicheres Niveau fällt.	H	E	2	1	6	9	3	3	Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können prEN 746-2:—, 4.2.3.2/4.3.3.2: Strömungs- und Druckwächter für Verbrennungsluft Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
			E	B	1	1		8	.		
			F	E				8	2		

SIF	Gefährdungs- ereignis	Sicherheitstechnische Funktion (SIF)	Konsequenzen		Einfluss		Bedarf	Wahr- schein- lichkeit	Unver- sehrtheit		Gefährdungsbeschreibung und Kommentare
Nr.	Beschreibung	Beschreibung	Schaden	C	F	P	W	Summe	SIL	SIL	
13	Luft-/Gasregler außerhalb des sicheren Betriebsbereiches	Der korrekte Luft-/Gasregler wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Reglersensor kombiniert mit einem Logiksystem muss den Regler auf ein sicheres Niveau bringen.	H	D	1	0	7	8	1	2	Geringfügige Konsequenzen für wenige Personen, die gute Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.3/4.3.3.3: Luft-Brennstoff-Verhältnis Gefährdungen: Explosion, Feuer, Vergiftung
			E	B	1	0		8	–		
			F	E				8	2		
13	Luft-/Gasregler außerhalb des sicheren Betriebsbereiches	Der korrekte Luft-/Gasregler wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Reglersensor kombiniert mit einem Logiksystem muss den Regler auf ein sicheres Niveau bringen.	H	D	2	1	7	10	2	3	Geringfügige Konsequenzen für wenige Personen, die angemessene Aussichten haben, rechtzeitig zu fliehen prEN 746-2:—, 4.2.3.3/4.3.3.3: Luft-Brennstoff-Verhältnis Gefährdungen: Explosion, Feuer, Vergiftung
			E	B	1	1		9	a		
			F	E				9	3		
13	Luft-/Gasregler außerhalb des sicheren Betriebsbereiches	Der korrekte Luft-/Gasregler wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Reglersensor kombiniert mit einem Logiksystem muss den Regler auf ein sicheres Niveau bringen.	H	E	2	1	7	10	3	3	Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können prEN 746-2:—, 4.2.3.3/4.3.3.3: Luft-Brennstoff-Verhältnis Gefährdungen: Explosion, Feuer, Vergiftung
			E	B	1	1		9	a		
			F	E				9	3		
ANMERKUNG C.2.4 enthält eine Anleitung zu diesem Risikograph.											

C.2.3 Risikoeinschätzung und SIL-Zuweisung in Übereinstimmung mit Anhang A von EN 62061:2005 (d. h. Tabelle C.1)

C.2.3.1 Gefährdungsbestimmung/-angabe

Gefährdungen, einschließlich solcher aus vernünftigerweise vorhersehbarer Fehlanwendung, deren Risiken durch Umsetzung einer SRCF vermindert werden sollen, sind anzugeben. Sie sind in der Gefährdungsspalte von Tabelle C.7 aufzulisten.

C.2.3.2 Risikoeinschätzung

Die Risikobeurteilung sollte für jede Gefährdung durch Bestimmung der Risikoparameter durchgeführt werden, die, wie in Bild C.1 gezeigt, aus dem Folgenden abgeleitet werden sollten:

- Schwere des Schadens, Se;
- Wahrscheinlichkeit des Eintretens des Schadens, der eine Funktion ist von
- Häufigkeit und Dauer der Exposition von Personen gegenüber der Gefährdung, Fr;
- Wahrscheinlichkeit des Eintretens eines Gefährdungsereignisses, Pr; und
- die Möglichkeiten zur Vermeidung oder Begrenzung des Schadens, Av.

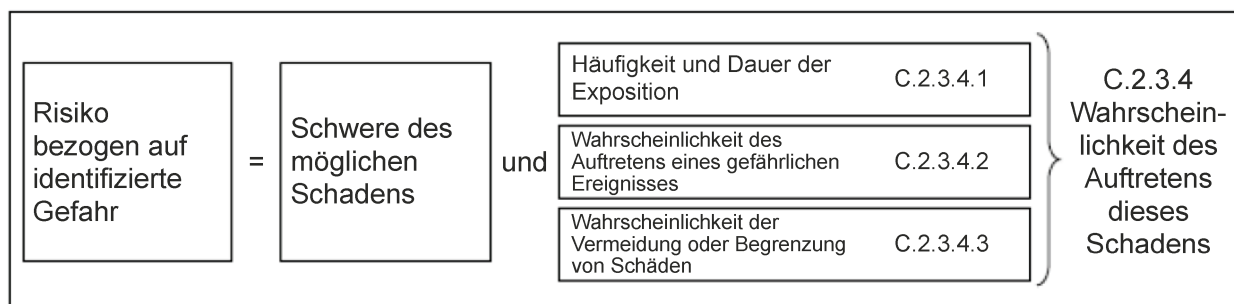


Bild C.1 — In der Risikoeinschätzung verwendete Parameter

Die in Tabelle C.7 verzeichneten Einschätzungen sollten normalerweise auf Grundlage von Betrachtungen der schlechtesten Fälle für die SRCF beruhen. Allerdings sollte in Situationen, in denen beispielsweise eine irreversible Verletzung möglich, aber deutlich unwahrscheinlicher als eine reversible ist, jeder Schweregrad über eine eigene Zeile in der Tabelle verfügen. Es kann der Fall sein, dass für jede Zeile eine andere SRCF eingesetzt wird. Falls eine SRCF zur Abdeckung von zwei Zeilen eingesetzt wird, sollte die höchste Ziel-SIL-Anforderung verwendet werden.

C.2.3.3 Schwere (Se)

Die Schwere von Verletzungen oder Gesundheitsschäden können durch Berücksichtigung reversibler, irreversibler oder tödlicher Verletzungen eingeschätzt werden. Der geeignete Wert der Schwere ist auf Grundlage der Folgen einer Verletzung aus Tabelle C.3 zu wählen, wobei:

- 4 bedeutet eine tödliche oder erhebliche, irreversible Verletzung derart, dass es sehr schwer sein wird, dieselbe Arbeit nach der Heilung auszuüben, falls dies überhaupt möglich ist;
- 3 bedeutet eine größere oder irreversible Verletzung derart, dass es möglich sein kann, nach der Heilung dieselbe Tätigkeit auszuüben. Dies kann auch schwere größere, jedoch reversible Verletzungen wie gebrochen Gliedmaßen beinhalten;

- 2 bedeutet eine reversible Verletzung, einschließlich schwerer Schnittwunden, Stiche und schweren Prellungen, die ärztliche Behandlung erfordert; und
- 1 bedeutet eine kleinere Verletzung, einschließlich Kratzern und kleineren Prellungen, die erste Hilfe erfordert.

Die entsprechende Reihe der Konsequenzen (Se) aus Tabelle C.3 ist zu wählen. Die entsprechende Nummer ist in der Se-Spalte in Tabelle C.7 einzutragen.

Tabelle C.3 — Schweregrad der Konsequenz – Gesundheitsgefährdung (H)

Konsequenzen	Schwere (Se)
Irreversibel: Tod, Verlust eines Arms oder Auges	4
Irreversibel: ein/mehrere gebrochene Gliedmaßen, Verlust eines/mehrerer Finger	3
Heilbar: ärztliche Behandlung erforderlich	2
Heilbar: erste Hilfe erforderlich	1

C.2.3.4 Wahrscheinlichkeit des Eintretens von Schäden

C.2.3.4.1 Allgemeines

Jeder der drei Parameter der Wahrscheinlichkeit des Eintretens von Schäden (d. h. Fr, Pr und Av) sollte unabhängig von den anderen eingeschätzt werden. Für jeden Parameter muss eine Annahme des schlechtesten Falls verwendet werden, um sicherzustellen, dass der/die SRCF nicht fälschlicherweise einem niedrigeren SIL als erforderlich zugewiesen werden. Allgemein wird die Verwendung einer Analyse auf Grundlage der Aufgaben dringend empfohlen, um sicherzustellen, dass der Einschätzung der Wahrscheinlichkeit des Eintretens von Schäden sachgemäße Berücksichtigung zuteil wird.

C.2.3.4.2 Häufigkeit und Dauer der Exposition

Zur Bestimmung des Expositionslevels sind die folgenden Aspekte zu berücksichtigen:

- Notwendigkeit des Zugangs zum Gefährdungsbereich in allen Nutzungsarten, beispielsweise Normalbetrieb, Wartung;
- Art des Zugriffs, z. B. manuelle Materialzufuhr, Einstellung.

Es sollte dann möglich sein, die durchschnittliche Dauer zwischen Expositionen und damit die durchschnittliche Häufigkeit des Zugangs abzuschätzen.

Es sollte außerdem möglich sein, die Dauer abzuschätzen, beispielsweise ob sie 10 min überschreitet. Wo die Dauer unter 10 min liegt, kann der Wert auf die nächste Stufe verringert werden. Dies gilt nicht für eine Häufigkeit der Exposition ≤ 1 h, die niemals verringert werden sollte.

ANMERKUNG Die Dauer hängt mit der Durchführung von Aktivitäten zusammen, die unter Schutz der SRCF stattfinden. Für größere Eingriffe sollten bezüglich der Isolierung der Spannungsversorgung und der Energiedissipation die Anforderungen der EN 60204-1:2018 und EN ISO 14118 angewandt werden.

Dieser Faktor beinhaltet nicht die Berücksichtigung des Ausfalls der SRCF.

Aus Tabelle C.4 muss die geeignete Reihe für Häufigkeit und Dauer der Exposition (Fr) gewählt werden. Die entsprechende Nummer ist in der Fr-Spalte in Tabelle C.7 einzutragen.

Tabelle C.4 — Einstufung der Häufigkeit und Dauer der Exposition (Fr)

Häufigkeit und Dauer der Exposition (Fr)	
Häufigkeit der Exposition	Dauer > 10 min.
≤ 1 Stunde	5
> 1 Stunde bis ≤ 1 Tag	5
> 1 Tag bis ≤ 2 Wochen	4
> 2 Wochen bis ≤ 1 Jahr	3
> 1 Jahr	2

C.2.3.4.3 Wahrscheinlichkeit des Eintretens eines Gefährdungsereignisses

Die Wahrscheinlichkeit des Eintretens von Schäden sollte unabhängig von anderen zugehörigen Parametern Fr und Av eingeschätzt werden. Für jeden Parameter sollte eine Annahme des schlechtesten Falls verwendet werden, um sicherzustellen, dass der/die SRCF nicht fälschlicherweise einem niedrigeren SIL als erforderlich zugewiesen werden. Um dies zu verhindern, wird die Verwendung einer Analyse auf Grundlage der Aufgaben dringend empfohlen, um sicherzustellen, dass der Einschätzung der Wahrscheinlichkeit des Eintretens von Schäden sachgemäße Berücksichtigung zuteil wird. Dieser Parameter kann durch Berücksichtigung des Folgenden geschätzt werden:

- a) der Vorhersagbarkeit des Verhaltens von Bauteilen der Maschine, die für die Gefährdung in verschiedenen Betriebsarten relevant sind (z. B. Normalbetrieb, Wartung, Fehlersuche).

Dies wird die sorgfältige Betrachtung des Steuerungssystems erforderlich machen, insbesondere hinsichtlich des Risikos des unerwarteten Anlaufens. Die Schutzwirkung jeglichen SRECS darf nicht berücksichtigt werden. Dies ist erforderlich, um die Größe des Risikos, dem Personen ausgesetzt sind, einzuschätzen, wenn das SRECS ausfällt. Im Allgemeinen muss berücksichtigt werden, ob die Maschine oder verarbeitetes Material die Tendenz zu unerwartetem Verhalten hat.

Das Verhalten der Maschine wird von sehr vorhersehbar bis nicht vorhersehbar schwanken, jedoch können unerwartete Ereignisse nicht unberücksichtigt gelassen werden.

ANMERKUNG Vorhersehbarkeit wird oft mit der Komplexität der Funktion der Maschine verbunden.

- b) Die angegebenen oder vorhersehbaren Eigenschaften des menschlichen Verhaltens hinsichtlich der Interaktion mit den Bauteilen der Maschine, die für die Gefährdung relevant sind. Dies kann beschrieben werden durch

- Stress (z. B. wegen Zeitmangel, Arbeitsaufgabe, wahrgenommene Schadensbegrenzung) und/oder
- mangelhafte Bekanntheit der für die Gefährdung relevanten Informationen. Dies wird durch Faktoren wie Fertigkeiten, Schulung, Erfahrung und Komplexität der Maschine/des Verfahrens beeinflusst.

Diese Merkmale sind normalerweise nicht direkt vom SRECS-Konstrukteur beeinflussbar, jedoch wird eine Aufgabenanalyse Aktivitäten aufdecken, für die die völlige Bekanntheit aller Probleme, einschließlich unerwarteter Ergebnisse, vernünftigerweise nicht angenommen werden kann.

„Sehr hohe“ Wahrscheinlichkeit des Eintretens eines Gefährdungsereignisses sollte gewählt werden, um normale Produktionsbeschränkungen und Annahmen schlechtester Fälle zu reflektieren. Für die Verwendung jeglicher geringerer Werte sind positive Gründe (z. B. gut definierte Anwendung und sehr hohe Fachkenntnis der Anwender) erforderlich.

Jegliche erforderliche oder angenommene Fähigkeiten, Fachwissen, usw. sollten in der Benutzerinformation genannt sein.

Aus Tabelle C.5 muss die geeignete Reihe für die Wahrscheinlichkeit des Eintretens von Gefährdungsereignissen (Pr) gewählt werden. Die entsprechende Nummer ist in der Pr-Spalte in Tabelle C.7 einzutragen.

Tabelle C.5 —Einstufung der Wahrscheinlichkeit (Pr)

Wahrscheinlichkeit des Eintretens	Wahrscheinlichkeit (Pr)
Sehr hoch	5
Wahrscheinlich	4
Möglich	3
Selten	2
Vernachlässigbar	1

C.2.3.4.4 Wahrscheinlichkeit der Vermeidung oder Beschränkung des Schadens (Av)

Dieser Parameter kann durch Berücksichtigung von Aspekten der Auslegung der Maschine und ihrer vorgesehenen Anwendung eingeschätzt werden, die helfen können, den Schaden aus einer Gefährdung zu vermeiden oder zu begrenzen. Diese Aspekte beinhalten beispielsweise:

- plötzliche, schnelle oder langsame Geschwindigkeit des Auftretens des Gefährdungsereignisses;
- Möglichkeit, sich räumlich von der Gefährdung zu entfernen;
- die Eigenart des Bauteils oder Systems, beispielsweise ist ein Messer üblicherweise scharf, ein Rohr in einer Molkerei normalerweise heiß, Elektrizität normalerweise von sich aus gefährlich aber nicht sichtbar; und
- die Wahrscheinlichkeit, eine Gefährdung zu erkennen, beispielsweise eine elektrische Gefährdung: eine Kupferstange ändert ihre Erscheinung nicht, ob sie unter Spannung steht oder nicht; um zu erkennen, ob ein Messgerät erforderlich ist, um festzustellen, ob elektrische Ausrüstung Spannung führt oder nicht; Umgebungsbedingungen, beispielsweise können hohe Lärmpegel verhindern, dass eine Person das Anlaufen einer Maschine hört.

Aus Tabelle C.6 muss die geeignete Reihe für die Vermeidung oder Begrenzung von Schäden (Av) gewählt werden. Die entsprechende Nummer ist in der Av-Spalte in Tabelle C.7 einzutragen.

Tabelle C.6 — Einstufung der Wahrscheinlichkeit der Vermeidung oder Beschränkung des Schadens (Av)

Wahrscheinlichkeit der Vermeidung oder Beschränkung des Schadens (Av)	
Unmöglich	5
Selten	3
Wahrscheinlich	1

C.2.3.5 Klasse der Schadenswahrscheinlichkeit (Cl)

Für jede Gefährdung und ggf. für jeden Schweregrad sind die Punkte aus den Spalten Fr, Pr und Av zu addieren und die Summe ist in die Spalte Cl in Tabelle C.7 einzutragen.

Tabelle C.7 — Parameter, die zur Bestimmung der Klasse der Schadenswahrscheinlichkeit (Cl) verwendet werden

Serienr.	Gefährdung	Se	Fr	Pr	Av	Cl
1						
2						
3						
4						

C.2.3.6 SIL-Zuweisung

In Tabelle C.8 zeigt der Schnittpunkt der Reihe für Schwere (Se) mit der entsprechenden Spalte (Cl) an, ob Maßnahmen erforderlich sind. Die Kästen zeigen den SIL x an, der als Zielwert für die SRCF zugewiesen ist. Die Kästen, die (OM) angeben, sollten als Empfehlungen verwendet werden, andere Maßnahmen (en: Other Measures, OM) zu verwenden.

Tabelle C.8 — Matrix der SIL-Zuweisung

Schwere (Se)	Klasse Cl				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

BEISPIEL Für eine spezielle Gefährdung mit Se gleich 3, Fr gleich 4, Pr gleich 5 und Av gleich 5 ergibt sich

$$Cl = Fr + Pr + Av = 4 + 5 + 5 = 14$$

Dies würde unter Anwendung von Tabelle C.8 dazu führen, dass der SRCF, die diese spezielle Gefährdung mindern soll, SIL 3 zugewiesen werden würde.

C.2.4 Benutzer-Richtlinie für den Risikograph in Übereinstimmung mit EN61511-3:2017 (d. h. Tabelle C.2)

C.2.4.1 Allgemeines

Die Risikograph-Matrix in Übereinstimmung mit EN 61511-3:2017 wird für die SIL-Zuweisung sicherheitstechnischer Funktionen verwendet. Integritätslevel werden durch die Kombination des Konsequenzparameters C des Risikographen und der Wahrscheinlichkeit, die als die Risikographenparameter F, P und W zusammengefasst ist, festgelegt. Individuelle Integritätslevel für Gesundheits- (H), Umwelt- (E) und finanzielle (F) Gefährdungen können bestimmt werden. Der allgemeine Ziel-SIL der betrachteten sicherheitstechnischen Funktion (SIF) ist der maximal bestimmte Integritätslevel.

C.2.4.2 Auswahl des Konsequenzparameters

Der Konsequenzparameter stellt die Anzahl der Todesfälle und/oder schweren Verletzungen dar, die sich aus dem Auftreten des Gefährdungsereignisses ergeben. Er wird durch Berechnung der Anzahl der Personen im exponierten Bereich berechnet, wenn der Bereich belegt ist, wobei die Anfälligkeit gegenüber dem Gefährdungsereignis berücksichtigt wird.

Der Schweregrad (C) ist die geschätzte Konsequenz des Gefährdungsereignisses. Die angemessenen Level für Gesundheits- (H), Umwelt- (E) und finanzielle (F) Gefährdungen sind auszuwählen. Den gewählten Schwere-Buchstaben (A bis F) für jede einzelne Gefährdung in Spalte C eintragen.

ANMERKUNG Die Bestimmung angemessener Schweregrade setzt voraus, dass die Konsequenzkategorien so kalibriert sind, dass sie den vom Risikomanagement des Unternehmens und von den Behörden festgelegten tolerierbaren Risikoniveaus entsprechen.

Siehe Tabelle C.9, C.10 und C.11 für Einzelheiten zum Schweregrad von Konsequenzen.

Tabelle C.9 — Schweregrad der Konsequenz – Gesundheitsgefährdung (H)

C	Gesundheits- gefährdung (H)	Wahrschein- lichkeit von Todesfällen	Max. Gesundheitskonse- quenzen aufgrund des Gefährdungsereignisses	Zusätzliche Kommentare zu den Kategorien der Gesundheits- konsequenzen
C _F	Katastrophal	PLL > 1	Mehrere (drei oder mehr) Tote. Viele (10 oder mehr) Schwerverletzte.	Mehrere Todesfälle wahrscheinlich.
C _E	Umfangreich	PLL = 0,1—1,0	Einige (ein oder zwei) Tote. Mehrere (drei oder mehr) Schwerverletzte.	Einzelner Todesfall/Todesfälle wahrscheinlich.
C _D	Ernst	PLL = 0,01—0,1	Einige (ein oder zwei) Schwerverletzte. Mehrere (3 oder mehr) Verletzte.	Mehrere verletzungsbedingte Ausfallzeiten. Eine oder einige dauerhafte Behinderungen. Todesfall/Todesfälle nicht wahrscheinlich, aber möglich.
C _C	Beträchtlich	PLL < 0,01	Einige (ein oder zwei) Verletzte. Schwerwiegende Unannehmlichkeiten.	Eine oder einige verletzungsbedingte Ausfallzeiten. Geringe Wahrscheinlichkeit dauerhafter Behinderung. Todesfall unwahrscheinlich.
C _B	Geringfügig	PLL = 0	Leichte Verletzung/Verletzungen. Dauerhafte Unannehmlichkeiten.	Keine verletzungsbedingten Ausfallzeiten. Ärztliche Behandlung erforderlich.
C _A	Vernach- lässigbar	PLL = 0	Vernachlässigbare Verletzung/Verletzungen. Zeitweilige Unannehmlichkeiten.	Keine verletzungsbedingten Ausfallzeiten. Keine ärztliche Behandlung erforderlich.
ANMERKUNG C: Schweregrad				

Tabelle C.10 — Schweregrad der Konsequenz – Umweltgefährdung (E)

C	Umwelt- gefährdung (E)	Abwasser- einfluss	Abwasser- ausdeh- nung	Max. Umweltkonse- quenzen aufgrund des Gefährdungs- ereignisses	Zusätzliche Kommentare zu den Kategorien der Umwelt- konsequenzen
C _F	Katastrophal	Dauerhaft	Breit- gefächert	Breitgefächerte permanente oder langfristige Gefährdung. Dekontamination unmöglich oder schwierig.	Ein Flüssigkeitsaustritt in einen Fluss oder die See. Eine breitgefächerte Freisetzung von Dampf oder Aerosol. Das Abwasser erzeugt dauerhafte oder permanente Schäden an Pflanzen und Tieren.
C _E	Umfangreich	Dauerhaft	Begrenzt	Begrenzte permanente oder langfristige Gefährdung. Dekontamination unmöglich oder schwierig.	Ein Flüssigkeitsaustritt in Grundwasser. Eine begrenzte Freisetzung von Dampf oder Aerosol. Das Abwasser erzeugt dauerhafte oder permanente Schäden an Pflanzen und Tieren.
C _D	Ernst	Dauerhaft	Einge- schränkt	Eingeschränkte permanente oder langfristige Gefährdung. Dekontamination unmöglich oder schwierig.	Flüssigkeitsaustritt am Standort. Eine eingeschränkte Freisetzung von Dampf oder Aerosol (eingezaunt). Das Abwasser erzeugt dauerhafte oder permanente Schäden an Pflanzen und Tieren.
C _C	Beträchtlich	Befristet	Breit- gefächert/ Begrenzt	Breitgefächerte bis begrenzte zeitweilige Gefährdung. Dekontamination leicht oder nicht erforderlich.	Ein Flüssigkeitsaustritt in einen Fluss oder die See. Eine eingeschränkte Freisetzung von Dampf oder Aerosol. Das Abwasser erzeugt zeitweilige Schäden an Pflanzen und Tieren.
C _B	Geringfügig	Befristet	Einge- schränkt	Eingeschränkte zeitweilige Gefährdung (am Standort). Dekontamination leicht oder nicht erforderlich.	Flüssigkeitsaustritt am Standort. Eine eingeschränkte Freisetzung von Dampf oder Aerosol (eingezaunt). Das Abwasser erzeugt zeitweilige Schäden an Pflanzen und Tieren.
C _A	Vernach- lässigbar	Vernach- lässigbar		Vernachlässigbare Umweltgefährdung. Dekontamination nicht erforderlich.	Mäßiges Leck an einem Flansch oder Ventil. Geringer Flüssigkeitsaustritt oder geringe Bodenverschmutzung ohne Auswirkungen auf Grundwasser. Vernachlässigbare Umweltauswirkungen.
ANMERKUNG C: Schweregrad					