

DIN EN ISO 13577-4

ICS 13.100; 25.180.01

Einsprüche bis 2021-11-24

Entwurf

**Industrielle Thermoprozessanlagen und dazugehörige
Prozesskomponenten –
Sicherheitsanforderungen –
Teil 4: Schutzsysteme (ISO/DIS 13577-4:2021);
Deutsche und Englische Fassung prEN ISO 13577-4:2021**

Industrial furnaces and associated processing equipment –
Safety –

Part 4: Protective systems (ISO/DIS 13577-4:2021);
German and English version prEN ISO 13577-4:2021

Fours industriels et équipements associés –
Sécurité –

Partie 4: Systèmes de protection (ISO/DIS 13577-4:2021);
Version allemande et anglaise prEN ISO 13577-4:2021

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-09-24 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@vdma.org 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 oder 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 189 Seiten

DIN-Normenausschuss Maschinenbau (NAM)
DIN-Normenausschuss Gastechnik (NAGas)

Nationales Vorwort

Dieser Norm-Entwurf enthält sicherheitstechnische Festlegungen.

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.

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

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 13849-1	siehe	DIN EN ISO 13849-1
IEC 60947-4-1	siehe	DIN EN IEC 60947-4-1

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

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO 13850, *Sicherheit von Maschinen — Not-Halt-Funktion — Gestaltungsleitsätze (ISO 13850:2015)*

DIN EN ISO 14118, *Sicherheit von Maschinen — Vermeidung von unerwartetem Anlauf (ISO 14118:2017)*

DIN EN ISO/IEC 17025, *Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien (ISO/IEC 17025:2017)*

<i>Titel de:</i>	Industrielle Thermoprozessanlagen und dazugehörige Prozesskomponenten — Sicherheitsanforderungen — Teil 4: Schutzsysteme (ISO/DIS 13577-4:2021)
<i>Titel en:</i>	Industrial furnaces and associated processing equipment — Safety — Part 4: Protective systems (ISO/DIS 13577-4:2021)
<i>Titel fr:</i>	Fours industriels et équipements associés — Sécurité — Partie 4: Systèmes de protection (ISO/DIS 13577-4:2021)

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	8
4 Anforderungen an die Gestaltung von Anlageteilen in einem Schutzsystem	10
4.1 Allgemeines	10
4.2 Anforderungen an Schutzsysteme	12
4.2.1 Übersicht der Verfahren	12
4.2.2 Verfahren A	13
4.2.3 Verfahren BC	14
4.2.4 Verfahren D	16
4.3 Fehlerbetrachtung für den verkabelten Teil von Schutzsystemen	18
4.4 Ausfall von Versorgungseinrichtungen	18
4.5 Rücksetzen	18
5 Benutzerinformationen	19
Anhang A (informativ) Erläuterung der Techniken und Maßnahmen zur Vermeidung systematischer Fehler	20
A.1 Allgemeines	20
A.2 Kompetenzen	20
A.3 Vermeidung systematischer Fehler	21
Anhang B (normativ) Verkabelung von Schutzsystemen	22
B.1 Allgemeines	22
B.2 Schutz vor Fehlern des Schutzsystems	22
B.3 Maßnahmen zur Vermeidung von Fehlern	23
B.4 Hardwareauslegung	23
B.4.1 Allgemeine Anforderungen an die Hardware	23
B.4.2 Verdrahteter Teil eines Schutzsystems	23
B.5 Ordnungsgemäße Eingangsverkabelung	26
B.6 Ordnungsgemäße Ausgangsverkabelung	29
B.7 Unsachgemäße Eingangs- und Ausgangsverkabelung	31
Anhang C (informativ) Beispiele für die Bestimmung des Sicherheits-Integritäts- oder Performance Level SIL/PL mittels des Risikograph-Verfahrens	36
C.1 Allgemeines	36
C.2 Beispiele für die Bestimmung des erforderlichen SIL/PL	37
C.2.1 Beispiel 1 - Tabelle C.1	37
C.2.2 Beispiel 2 - Tabelle C.2	37
C.2.3 Risikoeinschätzung und SIL-Zuweisung in Übereinstimmung mit IEC 62061:2021, Anhang A (d. h. Tabelle C.1)	48
C.2.4 Benutzer-Anleitung für den Risikograph in Übereinstimmung mit IEC 61511-3:2016 (d. h. Tabelle C.2)	53

Anhang D (informativ) Beispiel für eine erweiterte Risikobeurteilung für eine sicherheitstechnische Funktion mittels des Verfahrens nach IEC 61511:2016.....	59
D.1 Allgemeines	59
D.2 Konzeptbeschreibung der gesteuerten Ausrüstung.....	59
D.3 Gefährdungs- und Risikobeurteilung.....	60
D.3.1 Auslösende Ereignisse	60
D.3.2 Gefährdung – Prozessabweichung – unzureichende Verbrennungsluft	60
D.4 Konsequenzen	60
D.5 Beispiel eines Ereignisbaums	61
D.6 Sicherheitsanforderungsspezifikation des Schutzsystems.....	61
D.6.1 Allgemeine Anforderungen	61
D.6.2 Funktionale Anforderungen an Sicherheitssensoren.....	63
D.6.3 Anforderungen an das Logiksystem, einschließlich Alarm, externem Vergleich und HMI.....	64
D.6.4 Anforderungen an den Akteur	65
D.6.5 Anforderungen an manuelle Eingriffe	66
D.6.6 Anforderungen an den Anlauf	66
Anhang E (informativ) Beispiele für Schutzfunktionen	67
E.1 Einleitung	67
E.2 Beispiele für Unterfunktionen.....	73
E.2.1 Übersicht über die verschiedenen Anforderungen an die Eingangsunterfunktionen	73
E.3 Beispiele für Sicherheitsfunktionen.....	77
Anhang F (informativ) Begriffe, die für ISO 13577-4 relevant sind, sind in ISO 13574:2015 aufgeführt.....	92
F.1 Liste der Begriffe	92
F.2 Ausgeschlossene Begriffe, die in ISO 13574:2015 aufgeführt sind.....	93
Anhang G (normativ) Anforderungen an Anwendungssoftware	94
Literaturhinweise.....	96

Europäisches Vorwort

Dieses Dokument (prEN ISO 13577-4:2021) wurde vom Technischen Komitee ISO/TC 244 „Industrial furnaces and associated processing equipment“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 186 „Thermoprozesstechnik – Sicherheit“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Anerkennungsnotiz

Der Text von ISO/DIS 13577-4:2021 wurde von CEN als prEN ISO 13577-4:2021 ohne irgendeine Abänderung genehmigt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 244, *Industrial furnaces and associated processing equipment*, erarbeitet.

ISO 13577 besteht unter dem allgemeinen Titel *Industrial furnaces and associated processing equipment — Safety* aus den folgenden Teilen:

- *Part 1: General requirements*
- *Part 2: Combustion and fuel handling systems*
- *Part 3: Generation and use of protective and reactive atmosphere gases*
- *Part 4: Protective systems*

Einleitung

Dieser Teil von ISO 13577 wurde entwickelt, um Anforderungen an ein Schutzsystem festzulegen, bei dem es sich um eine sicherheitsbezogene Steuerung (SCS) für industrielle Öfen und zugehörige Prozesskomponenten (TPE) handelt. Es ist vorgesehen, dass die Hersteller von TPE bei der Auslegung der TPE eine Auswahl zwischen den drei Verfahren treffen, die in diesem Teil von ISO 13577 festgelegt werden. Obligatorische sicherheitsbezogene Steuerungen von TPE werden in den anderen Teilen von ISO 13577 (d. h. ISO 13577-1, ISO 13577-2, und ISO 13577-3) behandelt.

Dieser Teil von ISO 13577 ist als wesentlicher Teil der anderen Teile von ISO 13577 zu verwenden. Da andere Teile von ISO 13577 Typ-C-Normen von ISO 12100 sind, müssen TPE in Übereinstimmung mit den Grundsätzen von ISO 12100 ausgelegt werden. Die Typ-B-Normen von ISO 12100 für SCS sind IEC 62061 oder ISO 13849-1, in denen immer von Anwendungen mit hohem Bedarf ausgegangen wird. Allerdings gibt es Fälle, in denen eine Risikobeurteilung nach IEC 61511 (alle Teile), die die Möglichkeit einer geringen Bedarfsrate am Schutzsystem enthält, für die Auslegung eines TPE-Schutzsystems geeigneter ist.

Grundsätzlich, wenn die Anforderungen der anderen Teile von ISO 13577 (Typ-C-Normen) von den in Typ-A- oder Typ-B-Normen festgelegten abweichen, haben die Anforderungen dieser Typ-C-Normen bei Maschinen, die nach den Anforderungen dieser Typ-C-Norm gestaltet und gebaut wurden, Vorrang gegenüber den Anforderungen in anderen Normen. Daher gestattet dieser Teil von ISO 13577 eine erweiterte Risikobeurteilung für SRECS, in der alternativ eine Risikobeurteilung nach IEC 61511 (alle Teile) gewählt werden kann.

1 Anwendungsbereich

Dieser Teil von ISO 13577 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 von ISO 13577 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).

ISO 13574:2015, *Industrial furnaces and associated processing equipment — Vocabulary*

ISO 13849-1:—¹, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

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

IEC 60947-5-1:2016, *Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices*

IEC 60204-1:2016, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020, *CSV, Automatic electrical controls for household and similar use — Part 2-5: Particular requirements for automatic electrical burner control systems*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

1 Die Ausgabe 4 von ISO 13849-1 befindet sich in der Entwicklung und soll im Jahr 2022 erscheinen.

IEC 61131-3:2013, *Programmable controllers — Part 3: Programming languages*

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

IEC 61511-2:2016, *Functional safety — Safety instrumented systems for the process industry sector — Part 2: Guidelines for the application of IEC 61511-1:2016*

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 62061:2021, *Safety of machinery — Functional safety of safety-related control systems*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 13574:2015 und die folgenden Begriffe. Anhang F enthält Kopien der Definitionen aus ISO 13574, die in diesem Dokument verwendet werden.

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: IEC 61511-1:2003, 3.2.24, modifiziert: „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: ISO 13574:2015, 2.65, modifiziert: Der zweite Satz der ursprünglichen Definition wurde in die Anmerkung 1 zum Begriff übertragen.]

3.3

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 ausgeführt.

[QUELLE: IEC 61511-1:2003, 3.2.39, modifiziert — in der Beschreibung wurde „Eingangsfunktionen“ zu „Eingangsinformationen und Sensoren“ und „Ausgangsfunktionen“ zu „Ausgangsfunktionen oder Aktoren“ geändert, der zweite Satz der ursprünglichen Beschreibung wurde gestrichen und die Anmerkung wurde hinzugefügt.]

3.4

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: IEC 61511-1:2003, 3.2.40, modifiziert: „eines BPCS oder einer SIS“ wurde in der Definition zu „eines Schutzsystems“ geändert und ANMERKUNG 1 der ursprünglichen Definition wurde gestrichen.]

3.5

speicherprogrammierbare Steuerung

SPS

digitales elektronisches Betriebssystem, entwickelt für den Einsatz in einer industriellen Umgebung, das einen programmierbaren Speicher für die interne Speicherung von benutzerorientierten Anweisungen verwendet, um spezifische Funktionen wie Logik, Sequenzierung, Zeitsteuerung, Zählen und Arithmetik zu implementieren, um über digitale und analoge Ein- und Ausgaben verschiedene Arten von Maschinen oder Prozessen zu steuern

[QUELLE: IEC 61131-1:2003]

3.6

Schutzsystem

instrumentiertes System, das zur Implementierung einer oder mehrerer sicherheitsbezogener Funktion(en) eingesetzt wird und aus einer Kombination von Sensor(en), Logiksystem(en) und Aktoren besteht (Bild 2 enthält ein Beispiel)

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

[QUELLE: ISO 13574:2015, 2.138, modifiziert: Anmerkung 1 zum Begriff wurde in die Definition eingefügt.]

3.7

Sicherheitsbus

Bussystem und/oder Protokoll für digitale Netzwerkkommunikation zwischen Sicherheitskomponenten, um einen sicheren Zustand des Schutzsystems gemäß IEC 61508 (alle Teile):2010 oder IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020 CSV zu erreichen oder beizubehalten

[QUELLE: ISO 13574:2015, 2.164, modifiziert: Die referenzierten Normen wurden in datierte Normen geändert.]

3.8

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.

3.9

Sensor

Einrichtung, die auf Basis einer Prozessvariable ein Signal erzeugt

BEISPIEL Sender, Aufnehmer, Prozessschalter und Positionsschalter.

3.10

System für Dauerbetrieb

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

[QUELLE: IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020 CSV, 2.5.101]

3.11

System für intermittierenden Betrieb

System, das für eine Verweildauer von weniger als 24 h in der Betriebsposition vorgesehen ist

[QUELLE: IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020 CSV, 2.5.102]

4 Anforderungen an die Gestaltung von Anlageteilen in einem Schutzsystem

4.1 Allgemeines

Elektrische Installationen und Ausrüstung müssen den Anforderungen der IEC 60204-1:2016 entsprechen und den vorgesehenen Betriebsbeanspruchungen sowie den äußeren Einflüssen und Gefahren standhalten, die in der in der Auslegungsphase erforderlichen Risikobeurteilung ermittelt wurden. Die elektrische Installation und Ausrüstung müssen gegen Beschädigung geschützt werden. Insbesondere muss sie gegen Beschädigungen während des Dauerbetriebs widerstandsfähig sein.

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

Einrichtungen eines Schutzsystems müssen den Umgebungsbedingungen nach IEC 60204-1:2016, 4.4 widerstehen und ihre vorgesehene Funktion erfüllen.

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

ANMERKUNG 1 Angaben zum Betrieb können ausgetauscht werden, ohne die funktionale Sicherheit des Schutzsystems zu beeinträchtigen.

Der sichere Zustand darf nur durch spannungsfreie Stromkreise realisiert werden.

Die Anforderungen an die funktionale Sicherheit, wie sie in ISO 13577 (alle Teile) festgelegt sind, müssen in Übereinstimmung mit den Normen IEC 61508 (alle Teile):2010, IEC 61511 (alle Teile):2016, IEC 62061:2021 oder ISO 13849-1:—², wie zutreffend, sein und mit dem erforderlichen SIL/PL für jede Funktion umgesetzt werden.

Für die Bestimmung des Performance Levels einer Sicherheitsfunktion nach ISO 13849-1:— ist das alternative Verfahren nach ISO 13849-1:—, 6.1.9 nicht zulässig.

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

² Die Ausgabe 4 von ISO 13849-1 befindet sich in der Entwicklung und soll im Jahr 2022 erscheinen.

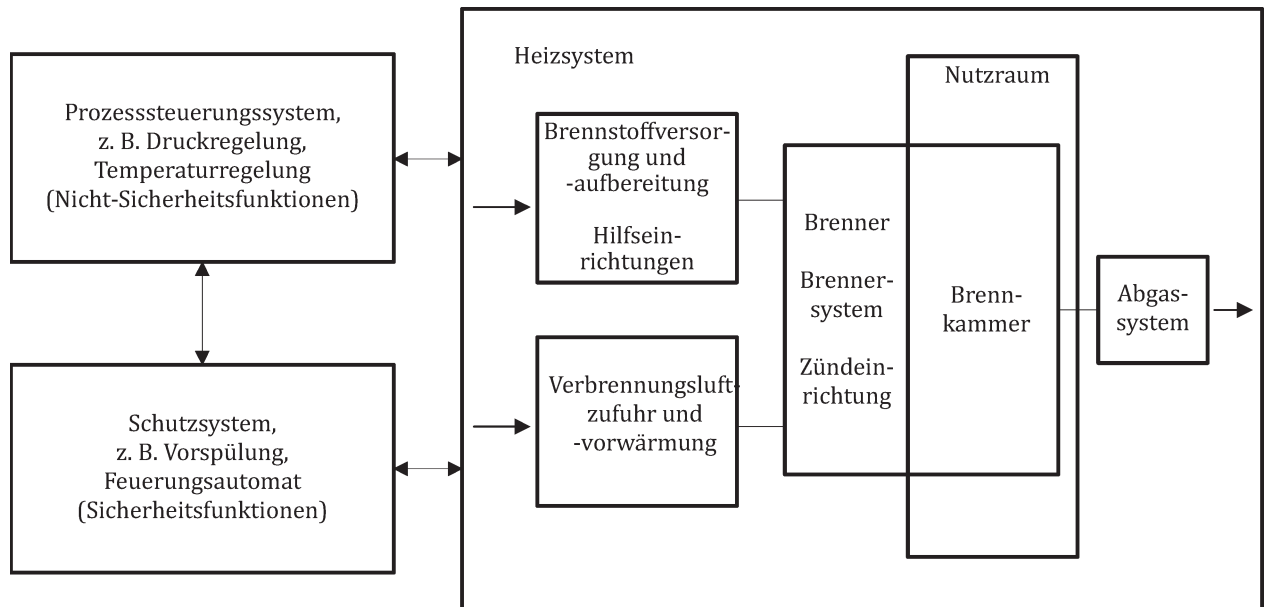


Bild 1 — Blockdiagramm der Steuer- und Schutzsysteme

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

Ausfälle durch Kurzschluss in der externen Verkabelung müssen vermieden werden (siehe B.5 und Bild B.10).

Die Verkabelung von sicherheitsrelevanten Sensoren und Stellteilen, die Teil eines Schutzsystems sind, erfolgt in der Regel vor Ort, außerhalb von Schaltschränken. Kurz-, Quer- und Erdschlüsse in dieser Feldverkabelung können zu sicherheitskritischen Fehlern im gesamten Schutzsystem führen. Kabelschleifen zum Anschluss von Feldeinrichtungen müssen in geeigneter Weise verlegt und befestigt werden, um eine Beschädigung der Kabel zu verhindern.

Um das gesamte Schutzsystem in einem sicheren Zustand zu halten, muss die Feldverkabelung von sicherheitsrelevanten Sensoren und Stellteilen (z. B. Druckschalter, Gasventile usw.) gegen mechanische Beschädigung (auch z. B. durch Vibration oder Knicken) geschützt werden, um Kurz-, Quer- und Erdschlüsse zu vermeiden.

ANMERKUNG 2 Ein Verfahren zum Schutz vor Kurz-, Quer- und Erdschlüssen ist die Verwendung von Kabelkanälen, Kabelrinnen oder Leerrohren für die Feldverkabelung.

Wenn das Schutzsystem in nicht geerdeten, isolierten Netzen betrieben wird, muss eine Isolationsüberwachungseinrichtung vorgesehen werden. Diese Isolationsüberwachungseinrichtung muss bei der ersten Fehlererkennung sofort alle Pole des Schutzsystems vom Netz trennen.

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 Anhang D für Beispiele für SIL/PL-Bestimmungen.

4.2 Anforderungen an Schutzsysteme

4.2.1 Übersicht der Verfahren

Jedes oder eine Kombination der drei (3) Verfahren muss zur Implementierung eines Schutzsystems für die in ISO 13577 (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 drei Verfahren:

- Verfahren A, wie in 4.2.2 festgelegt;
- Verfahren BC, wie in 4.2.3 festgelegt;
- Verfahren D, wie in 4.2.4 festgelegt.

Bild 2 zeigt die grundlegende Konfiguration eines Schutzsystems.

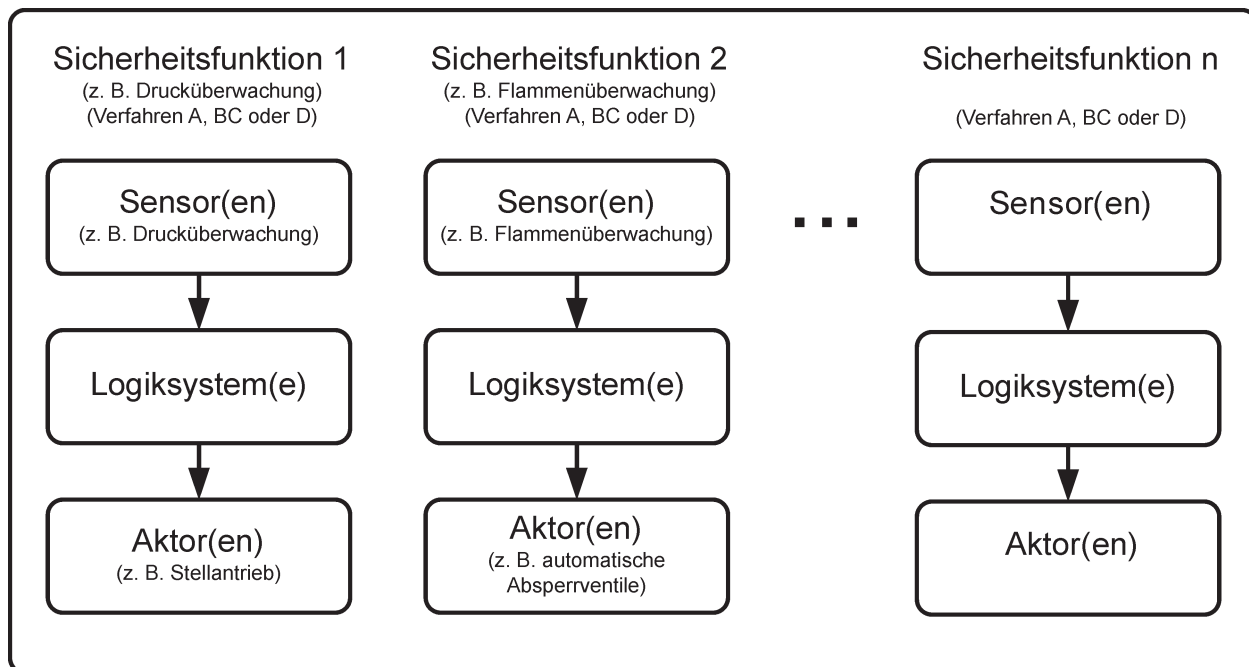


Bild 2 — Grundlegende Konfiguration eines Schutzsystems

Bild 3 zeigt die grundlegenden Eigenschaften der einzelnen Verfahren.

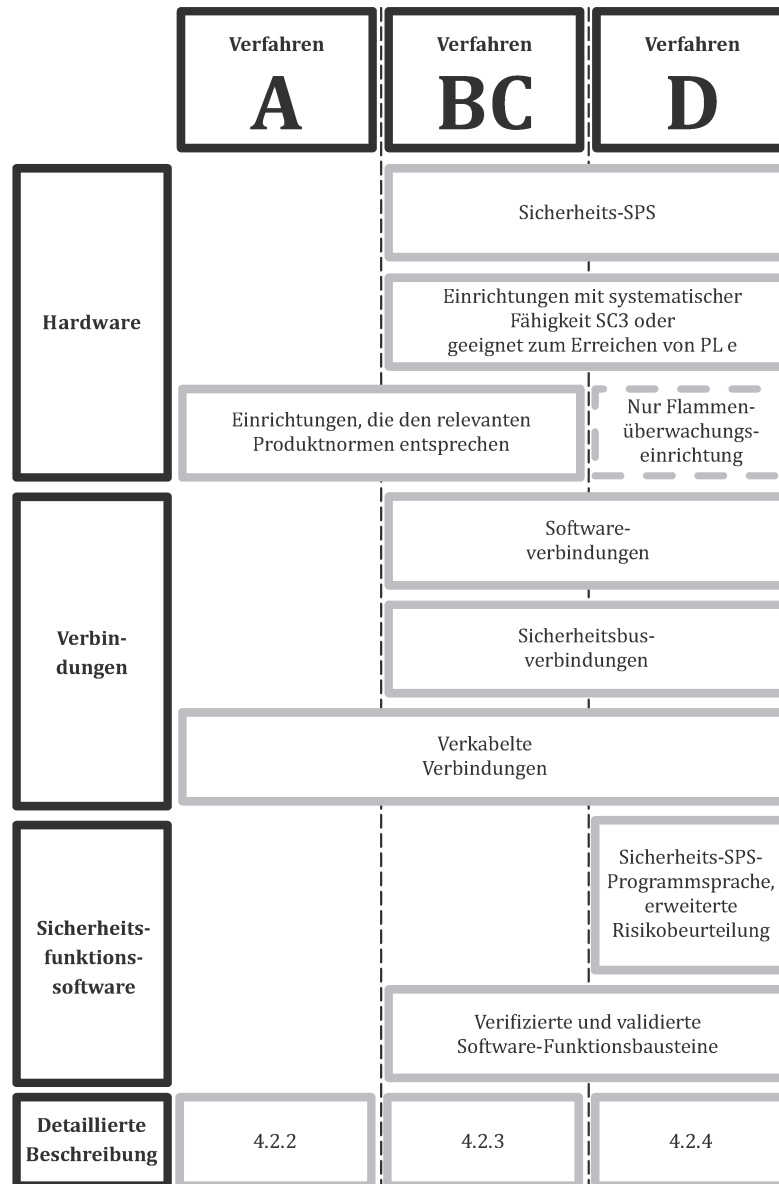


Bild 3 — Überblick über die Verfahren

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

ANMERKUNG 2 Die Sicherheitsfunktionssoftware ist entweder ein Software-Funktionsbaustein oder ein Programm zur Ausführung von Sicherheitslogikfunktionen (z. B. Vorspülung, Feuerungsautomat). Siehe 4.2.2.1.

Zu Beispielen für Schutzfunktionen der verschiedenen Verfahren siehe Anhang E.

4.2.2 Verfahren A

Verfahren A muss ein verkabeltes System sein, in dem alle Einrichtungen (d. h. Sensoren, Logiksysteme und Aktoren, wie in Bild 4 beschrieben) den anwendbaren Produktnormen nach ISO 13577 (alle Teile) entsprechen.

Die Anforderungen nach IEC 61508 (alle Teile):2010, IEC 61511 (alle Teile):2016, IEC 62061:2021 und ISO 13849-1:— gelten nicht für diese Art von Schutzsystem.

Die folgenden Anforderungen an die Verkabelung 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 durch Datenkommunikationsbusse sind unzulässig;
- die Verkabelung des Schutzsystems muss die Anforderungen in Anhang B erfüllen.

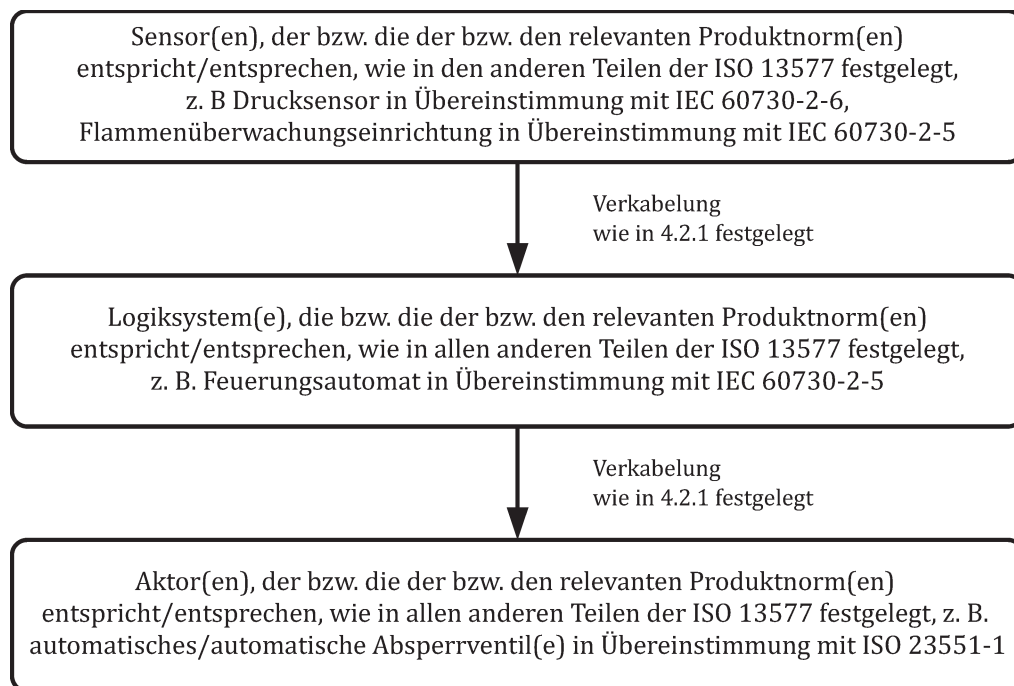


Bild 4 — Hardwarekonfiguration von Verfahren A

ANMERKUNG Die in 4.2.2 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 4.2.2 ist eines von verschiedenen alternativen Verfahren.

4.2.3 Verfahren BC

Verfahren BC muss eine Kombination aus Einrichtungen, die den relevanten Produktnormen entsprechen, und/oder SIL/PL-fähigen Geräten, für die keine relevante Produktnorm existiert, sein. Der Einsatz von Sicherheits-SPS ist optional (siehe Bild 5).

Die folgenden Anforderungen an die Verkabelung 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 müssen verkabelt oder durch einen Sicherheitsbus oder Softwareverbindungen hergestellt sein;
- die Verkabelung des Schutzsystems muss die Anforderungen in Anhang B erfüllen.

Bei Verwendung eines programmierbaren Logiksystems (z. B. Sicherheits-SPS) ist Sicherheitsfunktionssoftware nur in Form von verifizierten und validierten SIL 3-fähigen Software-Funktionsblöcken zulässig (siehe Bild 5), und Sicherheitsfunktionen sind innerhalb einer sicherheitsbewerteten Einrichtung oder innerhalb einer externen Einrichtung zulässig, die von der entsprechenden Produktnorm abgedeckt wird. Zusätzlich müssen die folgenden Anforderungen erfüllt werden:

- 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;
- Software-Verbindungen in einer programmierbaren Einrichtung müssen durch einen Funktionstest nach den Normen zur funktionalen Sicherheit verifiziert und dokumentiert werden;
- Software-Programmiersprachen für SPS müssen IEC 61131-3:2013 entsprechen;
- Software muss gegen unautorisierte und unbeabsichtigte Änderungen verriegelt und gesichert werden.

ANMERKUNG 1 Die Überprüfung und Validierung der SIL/PL-Zertifizierung von Systemsoftware (siehe IEC 61508-4:2010, 3.2.6 und 3.2.7) und Einrichtungen erfolgt in der Regel durch eine notifizierte Stelle, ein akkreditiertes nationales Prüflabor oder durch eine Organisation nach ISO/IEC 17025.

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

- die Einrichtungen müssen eine systematische Fähigkeit (en: Systematic Capability) von SC 3 (SIL 3-fähig) nach IEC 61508 (alle Teile):2010, IEC 62061:2021 oder IEC 61511 (alle Teile):2016 aufweisen oder geeignet sein, PL e nach ISO 13849-1:— zu erreichen;
- Die Zertifizierung für die muss für die gesamte Einrichtung, einschließlich Hard- und Software, gelten.

Einrichtungen mit einer geringeren Kapazität als SIL 3/PL e sind zulässig, sofern die SIL/PL-Anforderungen an die Schleife (Sicherheitsfunktion) auf der Grundlage der Risikobeurteilung bestimmt und in Übereinstimmung mit der/den Norm(en) für die funktionale Sicherheit berechnet wurden.

Wenn der SIL auf der Grundlage des bewährten Betriebs bestimmt wird, müssen die Anforderungen in IEC 61508 (alle Teile):2010 eingehalten und die erforderliche Dokumentation in der endgültigen Installationsdokumentation bereitgestellt werden. Diese Vorgehensweisen müssen vom Endanwender angenommen werden.

Wenn der PL mit bewährten Bauteilen bestimmt wird, müssen die Anforderungen aus ISO 13849-1:— befolgt werden.

Alle Anforderungen in den Anweisungen für die Einrichtung, wie etwa das Prüfungsintervall, müssen eingehalten werden.

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

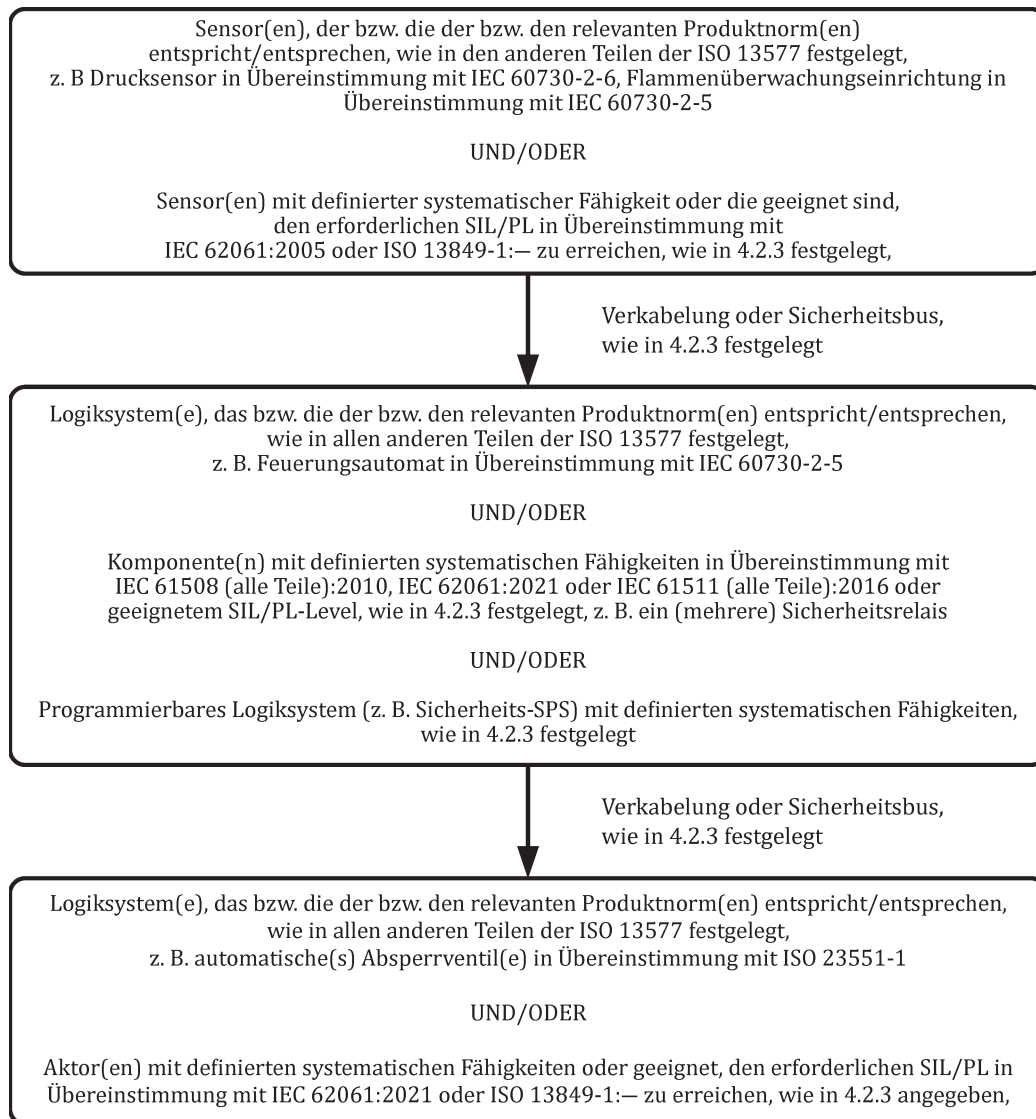


Bild 5 — Hardwarekonfiguration von Verfahren BC

4.2.3.1 Anforderungen an Anwendungssoftware von programmierbaren Logiksystemen

Anwendungssoftware muss in Übereinstimmung mit den Verfahren der funktionalen Sicherheit programmierbarer elektronischer sicherheitsbezogener Systeme entwickelt werden, die in den Anforderungen der IEC 61508 (alle Teile), IEC 61511 (alle Teile), IEC 62061:2021 oder ISO 13849-1:— definiert sind. Anhang G enthält zusätzliche Richtlinien zur Anwendung auf Grundlage von IEC 61508.

Die Anleitung des Herstellers für die Einrichtung muss alle anwendbaren Anforderungen der IEC 61508-3:2010 enthalten, wenn Softwareänderungen durch den Endanwender veranlasst werden.

4.2.4 Verfahren D

Verfahren D muss alle Anforderungen funktionaler Sicherheitsnormen nach IEC 61508 (alle Teile):2010, IEC 62061:2021, IEC 61511 (alle Teile):2016 oder ISO 13849-1:— erfüllen (siehe Bild 6).

ANMERKUNG 1 Siehe Anhang D für das Verfahren in Übereinstimmung mit IEC 61511 (alle Teile):2016.

Verfahren D muss auch die folgenden Anforderungen erfüllen:

- a) die Flammenüberwachungseinrichtung muss IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020 CSV entsprechen;
- b) alle Anforderungen der SPS und der Sicherheitseinrichtungen müssen in Übereinstimmung mit den Anweisungen des Herstellers und dem Produktsicherheitshandbuch verwendet werden;
- c) jede Anforderung an die funktionale Sicherheit, wie sie in ISO 13577 (alle Teile) festgelegt ist, muss nach den Normen für funktionale Sicherheit 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 entsprechenden Produktnormen entsprechen;

ANMERKUNG 2 Eine erweiterte Risikobeurteilung in Verfahren D kann Vorrang vor den Sicherheitsanforderungen in ISO 13577 (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 ISO 13577 (alle Teile).

- d) Verbindungen müssen verkabelt oder durch einen Sicherheitsbus oder Softwareverbindungen hergestellt sein;
- e) Die Verkabelung des Schutzsystems muss die Anforderungen in Anhang B erfüllen.

ANMERKUNG 3 Die Verifizierung und Validierung des SIL/PL wird in der Regel mit einem unabhängigen Prüfverfahren durchgeführt, ähnlich wie bei der Verifizierung durch Dritte.

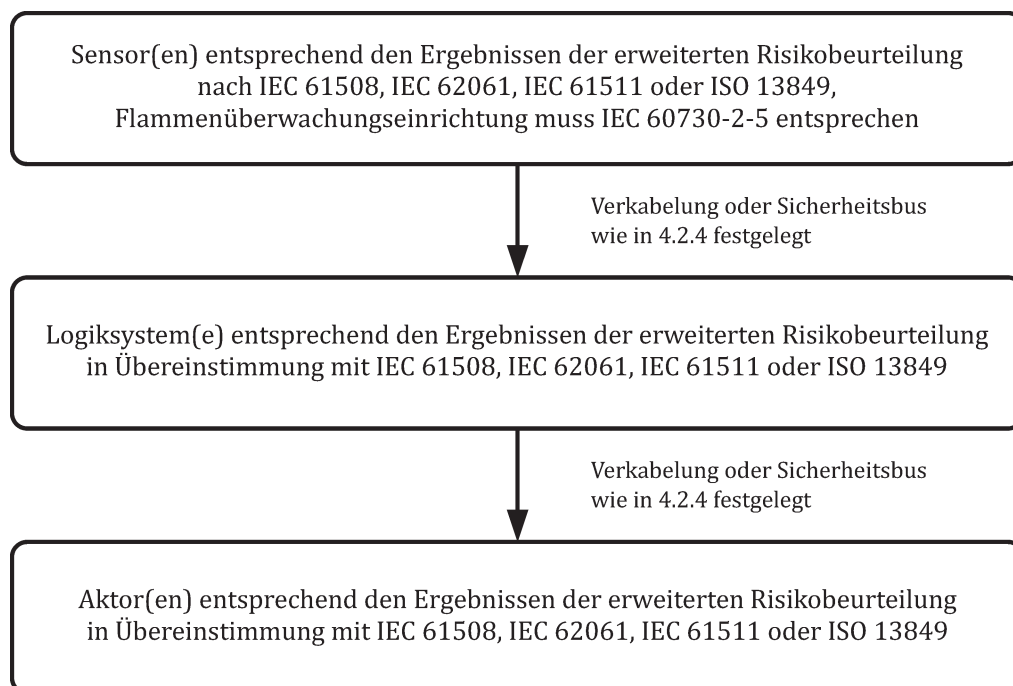


Bild 6 — Hardwarekonfiguration von Verfahren D

4.3 Fehlerbetrachtung für den verkabelten Teil von Schutzsystemen

Das Schutzsystem muss so ausgelegt sein, dass die nach ISO 13577 (alle Teile) erforderlichen Einrichtungen wie folgt verwendet werden müssen:

- a) Wenn Relais in Sicherheitsfunktionen eingesetzt werden, müssen die Kontakte überwacht und mechanisch verbunden sein, und der an alle Kontakte angelegte Strom darf höchstens 60 % der Nennleistung der Kontakte betragen. Steuerrelais für die Sicherheit müssen IEC 60947-5-1:2016 oder der geforderten SIL/PL-Anforderung entsprechen. Leistungsrelais für die Sicherheit mit oder ohne Spiegelkontakte müssen IEC 60947-4-1:2018 entsprechen.
- b) Die Einrichtungen müssen in Übereinstimmung mit den Anweisungen des Herstellers verkabelt werden.
- c) Wenn beim Verfahren BC Zeitsteuergeräte, die nicht, wie in allen anderen Teilen von ISO 13577 festgelegt, den anwendbaren 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 B enthält zusätzliche Anforderungen.

4.4 Ausfall von Versorgungseinrichtungen

Der Ausfall von Versorgungseinrichtungen (z. B. Strom, Instrumentenluft) für die TPE muss zu einem sicheren Zustand (z. B. Verriegelung) führen. Jedes erneute Anfahren darf nur durch einen manuellen Eingriff ausgelöst werden. Anfahr- und Zündungssequenz müssen erfüllt werden (siehe ISO 13577-2:—³, 4.11).

4.5 Rücksetzen

Sofern nach Verfahren D gestattet, muss an Einrichtungen, die eine Sicherheitsfunktion erfüllen, das Rücksetzen nach einer Verriegelung manuell nach Beseitigung des Fehlers durchgeführt werden (siehe ISO 13574:2015, 2.107).

Das Rücksetzen muss als Sicherheitsfunktion umgesetzt werden und ISO 13849-1:—, 5.2.3.2, entsprechen, und es darf keine Sicherheitsfunktion überbrücken.

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 sicherstellt.

Die maximale Anzahl der Rücksetzungen innerhalb eines bestimmten Zeitraums muss auf der Grundlage der Risikobeurteilung begrenzt und festgelegt werden, und sie muss in der Betriebsanleitung enthalten sein.

3 In Vorbereitung. Die zweite Ausgabe von 13577-2 soll im Jahr 2022 veröffentlicht werden.

Wenn die manuelle Rücksetzung ausgelöst wird, muss die TPE direkt oder mit einer Kamera zu sehen sein. Der sichere Betrieb muss ab der Rücksetzaktion sichergestellt sein, und der aktuelle Status und die relevanten Informationen des zu steuernden Prozesses müssen dem Bediener nachgewiesen werden.

5 Benutzerinformationen

Eine Dokumentation, die die Schutzmaßnahmen und den Betrieb detailliert beschreibt, muss in die Anlagendokumentation der aufgenommen werden.

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.

Zusätzliche Informationen zu Kompetenzen können IEC 61511-1:2016 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 IEC 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
 - Funktionalität,
 - Teilsystem- und Elementschnittstellen,
 - Sequenzierung und zeitbezogenen Informationen, und
 - 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 Fehler, zufällige Fehler sowie verbleibende Auslegungsfehler in der Hardware, Software und im Datenkommunikationsprozess schützen.

Während der Auslegung sind die Aktivitäten, die auf dem Gelände der Entwicklung durchgeführt werden können, von denen, die einen Zugang zum Gelände des Anwenders erfordern, zu unterscheiden und zu bestimmen.

Wartungsanforderungen müssen während der Auslegungsphase formal festgehalten werden, um sicherzustellen, dass die Anforderungen an die Sicherheitsintegrität der Schutzsysteme über ihre Lebenszyklen 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 sind zu entwerfen, und die Prüfplandokumentation, einschließlich der folgenden Punkte, ist zu erstellen:

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

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

Anhang B (normativ)

Verkabelung von Schutzsystemen

B.1 Allgemeines

Elektrische Ausrüstung und Anlagen müssen IEC 60204-1:2016:2016 erfüllen.

Dieser Anhang beschreibt die Verkabelung des Schutzsystems, so dass das Sicherheitsniveau nicht verringert wird.

Dieser Anhang gilt für die Verkabelung innerhalb des Logiksystems und für die Verkabelung zwischen dem Logiksystem und den Einrichtungen, die direkt oder indirekt die Aktoren steuern. Darüber hinaus gilt er für die Feldverkabelung zwischen Geräten wie Sensoren, Verriegelungen, Stellteilen, Aktoren, Flammenwächter, Zünder, usw.

Um das Sicherheitsniveau des verkabelten Schutzsystems aufrechtzuerhalten, müssen Techniken angewendet werden, um die Einbringung systematischer Fehler während der Auslegung und Entwicklung zu vermeiden oder zu verhindern und um Auslegungsmerkmale (z. B. Selbstprüfung, Redundanz) anzuwenden, um sowohl zufällige als auch systematische Fehler während des Betriebs zu kontrollieren.

Die Fehlerbetrachtung in Bild B.1 muss auf die Auslegung, die Fehleranalyse und den Nachweis der Sicherheit angewendet werden.

ANMERKUNG Basierend auf der Anwendung von Bild B.1 kann eine durch einen einzelnen Fehler hervorgerufene Gefährdungssituation ausgeschlossen werden.

B.2 Schutz vor Fehlern des Schutzsystems

Das Schutzsystem muss so ausgelegt sein, dass

- a) Fehler, die die Effektivität des Schutzsystems beeinträchtigen, durch Fehlervermeidungsmethoden, wie in den Beispielen in den Bildern B.2 bis B.8 dargestellt, vermieden werden müssen; oder

ANMERKUNG 1 Beispiele UNSACHGEMÄSSER Verkabelung sind in den Bildern B.10 bis B.14 dargestellt.

- b) bei internen Fehlern (z. B. verschweißtes Relais, falsche Platzierung der Verkabelung, zu hohe interne Temperatur) oder bei externen Einflüssen (z. B. EMV, Vibrationen, zu hohe Temperatur, Staub, Blitze) das Schutzsystem

- 1) nicht beeinträchtigt wird, oder
- 2) die Thermoprozesseinrichtungen im sicheren Zustand hält oder in den sicheren Zustand bringt (durch Verfahren zur Steuerung von Fehlern).

Das gleichzeitige Auftreten von zwei unabhängigen Fehlern in unterschiedlichen Einrichtungen muss nicht berücksichtigt werden (z. B., zwei Relais fallen ohne gemeinsame Ursache gleichzeitig aus).

Die Kombination eines zweiten Fehlers bei einem nicht erkannten ersten Fehler muss in Übereinstimmung mit Bild B.1 berücksichtigt werden. Jegliche Fehler, die sich aus einem ersten Fehler ergeben (Folgefehler), müssen zusammen mit diesem ersten Fehler berücksichtigt werden (siehe Bild B.14).

Bei Systemen für den nicht dauerhaften (nicht durchgängigen) Betrieb ist der Betrieb nicht zulässig, wenn beim Anfahren ein Fehler festgestellt wird.

Bei Systemen für Dauerbetrieb gilt 24 h nach dem ersten Fehler ein zweiter Fehler als aufgetreten (z. B. wenn der Fehler während des Betriebs erkannt wird, ist der Betrieb nicht länger als 24 h nach dem ersten Fehler zulässig).

ANMERKUNG 2 24 h ist eine Angabe der MTTR (durchschnittliche Zeit zur Wiederherstellung; en: mean time to restoration). Siehe IEC 61511-1:2016.

B.3 Maßnahmen zur Vermeidung von Fehlern

Während der Entwicklung müssen organisatorische und Auslegungsvorkehrungsmaßnahmen zur Vermeidung von Fehlern getroffen werden. Diese umfassen unter anderem:

- a) die Definition eines projektspezifischen Produktionsablaufplans, einschließlich unter anderem:
 - 1) Spezifikationen;
 - 2) Auslegung (Schema, Schaltplan, Teile-Verzeichnisse, Hardwareauslegung); und
 - 3) Prüfplan;
- b) Trennung der sicherheitsbezogenen und nicht sicherheitsbezogenen Funktionen von Einrichtungen; und
- c) die Verifizierung von Funktionen und Verbindungen durch Prüfungen.

Bei anwendungsspezifischen integrierten Schaltkreisen ist besonders auf Vorbeugungsmaßnahmen zur Fehlervermeidung zu achten.

ANMERKUNG Siehe Anhang A für Techniken und Maßnahmen zur Vermeidung systematischer Fehler.

B.4 Hardwareauslegung

B.4.1 Allgemeine Anforderungen an die Hardware

- a) Die Systembeschreibung muss leicht verständlich und logisch strukturiert sein, und sie muss die Sicherheitsphilosophie und die Schutzfunktion klar darstellen.
- b) Die geforderten Funktionen, die Reaktion im Fehlerfall, die Schnittstellen (Software, Hardware) und die zulässigen Umwelteinflüsse einer Funktionseinheit im System müssen eindeutig festgelegt werden.

B.4.2 Verdrahteter Teil eines Schutzsystems

Der verdrahtete Teil des Schutzsystems muss so aufgebaut sein, dass die Fehlerbetrachtung nach Bild B.1 zum Abbruch führt.

Bei der Fehlerbetrachtung für das Schutzsystem nach Bild B.1 ist der Ausfall der Hilfsenergie und die Unterbrechung von Verbindungsleitungen zu berücksichtigen.

ANMERKUNG 1 Wenn bei diesen Fehlern bestimmte betroffene Einrichtungen den sicheren Zustand erreichen (z.B. Ruhestromprinzip bei Binärkreisen), ist abgesehen von den folgenden Maßnahmen eine einkanalige Ausführung des jeweiligen Teiles ausreichend. Kann diese Annahme nicht getroffen werden (z.B. beim Arbeitsstromprinzip in Binärkreisen), so würde ein zweiter, üblicherweise eingeschalteter, unabhängiger Auslösekanal vorgesehen werden

(z. B. Betrieb geschlossener Kreise in Binärkreisen), damit die Wirksamkeit des Schutzsystems (inkl. aller pneumatischen, hydraulischen und mechanischen Stellelemente) für diese Funktion erreicht wird.

Bei Ausgangsschaltungen müssen für die Sicherheitsabschaltung der gesamten Brennstoffzufuhr in den Feuerraum mindestens zwei überwachte Abschaltglieder, d. h. Schütze bzw. Relais, vorgesehen werden, um eine Sicherheitsabschaltung der gesamten Brennstoffzufuhr zu erreichen.

Reed-Relais dürfen nicht für Schutzfunktionen verwendet werden.

ANMERKUNG 2 Gerätediversität wird durch unterschiedliche Bauart der elektromechanischen Schaltgeräte erreicht, z. B. wenn Schaltgeräte unterschiedlicher Konstruktion oder unterschiedlicher Auslegung verwendet werden. Funktionsdiversität wird z.B. durch Ruhestrom- und Arbeitsstromschaltung erreicht.

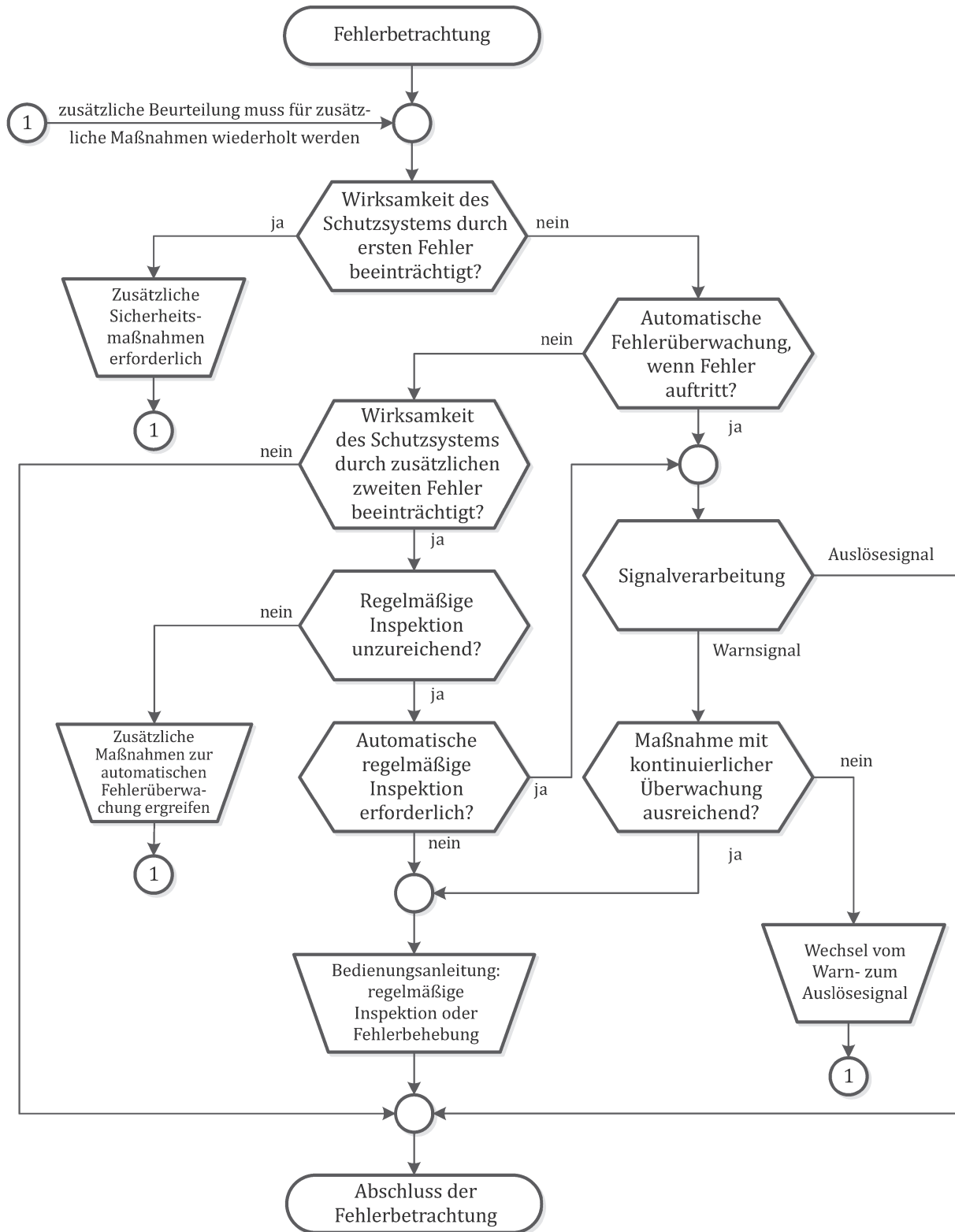


Bild B.1 — Fehlerbetrachtung für den verkabelten Teil eines Schutzsystems

B.5 Ordnungsgemäße Eingangsverkabelung

Im Folgenden stehen Beispiele für Techniken zur Vermeidung von Fehlern durch die externe Verkabelung.

Bild B.2 zeigt eine Technik, die bei Verwendung der Schutzsystemverfahren A, BC oder D 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. Zusätzlich nimmt das Schutzsystemgerät jeden Leiter von den Sensoren an.

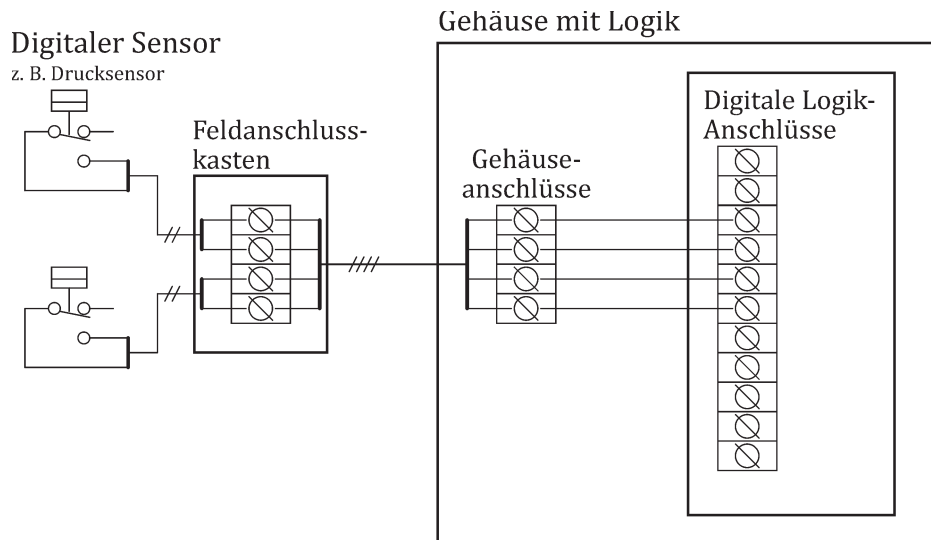
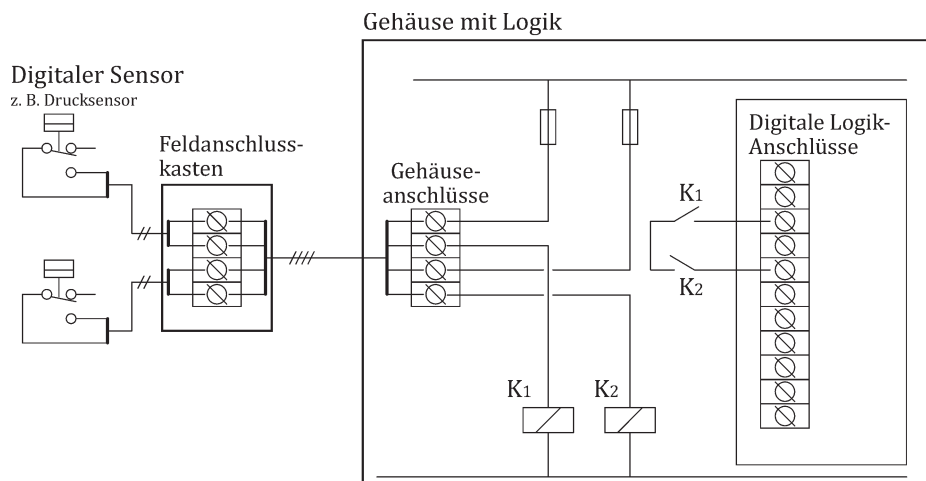


Bild B.2 Geschützte Verkabelung

Bild B.3 zeigt eine leichte Variation, die benötigt wird, wenn das Logiksystem nur einen digitalen Eingang akzeptiert.



Legende

K1, K2 Zusatzrelais (siehe Bild B.9)

Bild B.3 — Geschützte Verkabelung mit Zusatzrelais

Bild B.4 zeigt eine Technik, bei der beide Zustände des Sensorschalters (1 Normal-Offen- und 1 Normal-Geschlossen-Kontakt für jeden Sensor) durch das Schutzsystem überwacht werden und dessen Logiksystem den unzulässigen Zustand erkennt, der durch einen Kurzschluss in der Feldverkabelung verursacht wird. Diese Technik ist geeignet, wenn eines der Schutzsystemverfahren, A, BC oder D, verwendet wird.

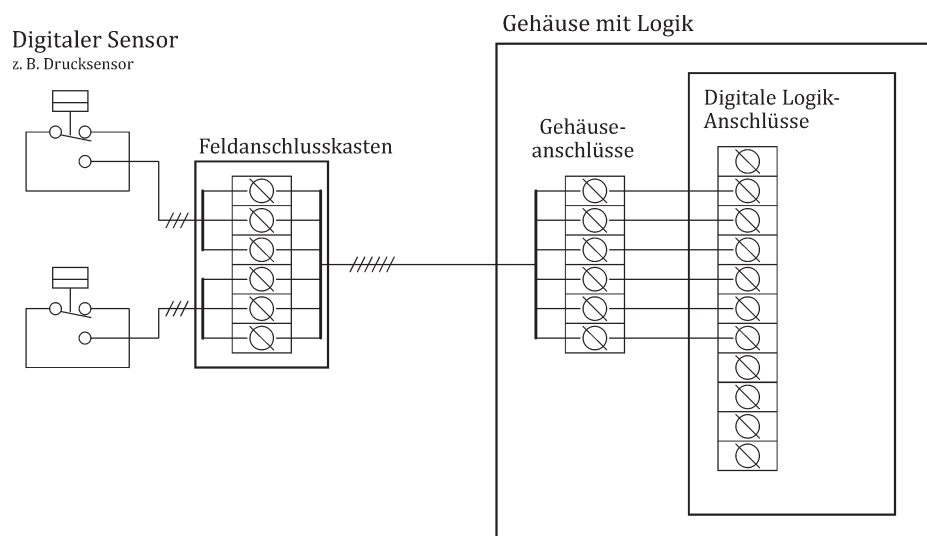


Bild B.4 — Überwachung der beiden Zustände

Bild B.5 zeigt eine Variation von Bild B.4, wobei das Einzelkabel mit 6 Leitern durch zwei Kabel mit je 3 Leitern ersetzt werden kann.

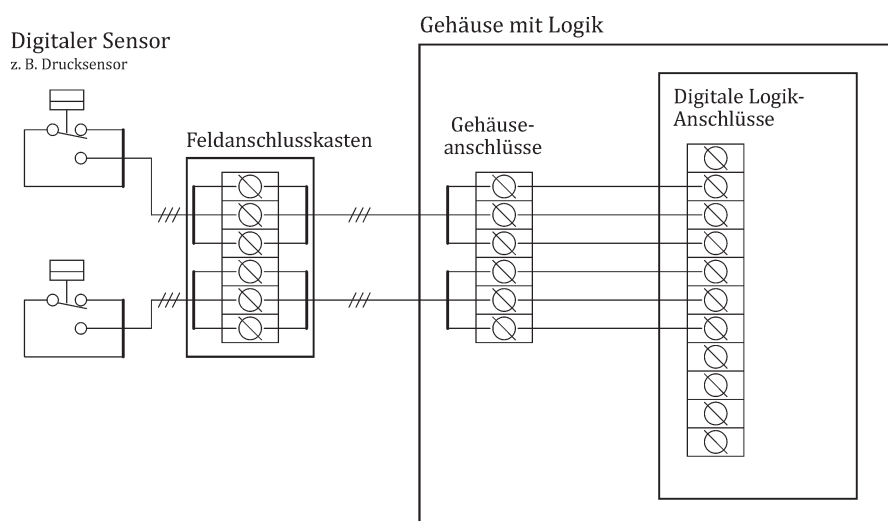
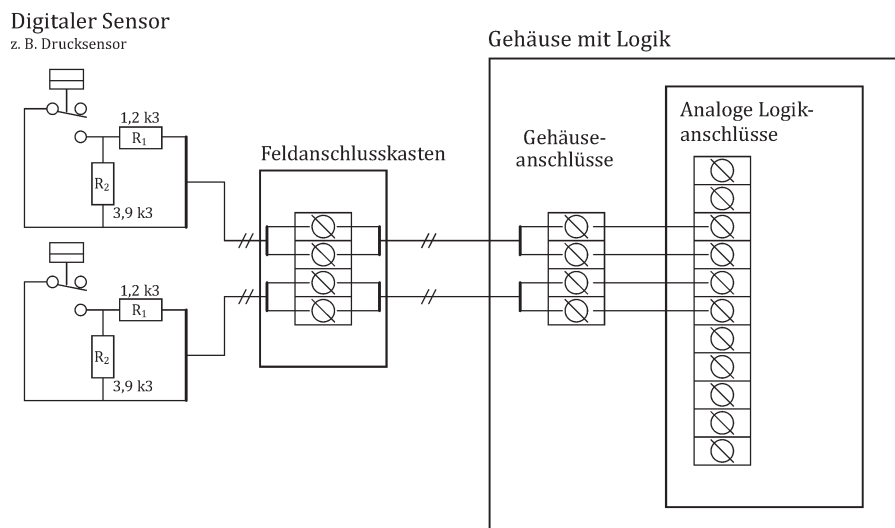


Bild B.5 — Überwachung der beiden Zustände, mehrere Kabel

Bild B.6 zeigt eine Technik mit Analogsignalen für die Schaltzustände, und das Logiksystem des Schutzsystems erkennt den unzulässigen Zustand durch einen Kurzschluss in der Feldverkabelung (der Analogpegel liegt außerhalb der zulässigen Bänder für den hohen oder niedrigen Zustand). Diese Technik ist geeignet, wenn Verfahren BC oder D verwendet wird.



ANMERKUNG 1 Die Eingangskarte sollte in der Lage sein, Leitungsunterbrechungen und Kurzschlüsse zu erkennen.

ANMERKUNG 2 Die im Bild angegebenen Werte sind nur Beispiele für 4 mA bis 20 mA.

Legende

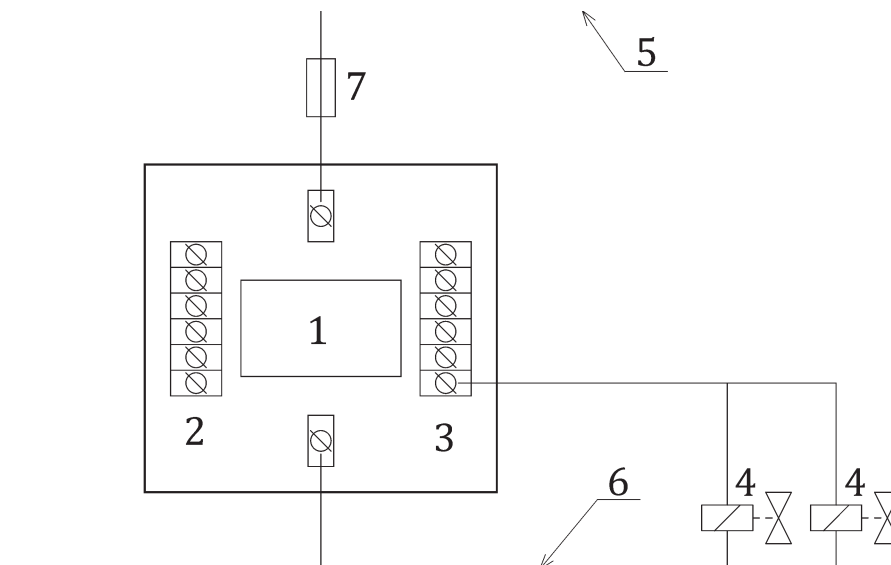
R_1 Widerstand 1 (1,2 k Ω)

R_2 Widerstand 1 (3,9 k Ω)

Bild B.6 — Überwachung durch Analogwert

B.6 Ordnungsgemäße Ausgangverkabelung

Bild B.7 zeigt, wie zwei Magnetventile im Fall einer Anwendung für einen einfachen automatischen elektrischen Feuerungsautomaten verkabelt werden. Diese Technik ist nur geeignet, wenn Schutzsystemverfahren A verwendet wird.



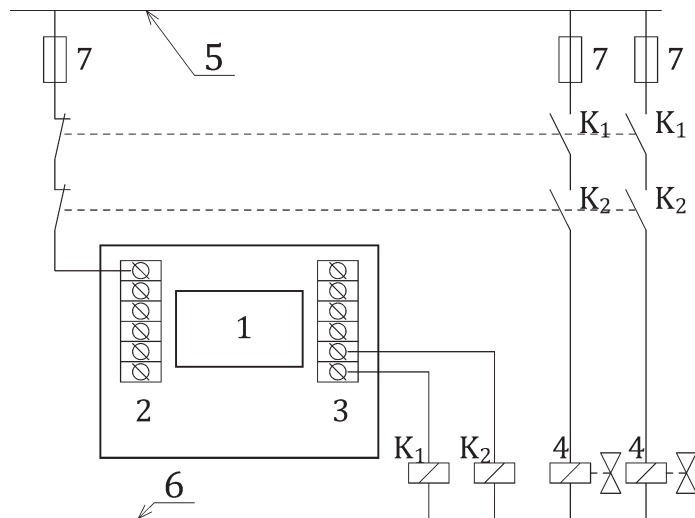
Legende

- 1 Elektrischer Feuerungsautomat
- 2 sicherer Eingang
- 3 sicherer Ausgang
- 4 Brennstoffventile
- 5 Betriebsspannung
- 6 neutral
- 7 Sicherung

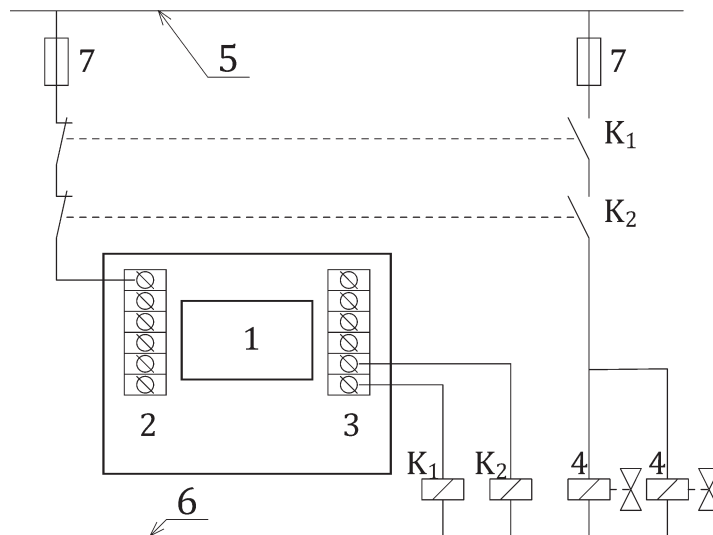
ANMERKUNG Dieses Bild zeigt einen sicheren Ausgang mit Ventilredundanz. Die Diagnose kann durch Flammenerkennung (Eingangssignal) erreicht werden. Mit anderen Worten: Sobald die Anlage abgeschaltet ist, erkennt der elektrische Feuerungsautomat das Fehlen der Flamme.

Bild B.7 — Beispiel für eine Anwendung eines einfachen elektrischen Feuerungsautomaten

Bild B.8 zeigt die Verkabelung, wenn Relais zur Spannungsversorgung der Magnetventile verwendet werden müssen. Diese Technik ist geeignet, wenn eines der Schutzsystemverfahren A, BC, oder D verwendet wird.



oder



Legende

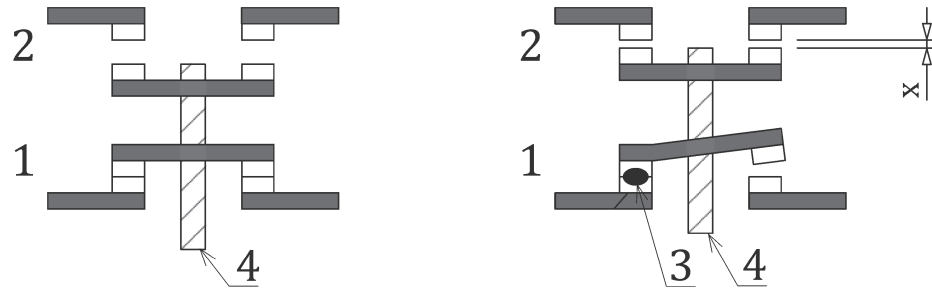
- | | |
|---------------------|-------------------------|
| 1 Logiksystem(e) | 6 neutral |
| 2 sicherer Eingang | 7 Sicherung |
| 3 sicherer Ausgang | K ₁ Relais 1 |
| 4 Brennstoffventile | K ₂ Relais 2 |
| 5 Betriebsspannung | |

ANMERKUNG 1 Relaisfehler werden erkannt, daher summieren sich Fehler nicht.

ANMERKUNG 2 Hinsichtlich der Anforderungen an Relais siehe 4.3 a). Siehe auch Bild B.9 hinsichtlich der grundlegenden Konfiguration von Relais in Sicherheitsstromkreisen.

Bild B.8 — Beispiel für Fehlervermeidung

Bild B.9 zeigt ein Beispiel einer mechanisch verbundenen (IEC 60947-5 1:2016) Konstruktion für Relaiskontakte.



Legende

- 1 normal geschlossene Kontakte
- 2 normal offene Kontakte
- 3 geschweißter Kontakt (Fehler)
- 4 mechanisch verbundenen Konstruktion
- x Mindestabstand

ANMERKUNG 1 Relais, die in Sicherheitsschaltungen mit Rückmeldung der Relaisposition verwendet werden, müssen mit mechanisch verbundenen Kontakten ausgestattet sein.

ANMERKUNG 2 Bei Leistungsrelais dürfen Spiegelkontakte nur als Rückmeldung über die Position der Hauptkontakte verwendet werden.

ANMERKUNG 3 Durch die Konstruktion des mechanischen Gestänges und den Mindestabstand bleiben die üblicherweise offenen Kontakte offen, wenn die Relaisspule unter Spannung steht und ein normalerweise geschlossener Kontakt verschweißt ist. Ebenso bewirkt ein Fehler beim Verschweißen eines normal offenen Kontaktes, dass die normal geschlossenen Kontakte beim Abschalten der Relaisspule geöffnet bleiben.

Bild B.9 — Beispiel eines Relais mit mechanisch verbundenen Kontakten

B.7 Unsachgemäße Eingangs- und Ausgangsverkabelung

Bild B.10 zeigt ein Beispiel eines möglichen Kurzschlusses an Legendenpunkt 2, der das Schutzsystem außer Kraft setzen würde. 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 Legendenpunkt 2 wird der offene Zustand von keinem der beiden Schalter erkannt.

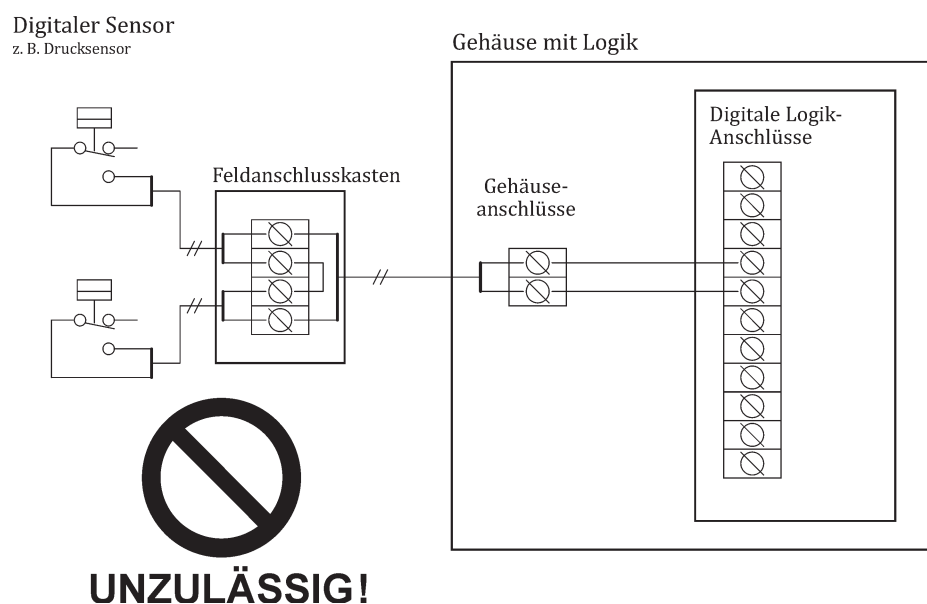
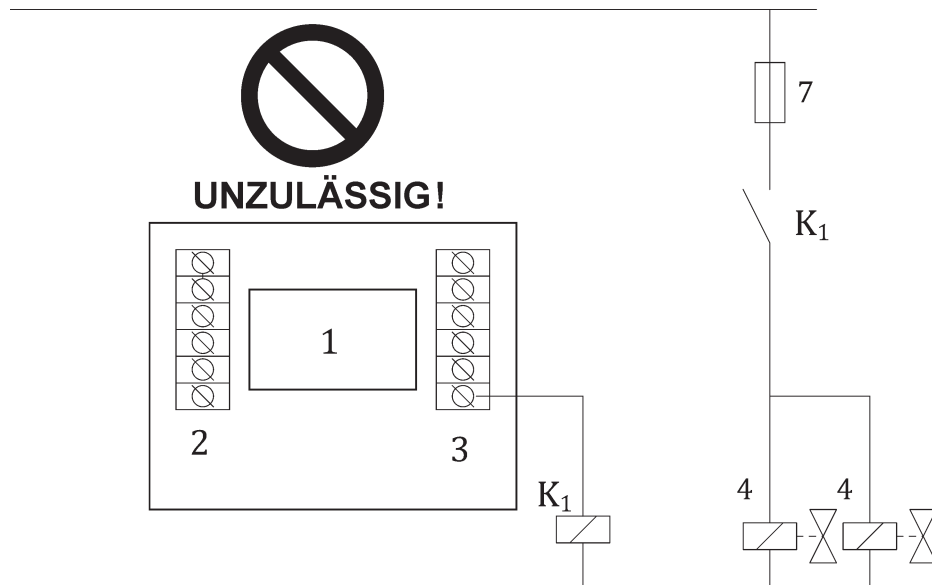


Bild B.10 — UNSACHGEMÄSSE externe Verkabelungsmethode

Bild B.11, Bild B.12 und Bild B.13 zeigen Beispiele für die UNSACHGEMÄSSE Verkabelung, selbst wenn Relais, wie in Bild B.9 beschrieben, verwendet werden.

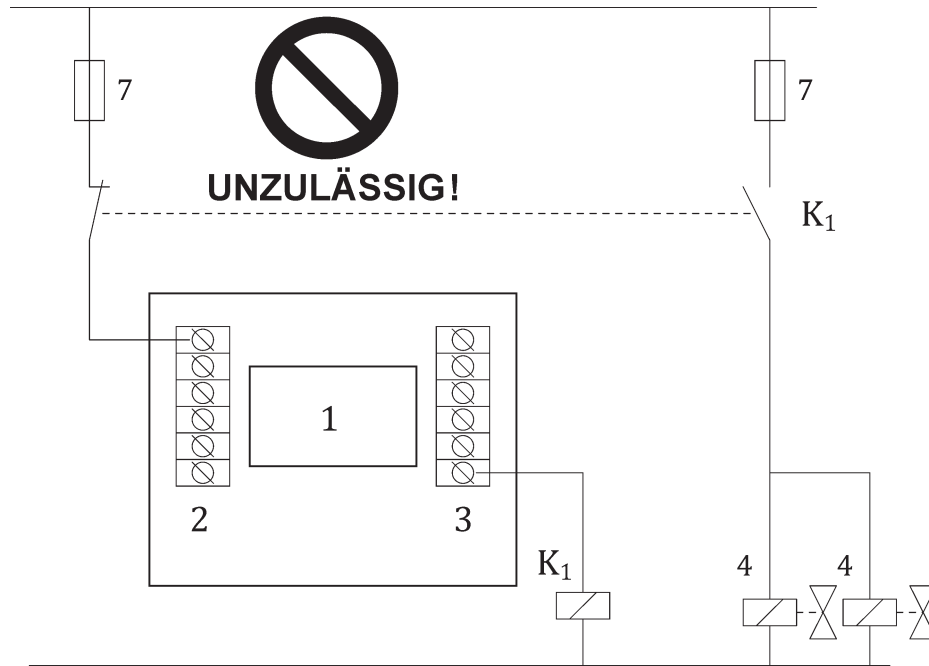


Legende

- 1 Logiksystem(e)
- 2 sicherer Eingang
- 3 sicherer Ausgang
- 4 Brennstoffventile
- 5 Betriebsspannung
- 6 neutral
- 7 Sicherung
- K₁ Relais 1

ANMERKUNG Da nur ein Relais verwendet wird, kann ein einzelner Ausfall zum Verlust der Sicherheitsfunktion führen.

Bild B.11 — Beispiel UNSACHGEMÄSSE Verkabelung

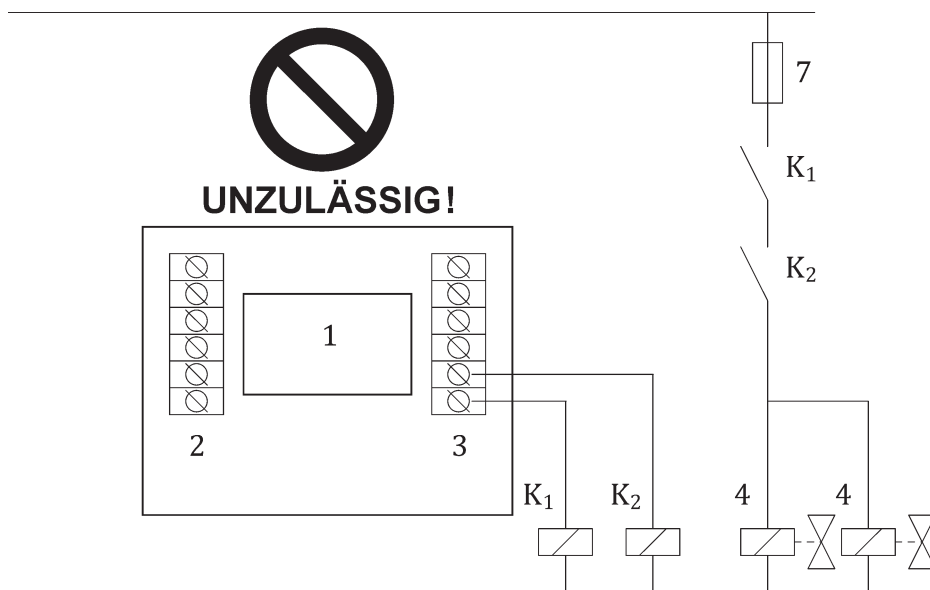


Legende

- 1 Logiksystem(e)
- 2 sicherer Eingang
- 3 sicherer Ausgang
- 4 Brennstoffventile
- 5 Betriebsspannung
- 6 neutral
- 7 Sicherung
- K₁ Relais 1

ANMERKUNG Da nur ein Relais verwendet wird, kann auch bei dessen Überwachung ein einziger Ausfall zum Verlust der Sicherheitsfunktion führen.

Bild B.12 — Beispiel UNSACHGEMÄSSER Verkabelung



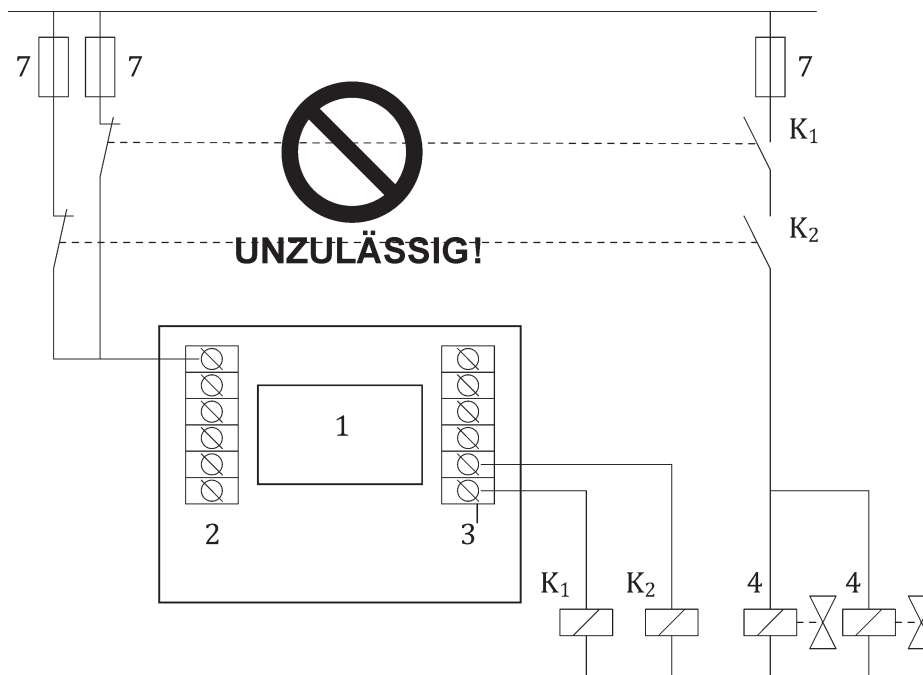
Legende

- 1 Logiksystem(e)
- 2 sicherer Eingang
- 3 sicherer Ausgang
- 4 Brennstoffventile
- 5 Betriebsspannung
- 6 neutral
- 7 Sicherung
- K₁ Relais 1
- K₂ Relais 2

ANMERKUNG Ein einzelner Ausfall vermeidet den Verlust der Sicherheitsfunktion, aber da Relaisausfälle unerkannt bleiben, können sich Ausfälle kumulieren und zum Verlust der Sicherheitsfunktion führen.

Bild B.13 — Beispiel UNSACHGEMÄSSER Verkabelung

Bild B.14 zeigt ein Beispiel einer UNSACHGEMÄSSEN Ausgangsverkabelung. Die ordnungsgemäße Verkabelung ist in Bild B.8 dargestellt.



Legende

- 1 Logiksystem(e)
- 2 sicherer Eingang
- 3 sicherer Ausgang
- 4 Brennstoffventile
- 5 Betriebsspannung
- 6 neutral
- 7 Sicherung
- K₁ Relais 1
- K₂ Relais 2

ANMERKUNG Ein einzelner Relaisausfall wird nicht erkannt, daher kann eine Häufung von Ausfällen zum Verlust der Sicherheitsfunktion führen.

Bild B.14 — Beispiel UNSACHGEMÄSSE Verkabelung der Überwachungsrelais

Anhang C (informativ)

Beispiele für die Bestimmung des Sicherheits-Integritäts- oder Performance Level SIL/PL mittels des Risikograph-Verfahrens

C.1 Allgemeines

Verschiedene Internationale Normen können zur Bestimmung des erforderlichen SIL/PL herangezogen werden. Für maschinelle Anlagen wurde IEC 62061:2021 zur Bestimmung des SIL entwickelt, während IEC 61511 (alle Teile):2016 zur Bestimmung des erforderlichen SIL in der Prozessindustrie entwickelt wurde. Risikograph-Verfahren für die Bestimmungen des Sicherheits-Integritätslevel (SIL) werden in den beiden IEC Normen [IEC 62061:2021 und IEC 61511 (alle Teile):2016] angegeben. Zudem deckt ISO 13849-1:— die Bestimmung des Performance Levels (PL) ab und enthält auch ein Verfahren zur Bestimmung eines PL aus einem SIL (ISO /FDIS 13849-1:2021, Tabelle 3).

Für jede Gefährdung des Industrieofens und der zugehörigen Prozessanlagen (TPE) ist eine Gefahren- und Risikoanalyse durchzuführen. 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.

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

- Folgen des Gefährdungsereignisses (Parameter Se nach IEC 62061:2021, Anhang A, Parameter C nach IEC 61511-3:2016); das Szenario der ungünstigsten Möglichkeiten muss berücksichtigt werden;
- Häufigkeit und Dauer der im Gefährdungsbereich verbrachten Zeit (Parameter Fr nach IEC 62061:2021, Anhang A, Parameter F nach IEC 61511-3:2016); 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 nach IEC 62061:2021, Anhang A, Parameter P nach IEC 61511-3:2016);
- Eintrittswahrscheinlichkeit des Gefährdungsereignisses oder der Anforderungsrate (Parameter Pr nach IEC 62061:2021, Anhang A, Parameter W nach IEC 61511-3:2016).

Der Parameter Av nach IEC 62061:2021, Anhang A und der Parameter P nach IEC 61511-3:2016 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 niedrigste Wert sollte nur verwendet werden, wenn alle folgenden Aussagen entsprechend zutreffen:

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

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

Der Parameter Pr nach IEC 62061:2021, Anhang A und der Parameter W nach IEC 61511-3:2016 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 Begründung und den getroffenen Entscheidungen 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 eines Beispiels der SIL/PL-Bestimmung in verschiedenen Risikoumgebungen nach IEC 62061:2021, Anhang A/ISO 13849-1:—, Tabelle 3.

C.2.2 Beispiel 2 – Tabelle C.2

Tabelle C.2 zeigt Beispiel der SIL-Bestimmung in verschiedenen Risikoumgebungen nach IEC 61511-3:2016.

Tabelle C.1 — Vergleich der SIL/PL-Bestimmung in verschiedenen Risikoumgebungen nach IEC 62061:2021 und ISO 13849-1:—, Tabelle 3

Risikobeurteilung und Sicherheitsmaßnahmen										Dokumentennr.: Teil von:		
Projekt: Beispiel einer typischen SIL-Bestimmung												
Herausgegeben von:												
Datum:												
Überarbeitet:												
<div style="display: flex; justify-content: space-between;"> <div> Schwarze Fläche = Sicherheitsmaßnahmen erforderlich Graue Fläche = Sicherheitsmaßnahmen empfohlen </div> <div style="border: 1px solid black; padding: 5px;"> ☐ Vor-Risikobeurteilung ☐ Zwischen-Risikobeurteilung ☐ Nachfolgende Risikobeurteilung </div> </div>												
Konsequenzen	Schweregrad	Klasse, Cl					Häufigkeit und Dauer, Fr		Wahrscheinlichkeit des Gefährdungsereignisses, Pr		Vermeidung Av	
	Se	3 – 4	5 – 7	8 – 10	11 – 13	14 – 15						
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 h	5	Sehr hoch	5		
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ Tag	5	Wahrscheinlich	4		
Heilbar, ärztliche Behandlung	2			OM	SIL 1	SIL 2	> 1 d – ≤ 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	Integrität		Kommentare
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
10	Anlagentemperatur übersteigt die höchstzulässige Arbeitstemperatur	Eine Temperaturfühler-Regelung 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 ISO 13577-2:—, 4.3.6/4.5.8 Automatic shut-off valves Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
10	Anlagentemperatur übersteigt die höchstzulässige Arbeitstemperatur	Eine Temperaturfühler-Regelung 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 ISO 13577-2:—, 4.3.6/4.5.8 Automatic shut-off valves Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen		Wahrscheinlichkeit des Eintretens			Klasse	Integrität		Kommentare
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
10	Anlagentemperatur übersteigt die höchstzulässige Arbeitstemperatur	Eine Temperaturfühler-Regelung 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. ISO 13577-2:—, 4.3.6,/4.5.8 Automatic shut-off valves Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
12	Verbrennungsluftdruck/-strom zu gering	Drucksensor, Druckgeber oder Durchflusssensor überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Luftdruck/-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 ISO 13577-2:—, 4.6.2 Air flow and pressure sensing devices Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen	Wahrscheinlichkeit des Eintretens				Klasse	Integrität		Kommentare
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
12	Verbrennungs-luftdruck/-strom zu gering	Drucksensor, Druckgeber oder Durchflusssensor überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Luftdruck/-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 ISO 13577-2:—, 4.6.2 Air flow and pressure sensing devices Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
12	Verbrennungs-luftdruck/-strom zu gering	Drucksensor, Druckgeber oder Durchflusssensor überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Luftdruck/-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 ISO 13577-2:—, 4.6.2 Air flow and pressure sensing devices Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen	Wahrscheinlichkeit des Eintretens				Klasse	Integrität		Kommentare
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
13	Luft-/Gasverhältnis außerhalb des sicheren Betriebsbereiches	Das korrekte Luft-/Gasverhältnis wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Verhältnissensor kombiniert mit einem Logiksystem muss das Verhältnis 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 ISO 13577-2:—, 4.6.3 Air/fuel ratio, Gefährdungen: Expollosion, Feuer, Vergiftung.
13	Luft-/Gasverhältnis außerhalb des sicheren Betriebsbereiches	Das korrekte Luft-/Gasverhältnis wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Verhältnissensor kombiniert mit einem Logiksystem muss das Verhältnis 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 ISO 13577-2:—, 4.6.3 Air/fuel ratio Gefährdungen: Explosion, Feuer, Vergiftung.

SRCF	Gefährdungsereignis	Sicherheitsbezogene Steuerungsfunktion (SRCF)	Konsequenzen		Wahrscheinlichkeit des Eintretens			Klasse	Integrität		Kommentare
Nr.	Beschreibung	Beschreibung		Se	Fr	Pr	Av	Cl	SIL	PL	
13	Luft-/Gasverhältnis außerhalb des sicheren Betriebsbereiches	Das korrekte Luft-/Gasverhältnis wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Verhältnissensor kombiniert mit einem Logiksystem muss das Verhältnis 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 ISO 13577-2:—, 4.6.3 Air/fuel ratio Gefährdungen: Explosion, Feuer, Vergiftung.
ANMERKUNG C.2.3 enthält eine Anleitung zu diesem Risikograph.											

Tabelle C.2 — SIL-Bestimmung in verschiedenen Risikoumgebungen nach IEC 61511:2016

Projekt:		Beispiel einer typischen SIL-Bestimmung						Prozess:	
Herausgegeben von:								SIF:	
Datum:								Anlage:	
Ausgabe								Risiko:	
Konsequenzparameter		Risikograph-Matrix						Belegungsparameter	
								Vermeidungsparameter	
								Anforderungsparameter	
								Geschätzte SIF-Anforderungsrate	
								W	
								W ₉	
								Oft	
								> 1/Jahr	
								9	
								W ₈	
								Häufig	
								1/1–3 Jahre	
								8	
								W ₇	
								Wahrscheinlich	
								1/3–10 Jahre	
								7	
								W ₆	
								Wahrscheinlich	
								1/10–30 Jahre	
								6	
								W ₅	
								Gelegentlich	
								1/30–100 Jahre	
								5	
								W ₄	
								Gering	
								1/100–300 Jahre	
								4	
								W ₃	
								Unwahrscheinlich	
								1/300–1 000 Jahre	
								3	
								W ₂	
								Unglaublich	
								1/1 000–10 000 Jahre	
								2	
								W ₁	
								Unvorstellbar	
								1/10 000–100 000 Jahre	
								1	

SIF	Gefährdungsereignis	Sicherheitstechnische Funktion (SIF)	Konsequenzen		Einfluss		Bedarf	Wahrscheinlichkeit	Integrität		Gefährdungsbeschreibung und Anmerkungen
Nr.	Beschreibung	Beschreibung	Schaden	C	F	P	W	Summe	SIL	SIL	
10	Anlagentemperatur übersteigt die höchstzulässige Arbeitstemperatur	Eine Temperaturfühler-Regelung 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	1	0	6	7	1	1	Erhebliche Konsequenzen für wenige Personen, die nicht rechtzeitig fliehen können ISO 13577-2:—, 4.3.6/4.5.8 Automatic shut-off valves Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
			E	B	1	0		7	—		
			F	D				7	1		
10	Anlagentemperatur übersteigt die maximal zulässige Arbeitstemperatur	Eine Temperaturfühler-Regelung 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 ISO 13577-2:—, 4.3.6/4.5.8 Automatic shut-off valves Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
			E	B	1	1		8	—		
			F	D				8	2		
10	Anlagentemperatur übersteigt die höchstzulässige Arbeitstemperatur	Eine Temperaturfühler-Regelung 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 ISO 13577-2:—, 4.3.6/4.5.8 Automatic shut-off valves Gefährdung: Feuer, Maschinenschaden, Verletzungen durch heiße Teile
			E	B	1	1		9	a		
			F	D				9	2		

SIF	Gefährdungsereignis	Sicherheitstechnische Funktion (SIF)	Konsequenzen		Einfluss		Bedarf	Wahrscheinlichkeit	Integrität		Gefährdungsbeschreibung und Anmerkungen
Nr.	Beschreibung	Beschreibung	Schaden	C	F	P	W	Summe	SIL	SIL	
12	Verbrennungs-luftdruck/-strom zu gering	Drucksensor, Druckgeber oder Durchflusssensor überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Luftdruck/-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 ISO 13577-2:—, 4.6.2 Air flow and pressure detectors Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
			E	B	1	0		7	—		
			F	E				7	2		
12	Verbrennungs-luftdruck/-strom zu gering	Drucksensor, Druckgeber oder Durchflusssensor überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Luftdruck/-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 ISO 13577-2:—, 4.6.2 Air flow and pressure detectors Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
			E	B	1	1		8	—		
			F	E				8	2		
12	Verbrennungs-luftdruck/-strom zu gering	Drucksensor, Druckgeber oder Durchflusssensor überwacht den Luftdruck/-strom und bringt die Anlage in Kombination mit dem Logikkreis in einen sicheren Zustand, wenn der Luftdruck/-strom unter ein sicheres Niveau fällt.	H	E	2	1	6	9	3	3	Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können ISO 13577-2:—, 4.6.2 Air flow and pressure detectors Gefährdungen: Explosion, Feuer, Vergiftung, unvollständige Verbrennung
			E	B	1	1		8	—		
			F	E				8	2		

SIF	Gefährdungsereignis	Sicherheitstechnische Funktion (SIF)	Konsequenzen		Einfluss		Bedarf	Wahrscheinlichkeit	Integrität		Gefährdungsbeschreibung und Anmerkungen
Nr.	Beschreibung	Beschreibung	Schaden	C	F	P	W	Summe	SIL	SIL	
13	Luft-/Gasverhältnis außerhalb des sicheren Betriebsbereiches	Das korrekte Luft-/Gasverhältnis wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Verhältnissensor kombiniert mit einem Logiksystem muss das Verhältnis 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 ISO 13577-2:—, 4.6.3 Air/fuel ratio Gefährdungen: Explosion, Feuer, Vergiftung.
			E	B	1	0		8	—		
			F	E				8	2		
13	Luft-/Gasverhältnis außerhalb des sicheren Betriebsbereiches	Das korrekte Luft-/Gasverhältnis wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Verhältnissensor kombiniert mit einem Logiksystem muss das Verhältnis 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 ISO 13577-2:—, 4.6.3 Air/fuel ratio Gefährdungen: Explosion, Feuer, Vergiftung.
			E	B	1	1		9	a		
			F	E				9	3		
13	Luft-/Gasverhältnis außerhalb des sicheren Betriebsbereiches	Das korrekte Luft-/Gasverhältnis wird durch mechanische, pneumatische oder elektrische Systeme gesteuert. Der elektrische Verhältnissensor kombiniert mit einem Logiksystem muss das Verhältnis auf ein sicheres Niveau bringen.	H	E	2	1	7	10	3	3	Erhebliche Konsequenzen für viele Personen, die nicht rechtzeitig fliehen können ISO 13577-2:—, 4.6.3 Air/fuel ratio 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 IEC 62061:2021, Anhang A (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 Risikoeinschätzung 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
 - a) Häufigkeit und Dauer der Exposition von Personen gegenüber der Gefährdung, Fr;
 - b) Wahrscheinlichkeit des Eintretens eines Gefährdungsereignisses, Pr; und
 - c) Möglichkeiten zur Vermeidung oder Begrenzung des Schadens, Av.

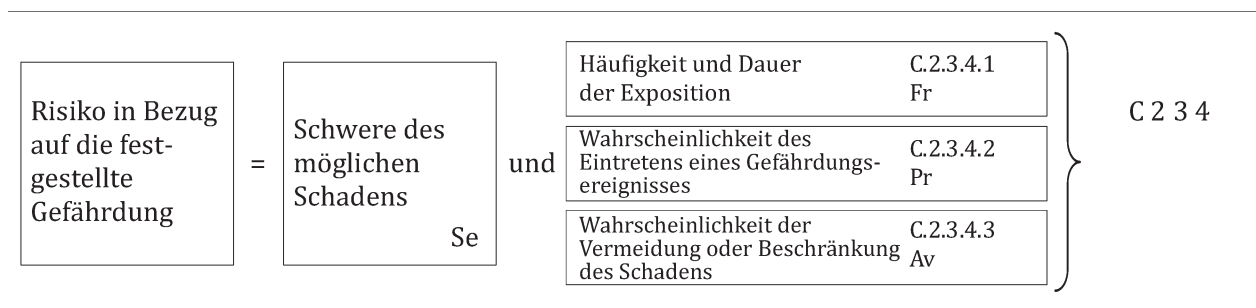


Bild C.1 — In der Risikoeinschätzung verwendete Parameter

Die in Tabelle C.7 verzeichneten Einschätzungen sollten üblicherweise 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 Schweregrade 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 eine tödliche oder erhebliche, irreversible Verletzung derart bedeutet, dass es sehr schwer sein wird, dieselbe Arbeit nach der Heilung auszuüben, falls dies überhaupt möglich ist;
- 3 eine größere oder irreversible Verletzung derart bedeutet, dass es möglich sein kann, nach der Heilung dieselbe Tätigkeit auszuüben. Dies kann auch schwere größere, jedoch reversible Verletzungen wie gebrochen Gliedmaßen beinhalten;