

	DIN EN ISO 13577-4	
ICS 13.100; 25.180.01 Industrielle Thermoprozessanlagen und dazugehörige Prozesskomponenten – Sicherheitsanforderungen – Teil 4: Schutzsysteme (ISO 13577-4:2022); Deutsche Fassung EN ISO 13577-4:2022 Industrial furnaces and associated processing equipment – Safety – Part 4: Protective systems (ISO 13577-4:2022); German version EN ISO 13577-4:2022 Fours industriels et équipements associés – Sécurité – Partie 4: Systèmes de protection (ISO 13577-4:2022); Version allemande EN ISO 13577-4:2022 Gesamtumfang 99 Seiten DIN-Normenausschuss Maschinenbau (NAM) DIN-Normenausschuss Gastechnik (NAGas)		

Nationales Vorwort

Diese Norm enthält sicherheitstechnische Festlegungen.

Die nationalen Interessen bei der Erarbeitung wurden vom Arbeitsausschuss NA 060-03-04 AA „Schutzsysteme“ im Fachbereich „Thermoprozesstechnik“ des DIN-Normenausschusses Maschinenbau (NAM) wahrgenommen. Vertreter der Hersteller und Anwender von „Maschinen“ sowie der Berufsgenossenschaften waren 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 60947-4-1:2018	siehe	DIN EN IEC 60947-4-1 (VDE 0660-102):2020-05, Berichtigung 1:2021-03, Berichtigung 2:2021-11
IEC 60947-5-1:2016	siehe	DIN EN 60947-5-1 (VDE 0660-200):2018-03
IEC 60204-1:2016	siehe	DIN EN 60204-1 (VDE 0113-1):2019-06
IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020	siehe	DIN EN 60730-2-5 (VDE 0631-2-5):2020-01, E DIN EN 60730-2-5/A2 (VDE 0631-2-5/A2):2022-08*
IEC 61508-1:2010	siehe	DIN EN 61508-1 (VDE 0803-1):2011-02
IEC 61508-2:2010	siehe	DIN EN 61508-2 (VDE 0803-2):2011-02
IEC 61508-3:2010	siehe	DIN EN 61508-3 (VDE 0803-3):2011-02
IEC 61508-4:2010	siehe	DIN EN 61508-4 (VDE 0803-4):2011-02
IEC 61508-5:2010	siehe	DIN EN 61508-5 (VDE 0803-5):2011-02
IEC 61508-6:2010	siehe	DIN EN 61508-6 (VDE 0803-6):2011-02
IEC 61508-7:2010	siehe	DIN EN 61508-7 (VDE 0803-7):2011-02
IEC 61131-3:2013	siehe	DIN EN 61131-3:2014-06
IEC 61511-1:2016	siehe	DIN EN 61511-1:2019-02
IEC 61511-2:2016	siehe	DIN EN 61511-2:2019-02
IEC 61511-3:2016	siehe	DIN EN 61511-3:2019-02
IEC 62061:2021	siehe	DIN EN IEC 62061:2023-02

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

* Zurzeit Entwurf.

Nationaler Anhang NA (informativ)

Literaturhinweise

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

DIN EN IEC 60947-4-1 (VDE 0660-102):2020-05, *Niederspannungsschaltgeräte — Teil 4-1: Schütze und Motorstarter — Elektromechanische Schütze und Motorstarter (IEC 60947-4-1:2018); Deutsche Fassung EN IEC 60947-4-1:2019*

DIN EN IEC 60947-4-1 Berichtigung 1 (VDE 0660-102 Berichtigung 1):2021-03, *Niederspannungsschaltgeräte — Teil 4-1: Schütze und Motorstarter — Elektromechanische Schütze und Motorstarter (IEC 60947-4-1:2018/COR1:2020); Deutsche Fassung EN IEC 60947-4-1:2019/AC:2020-05*

DIN EN IEC 60947-4-1 Berichtigung 2 (VDE 0660-102 Berichtigung 2):2021-11, *Niederspannungsschaltgeräte — Teil 4-1: Schütze und Motorstarter — Elektromechanische Schütze und Motorstarter (IEC 60947-4-1:2018/COR2:2021); Deutsche Fassung EN IEC 60947-4-1:2019/AC:2021-04*

DIN EN 60947-5-1 (VDE 0660-200):2018-03, *Niederspannungsschaltgeräte — Teil 5-1: Steuergeräte und Schaltelemente — Elektromechanische Steuergeräte (IEC 60947-5-1:2016 + COR1:2016); Deutsche Fassung EN 60947-5-1:2017*

DIN EN 60204-1 (VDE 0113-1):2019-06, *Sicherheit von Maschinen — Elektrische Ausrüstung von Maschinen — Teil 1: Allgemeine Anforderungen (IEC 60204-1:2016, modifiziert); Deutsche Fassung EN 60204-1:2018*

DIN EN 60730-2-5 (VDE 0631-2-5):2020-01, *Automatische elektrische Regel- und Steuergeräte — Teil 2-5: Besondere Anforderungen an automatische elektrische Brenner-Steuerungs- und Überwachungssysteme (IEC 60730-2-5:2013, modifiziert + A1:2017); Deutsche Fassung EN 60730-2-5:2015 + A1:2019*

E DIN EN 60730-2-5/A2 (VDE 0631-2-5/A2):2022-08*, *Automatische elektrische Regel- und Steuergeräte — Teil 2-5: Besondere Anforderungen an automatische elektrische Brenner-Steuerungs- und Überwachungssysteme (IEC 60730-2-5:2013/A2:2021); Deutsche Fassung EN 60730-2-5:2015/A2:2021*

DIN EN 61508-1 (VDE 0803-1):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010); Deutsche Fassung EN 61508-1:2010*

DIN EN 61508-2 (VDE 0803-2):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010*

DIN EN 61508-3 (VDE 0803-3):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 3: Anforderungen an Software (IEC 61508-3:2010); Deutsche Fassung EN 61508-3:2010*

DIN EN 61508-4 (VDE 0803-4):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010); Deutsche Fassung EN 61508-4:2010*

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

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

DIN EN 61508-7 (VDE 0803-7):2011-02, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme — Teil 7: Überblick über Verfahren und Maßnahmen (IEC 61508-7:2010); Deutsche Fassung EN 61508-7:2010*

DIN EN 61131-3:2014-06, *Speicherprogrammierbare Steuerungen — Teil 3: Programmiersprachen (IEC 61131-3:2013); Deutsche Fassung EN 61131-3:2013*

DIN EN 61511-1 (VDE 0810-1):2019-02, *Funktionale Sicherheit — PLT-Sicherheitseinrichtungen für die Prozessindustrie — Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Hardware und Anwendungsprogrammierung (IEC 61511-1:2016 + COR1:2016 + A1:2017); Deutsche Fassung EN 61511-1:2017 + A1:2017*

DIN EN 61511-2 (VDE 0810-2):2019-02, *Funktionale Sicherheit — PLT-Sicherheitseinrichtungen für die Prozessindustrie — Teil 2: Anleitungen zur Anwendung von IEC 61511-1 (IEC 61511-2:2016); Deutsche Fassung EN 61511-2:2017*

DIN EN 61511-3 (VDE 0810-3):2019-02, *Funktionale Sicherheit — PLT-Sicherheitseinrichtungen für die Prozessindustrie — Teil 3: Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel (IEC 61511-3:2016); Deutsche Fassung EN 61511-3:2017*

DIN EN IEC 62061 (VDE 0113-50):2023-02, *Sicherheit von Maschinen — Funktionale Sicherheit sicherheitsbezogener Steuerungssysteme (IEC 62061:2021); Deutsche Fassung EN IEC 62061:2021*

Deutsche Fassung

Industrielle Thermoprozessanlagen
und dazugehörige Prozesskomponenten —
Sicherheitsanforderungen —
Teil 4: Schutzsysteme (ISO 13577-4:2022)

Industrial furnaces
and associated processing equipment —
Safety —
Part 4: Protective systems (ISO 13577-4:2022)

Fours industriels et équipements associés —
Sécurité —
Partie 4: Systèmes de protection (ISO 13577-4:2022)

Diese Europäische Norm wurde vom CEN am 27. Juni 2022 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

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

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



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort.....	4
Vorwort.....	5
Einleitung.....	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen.....	7
3 Begriffe.....	8
4 Anforderungen an die Auslegung von Anlageteilen in einem Schutzsystem.....	10
4.1 Allgemeines.....	10
4.2 Anforderungen an Schutzsysteme.....	12
4.2.1 Übersicht der Methoden.....	12
4.2.2 Methode A.....	13
4.2.3 Methode BC.....	14
4.2.4 Methode D.....	16
4.3 Fehlerbetrachtung für den verkabelten Teil von Schutzsystemen.....	17
4.4 Ausfall von Versorgungseinrichtungen.....	18
4.5 Rücksetzen.....	18
5 Benutzerinformationen.....	18
Anhang A (informativ) Erläuterung der Techniken und Maßnahmen zur Vermeidung systematischer Fehler.....	19
A.1 Allgemeines.....	19
A.2 Kompetenzen.....	19
A.3 Vermeidung systematischer Fehler.....	20
Anhang B (normativ) Verkabelung von Schutzsystemen.....	21
B.1 Allgemeines.....	21
B.2 Schutz vor Fehlern des Schutzsystems.....	21
B.3 Maßnahmen zur Vermeidung von Fehlern.....	22
B.4 Hardwareauslegung.....	22
B.4.1 Allgemeine Anforderungen an die Hardware.....	22
B.4.2 Verdrahteter Teil eines Schutzsystems.....	22
B.5 Ordnungsgemäße Eingangsverkabelung.....	24
B.6 Ordnungsgemäße Ausgangsverkabelung.....	27
B.7 Unzulässige Eingangs- und Ausgangsverkabelung.....	29
Anhang C (informativ) Beispiele für die Bestimmung des Sicherheits-Integritäts- oder Performance Level SIL/PL mittels des Risikograph-Verfahrens.....	35
C.1 Allgemeines.....	35
C.2 Beispiele für die Bestimmung des erforderlichen SIL/PL.....	36
C.2.1 Beispiel 1 – Tabelle C.1.....	36
C.2.2 Beispiel 2 – Tabelle C.2.....	36
C.2.3 Risikoeinschätzung und SIL-Zuordnung in Übereinstimmung mit IEC 62061:2021, Anhang A (d. h. Tabelle C.1).....	45
C.2.4 Benutzer-Anleitung für den Risikograph in Übereinstimmung mit IEC 61511-3:2016 (d. h. Tabelle C.2).....	50

Anhang D (informativ) Beispiel eine Risikobeurteilung für eine sicherheitstechnische Funktion mittels des Verfahrens nach der Reihe IEC 61511:2016	56
D.1 Allgemeines	56
D.2 Konzeptbeschreibung der gesteuerten Ausrüstung.....	56
D.3 Gefährdungs- und Risikobeurteilung.....	57
D.3.1 Auslösende Ereignisse	57
D.3.2 Gefährdung – Prozessabweichung – unzureichende Verbrennungsluft	57
D.4 Folgen	57
D.5 Beispiel eines Ereignisbaums	58
D.6 Sicherheitsanforderungsspezifikation des Schutzsystems.....	58
D.6.1 Allgemeine Anforderungen	59
D.6.2 Funktionale Anforderungen an Sicherheitssensoren.....	60
D.6.3 Anforderungen an das Logiksystem, einschließlich Alarm, externem Vergleich und HMI.....	61
D.6.4 Anforderungen an das Stellglied	62
D.6.5 Anforderungen an manuelle Eingriffe	63
D.6.6 Anforderungen an den Anlauf	63
Anhang E (informativ) Beispiele für Schutzfunktionen	64
E.1 Allgemeines	64
E.2 Beispiele für Unterfunktionen.....	70
E.2.1 Übersicht über die verschiedenen Anforderungen an Eingangsunterfunktionen.....	70
E.2.2 Übersicht über die verschiedenen Anforderungen an Ausgangsunterfunktionen.....	78
E.3 Beispiele für Sicherheitsfunktionen.....	79
Anhang F (normativ) Anforderungen an Anwendungssoftware.....	93
Literaturhinweise.....	95

Europäisches Vorwort

Dieses Dokument (EN ISO 13577-4:2022) 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.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2023, und etwaige entgegenstehende nationale Normen müssen bis Januar 2023 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

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.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO 13577-4:2022 wurde von CEN als EN ISO 13577-4:2022 ohne irgendeine Abänderung genehmigt.

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 der 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 Directives, 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 Directives, 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*, in Zusammenarbeit mit dem Europäischen Komitee für Normung (CEN), Technisches Komitee CEN/TC 186, *Industrial thermoprocessing — Safety*, in Übereinstimmung mit der Vereinbarung zur technischen Zusammenarbeit zwischen ISO und CEN (Wiener Vereinbarung) erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 13577-4:2014), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

- Um eine bessere Übersicht zu gewährleisten, wurden die Methoden B und C zu einer neuen Methode BC zusammengefasst,
- Anhang E wurde umgeschrieben. Er enthält mehrere neue Beispiele, die die Bedeutung zuvor missverstandener Elemente besser wiedergeben,
- Anhang B wurde geändert, um eine eindeutige Sprache und Beispiele für normative Verkabelungen aufzunehmen. Der ursprüngliche Anhang F wurde in Anhang B integriert,
- Der Wortlaut wurde angepasst, um eine bessere Übereinstimmung mit IEC 62061, IEC 61511 und ISO 13849-1 zu erreichen.

Eine Auflistung aller Teile der Normenreihe ISO 13577 ist auf der ISO-Internetseite abrufbar.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

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 Methoden treffen, die in diesem Teil von ISO 13577 festgelegt werden. Anforderungen an sicherheitsbezogene Steuerfunktionen von TPE werden in den anderen Teilen von ISO 13577 (d. h. ISO 13577-1, ISO 13577-2, und ISO 13577-3) behandelt.

Dieses Dokument ist dazu vorgesehen, gemeinsam mit ISO 13577-1, ISO 13577-2 und ISO 13577-3 benutzt zu werden. Da die anderen 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 hoher Anforderungsrate ausgegangen wird. Allerdings gibt es Fälle, in denen eine Risikobeurteilung nach IEC 61511 (alle Teile), die die Möglichkeit einer niedrigen Anforderungsrate an das Schutzsystem enthält, für die Auslegung eines TPE-Schutzsystems besser geeignet ist.

Grundsätzlich, wenn die Anforderungen von ISO 13577-1, ISO 13577-2 und ISO 13577-3 (Typ-C-Normen) von denen 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 ausgelegt und gebaut wurden, Vorrang gegenüber den Anforderungen in anderen Normen. Daher gestattet dieses Dokument eine Risikobeurteilung für SRECS [*sicherheitsbezogenes elektrisches Steuerungssystem (en: Safety-Related Electrical Control System)*], in der alternativ eine Risikobeurteilung nach IEC 61511 (alle Teile) gewählt werden kann.

1 Anwendungsbereich

Dieses Dokument legt die Anforderungen an Schutzsysteme fest, die in Industrieöfen und zugehörigen Prozessanlagen (TPE) verwendet werden.

Die funktionalen Anforderungen, die für Schutzsysteme gelten, werden in ISO 13577-1, ISO 13577-2 und ISO 13577-3 festgelegt.

Dieses Dokument gilt nicht für Hochöfen, Konverter (in Stahlwerken), Kessel, befeuerte Erhitzer (einschließlich Reformeröfen) in der petrochemischen und chemischen Industrie.

Dieses Dokument gilt nicht für die elektrische Verkabelung und die Leistungsverkabelung vor dem TPE-Schaltschrank/Schutzsystem.

Dieses Dokument gilt nicht für Schutzsysteme, die vor dem Datum seiner Veröffentlichung hergestellt wurden.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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, *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 41: Contactors and motor-starters — Electromechanical contactors and motor-starters*

IEC 60947-5-1:2016, *Low-voltage switchgear and controlgear — Part 51: 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*

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

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*

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 und die folgenden Begriffe.

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

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

3.1 Stellglied

Teil eines Schutzsystems (3.6), der die physikalischen 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 ein Antrieb, wenn es bzw. er Teil der Sicherheitsfunktion ist).

[QUELLE: IEC 61511-1:2016, 3.2.22 modifiziert: „einer PLT-Betriebs- oder PLT-Sicherheitseinrichtung“ wurde in der Definition zu „Schutzsystem“ geändert.]

3.2 Flammenwächter

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

Anmerkung 1 zum Begriff: Dieses kann aus einem Sensor (3.9), 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 Eingangsinformationen [bereitgestellt durch eine oder mehrere Eingangsfunktionen oder Sensoren (3.9)] zu Ausgangsinformationen [verwendet durch eine oder mehrere Ausgangsfunktionen oder Stellglieder (3.1)] durchführt

Anmerkung 1 zum Begriff: Logikfunktionen werden vom Logiksystem (3.4) eines Schutzsystems (3.6) ausgeführt.

[QUELLE: IEC 61511-1:2016, 3.2.35 modifiziert: In der Definition wurde „Eingangsfunktionen“ zu „Eingangsinformationen und Sensoren“ und „Ausgangsfunktionen“ zu „Ausgangsinformationen oder Stellglieder“ geändert. Anmerkung 1 und Anmerkung 2 der ursprünglichen Beschreibung wurde gestrichen und die Anmerkung 1 zum Begriff wurde hinzugefügt.]

3.4

Logiksystem

Teil eines Schutzsystems (3.6), welches eine oder mehrere Logikfunktionen (3.3) ausführt

Anmerkung 1 zum Begriff: Beispiele sind elektrische Systeme, elektronische Systeme, programmierbare elektronische Systeme, pneumatische Systeme und hydraulische Systeme. Sensoren (3.9) und Stellglieder (3.1) sind nicht Teil des Logiksystems.

[QUELLE: IEC 61511-1:2016, 3.2.36 modifiziert: „eines BPCS oder einer SIS“ wurde in der Definition zu „eines Schutzsystems“ geändert und Anmerkung 1 zum Begriff der ursprünglichen Definition wurde gestrichen.]

3.5

speicherprogrammierbare Steuerung

SPS

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

[QUELLE: IEC 61131-1:2003, 3.5 modifiziert: Der zweite Satz der ursprünglichen Definition und die Anmerkung 1 zum Begriff wurden gestrichen]

3.6

Schutzsystem

instrumentiertes System, das zur Implementierung einer oder mehrerer sicherheitsbezogener Funktion(en) eingesetzt wird und aus einer Kombination von Sensor(en) (3.9), Logiksystem(en) (3.4) und Stellgliedern (3.1) besteht

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

Anmerkung 2 zum Begriff: Als Beispiel, siehe Bild 2.

[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 Sicherheitsgeräten (3.8), ausgelegt um einen sicheren Zustand des Schutzsystems (3.6) zu erreichen oder beizubehalten

[QUELLE: ISO 13574:2015, 2.164]

3.8

Sicherheitsgerät

Gerät, das entweder allein oder als Teil eines Schutzsystems (3.6) zur Durchführung von Schutzfunktionen verwendet wird

BEISPIEL Sensoren (3.9), Begrenzer, Flammenwächter, Feuerungsautomaten, Logiksysteme, Stellglieder (3.1) und automatische Absperrventile.

3.9

Sensor

Gerät, das auf Basis einer Prozessvariable ein Signal erzeugt

BEISPIEL Messwertgeber, Messwertaufnehmer, 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 Auslegung von Anlageteilen in einem Schutzsystem

4.1 Allgemeines

Elektrische Installationen und Ausrüstung müssen den Anforderungen von IEC 60204-1:2016 entsprechen und den vorgesehenen Betriebsbeanspruchungen sowie den äußeren Einflüssen und Gefährdungen 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.

Geräte müssen in Übereinstimmung mit ihren zugehörigen Gebrauchsanleitungen, einschließlich Sicherheitshandbüchern, verwendet werden. Jegliches Gerät, das außerhalb seiner veröffentlichten Gebrauchsanleitung verwendet wird, muss auf seine Eignung für den vorgesehenen Anwendungszweck geprüft und validiert werden.

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

Sensoren (z. B. Druckmesswertgeber, Temperaturmesswertgeber, Durchflussmesswertgeber), die im Schutzsystem verwendet werden, müssen vom Prozessleitsystem unabhängig sein.

ANMERKUNG 1 Betriebsbedingte Informationen können ausgetauscht werden, aber sind nicht in der Lage, die funktionale Sicherheit des Schutzsystems zu beeinträchtigen.

Der sichere Zustand darf nur durch spannungslose Stromkreise realisiert werden.

Die Anforderungen an die funktionale Sicherheit, wie sie in der Reihe ISO 13577 festgelegt sind, müssen in Übereinstimmung mit den Normen der Reihe IEC 61508:2010, der Reihe IEC 61511:2016, IEC 62061:2021 oder ISO 13849-1:—², soweit 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 deren zugehörigen Einrichtungen, dem Heizsystem, der Prozessleittechnik/Bedienebene und dem Schutzsystem.

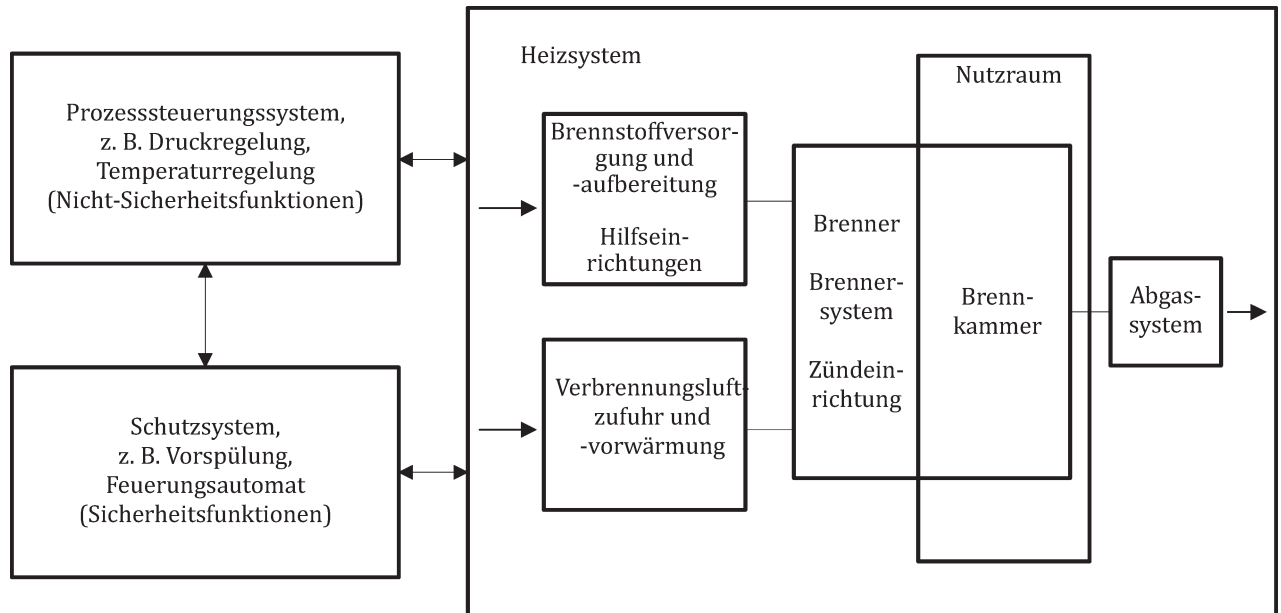


Bild 1 — Blockdiagramm der Steuer- und Schutzsysteme

Es müssen geeignete 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 Abschnitt B.5 und Bild B.10).

Die Verkabelung von sicherheitsrelevanten Sensoren und Aktoren, 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 Feldgeräten 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 Aktoren (z. B. Druckschalter, Gasventile usw.) gegen mechanische Beschädigung (auch z. B. durch Vibration oder Knicken) geschützt werden, um Kurz-, Quer- und Erdschlüsse zu vermeiden.

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

ANMERKUNG 2 Eine Methode zum Schutz vor Kurz-, Quer- und Erdschlüssen ist die Verwendung von Kabelkanälen, Kabeltrassen 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 Erkennung des ersten Fehlers das Schutzsystem allpolig vom Netz trennen.

Anforderungen an Prüfung und Prüfintervalle für Schutzsysteme müssen in der Gebrauchsanleitung festgelegt werden. Außer nach den Vorgaben von Methode D muss die Prüfung aller Sicherheitsfunktionen mindestens jährlich durchgeführt werden. Methode 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 Methoden

Jede oder eine Kombination der drei (3) Methoden 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 eine Methode verwendet werden. Es gibt die folgenden drei Methoden:

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

Bild 2 zeigt die grundlegende Konfiguration eines Schutzsystems.

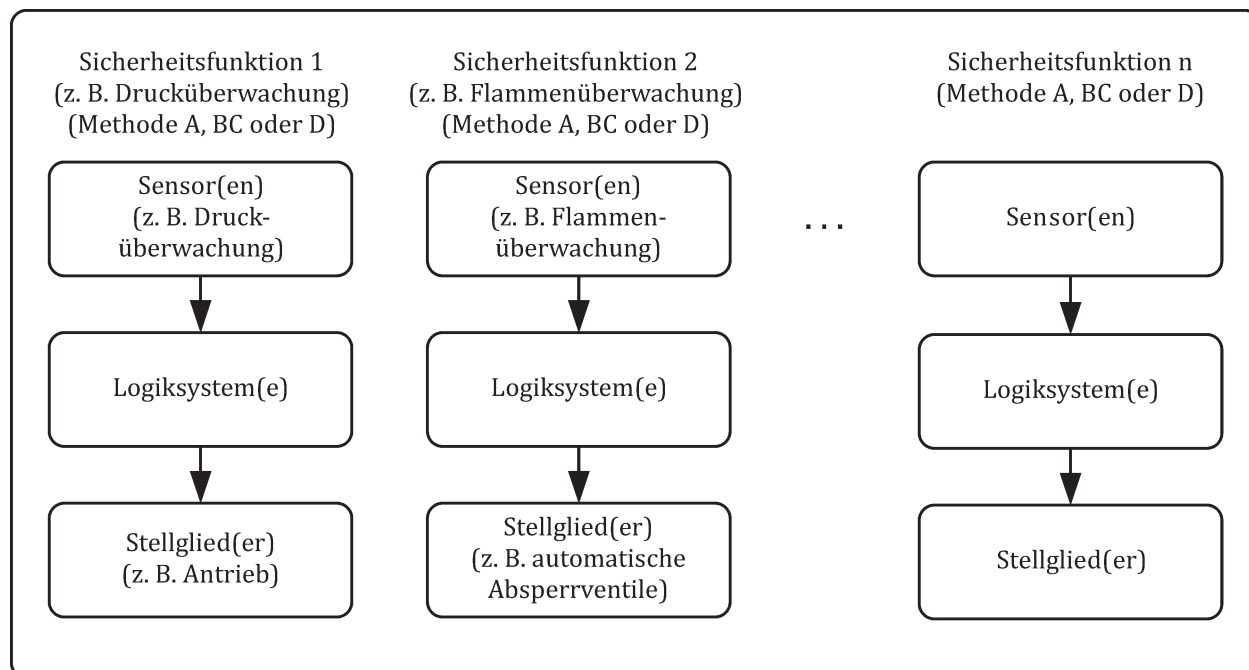


Bild 2 — Grundlegende Konfiguration eines Schutzsystems

Bild 3 zeigt die grundlegenden Eigenschaften der einzelnen Methoden.

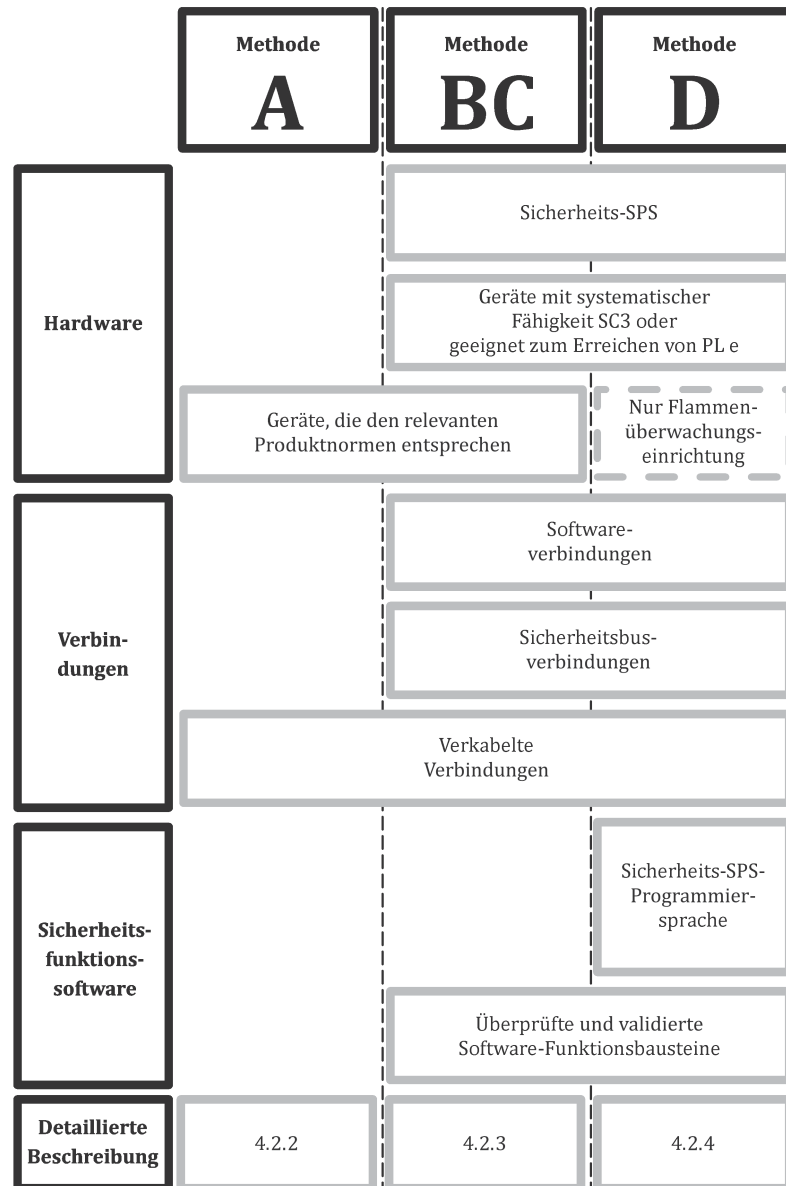


Bild 3 — Überblick über die Methoden

ANMERKUNG 1 Software-Verbindungen sind Verbindungen zwischen Software-Funktionsbausteinen, Sicherheits-SPS-Eingängen und Sicherheits-SPS-Ausgängen. Sie ähneln verkabelten Verbindungen zwischen Geräten.

ANMERKUNG 2 Die Sicherheitsfunktionssoftware ist entweder ein Software-Funktionsbaustein oder ein Programm zur Ausführung von Sicherheitslogikfunktionen (z. B. Vorspülung, Feuerungsautomat), siehe 4.2.2.

Zu Beispielen für Schutzfunktionen der verschiedenen Methoden siehe Anhang E.

4.2.2 Methode A

Methode A muss ein verkabeltes System sein, in dem alle Geräte (d. h. Sensoren, Logiksysteme und Stellglieder, wie in Bild 4 beschrieben) den Produktnormen nach der Reihe ISO 13577 entsprechen.

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

Die folgenden Anforderungen an die Verkabelung müssen erfüllt sein:

- a) alle Logiksysteme müssen durch die Geräte und über die direkten Verbindungen zwischen den Geräten gespeist werden;
- b) Geräte mit festen Programmsprachen, die die entsprechenden Produktnormen erfüllen, sind zulässig;
- c) Verbindungen durch Datenkommunikationsbusse sind unzulässig;
- d) die Verkabelung des Schutzsystems muss die Anforderungen in Anhang B erfüllen.

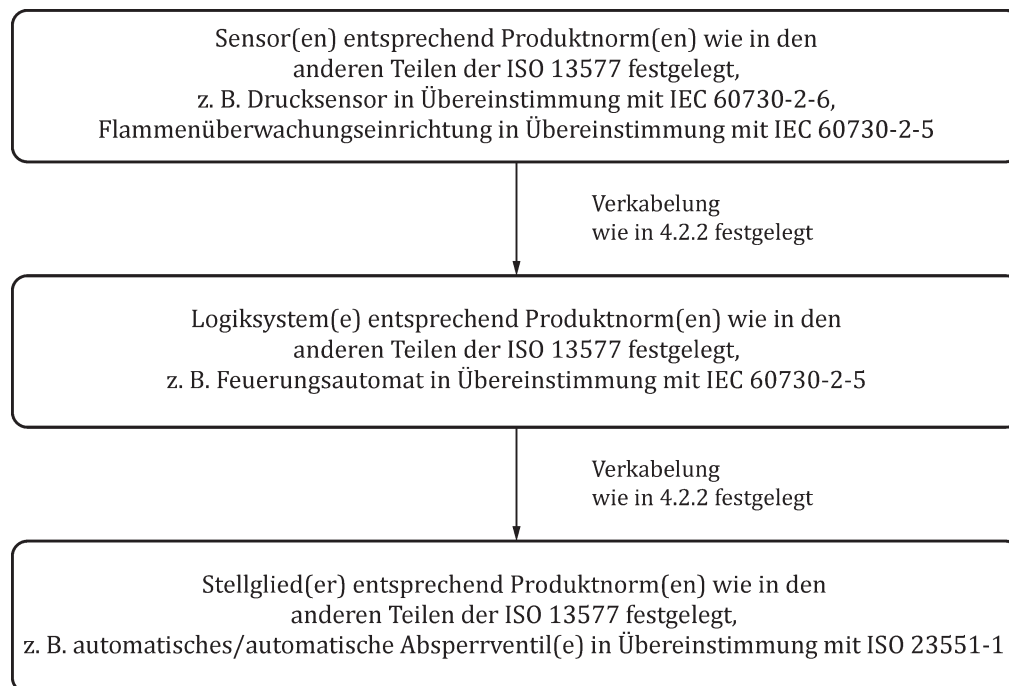


Bild 4 — Hardwarekonfiguration bei Methode A

ANMERKUNG Die in 4.2.2 verwendeten Sicherheitsgeräte entsprechen spezifischen Sicherheitsanforderungen, die auf den Anwendungsbereich und die funktionalen Anforderungen an diese Geräte abgestimmt sind, wie sie in den entsprechenden Produktnormen für Sicherheitsgeräte gefordert werden, z. B. Feuerungsautomaten, Ventilprüfsysteme, Drucksensoren, automatische Absperrventile. Selbst ohne zusätzliche SIL/PL-Zertifizierung dieser Sicherheitsgeräte entsprechen die Sicherheitsanforderungen für den Gebrauch der Sicherheitsgeräte den entsprechenden Produktnormen. Eine Implementierung des Schutzsystems nach 4.2.2 ist eine von verschiedenen alternativen Methoden.

4.2.3 Methode BC

Methode BC muss aus einer Kombination von Geräten bestehen, die den einschlägigen Produktnormen entsprechen, und/oder aus SIL/PL-fähigen Geräten, für die es keine Produktnorm gibt. Die Verwendung von Sicherheits-SPSen ist optional (siehe Bild 5). Die folgenden Anforderungen an die Verkabelung müssen erfüllt sein:

- a) alle Logiksysteme müssen durch die Geräte und über die direkten Verbindungen zwischen den Geräten gespeist werden;
- b) Geräte mit festen Programmsprachen, die die entsprechenden Produktnormen erfüllen, sind zulässig;
- c) Verbindungen müssen verkabelt oder durch einen Sicherheitsbus oder durch Softwareverbindungen hergestellt sein;
- d) die Verkabelung des Schutzsystems muss die Anforderungen in Anhang B erfüllen.

Bei Verwendung eines programmierbaren Logiksystems (z. B. Sicherheits-SPS) ist eine Sicherheitsfunktionssoftware nur in Form von überprüften und validierten SIL 3-fähigen Software-Funktionsblöcken zulässig (siehe Bild 5). Zusätzlich müssen die folgenden Anforderungen erfüllt werden:

- i) Wenn ein programmierbares Gerät eine Sicherheitsfunktion implementiert, die ganz oder teilweise in einer einschlägigen Produktnorm behandelt wird, so ist die Softwarefunktion im Hinblick auf die geltenden Anforderungen der entsprechenden Produktnorm zu überprüfen und zu validieren, einschließlich, aber nicht beschränkt auf die Abläufe und Zeitvorgaben der Produktnorm;
- ii) Software-Verbindungen in einem programmierbaren Gerät müssen durch einen Funktionstest nach den Normen zur funktionalen Sicherheit überprüft und dokumentiert werden;
- iii) Software-Programmiersprachen für SPS müssen IEC 61131-3:2013 entsprechen;
- iv) 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 Geräten erfolgt in der Regel durch eine Benannte Stelle, ein akkreditiertes nationales Prüflabor oder durch eine Organisation nach ISO/IEC 17025.

Die Sicherheitsfunktionen müssen sich in einem sicherheitsbewerteten Gerät oder in einem externen Gerät befinden, das unter die entsprechende Produktnorm fällt.

Geräte (Sicherheits-SPS, Zeitsteuergeräte, usw.), die NICHT von Produktnormen abgedeckt werden, müssen die folgenden Anforderungen erfüllen:

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

Geräte mit einer geringeren Kapazität als SIL 3/PL e sind zulässig, sofern die SIL/PL-Anforderungen an die Sicherheitsschleife (Sicherheitsfunktion) auf der Grundlage der Risikobeurteilung bestimmt wurden. Die systematische Fähigkeit der Geräte muss mindestens dem festgelegten SIL/PL entsprechen.

Wenn der SIL eines Geräts auf der Grundlage des bewährten Betriebs bestimmt wird, müssen die Anforderungen der Reihe IEC 61508:2010 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 Gebrauchsanleitungen oder Sicherheitshandbüchern der Geräte, wie etwa das Prüfintervall, müssen eingehalten werden.

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



Bild 5 — Hardwarekonfiguration bei Methode BC

4.2.3.1 Anforderungen an Anwendungssoftware von programmierbaren Logiksystemen

Anwendungssoftware muss in Übereinstimmung mit den Methoden der funktionalen Sicherheit programmierbarer elektronischer sicherheitsbezogener Systeme entwickelt werden, die in den Anforderungen der Reihe IEC 61508:2010, der Reihe IEC 61511:2016, IEC 62061:2021, ISO 13849-1:— oder Anhang F definiert sind.

ANMERKUNG Anhang F enthält Kriterien für Anwendungen auf der Grundlage der Reihe IEC 61508:2010.

Die Gebrauchsanleitungen der Hersteller für die Geräte müssen alle anwendbaren Anforderungen der IEC 61508-3:2010 enthalten, wenn Softwareänderungen durch den Endanwender veranlasst werden.

4.2.4 Methode D

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

ANMERKUNG 1 Siehe Anhang D für die Methode in Übereinstimmung mit der Reihe IEC 61511:2016.

ANMERKUNG 2 Siehe Anhang D für eine Methode der Gefährdungs- und Risikobewertung nach der Reihe IEC 61511:2016. Die Anwendung anderer Methoden nach diesem Dokument ist möglich. C.2.2 enthält ein Beispiel für die Bestimmung des SIL nach diesem Dokument.

Methode D muss auch die folgenden Anforderungen erfüllen:

- a) der Flammenwächter muss IEC 60730-2-5:2013+AMD 1:2017+AMD 2:2020 CSV entsprechen;
- b) alle Anforderungen der SPS und der Sicherheitsgeräte müssen in Übereinstimmung mit den Gebrauchsanleitungen der Hersteller und den Produktsicherheitshandbüchern verwendet werden;
- c) jede Anforderung an die funktionale Sicherheit, wie sie in der Reihe ISO 13577 festgelegt ist, muss nach den Normen für funktionale Sicherheit auf ihren Bedarf hin bewertet und mit dem erforderlichen SIL/PL für jede Funktion umgesetzt werden. Sicherheitsfunktionen des sicherheitsbezogenen Systems, wie z. B. Feuerungsautomat, Ventilprüfung, Luft-Brennstoff-Verbundregelung, usw., müssen den Sicherheitsanforderungen der entsprechenden Produktnormen entsprechen;

ANMERKUNG 3 Eine erweiterte Risikobeurteilung in Methode D kann Vorrang vor den Sicherheitsanforderungen in der Reihe ISO 13577 haben. Aufgrund der Art der erweiterten Risikobeurteilung im Rahmen von Methode D wird die allgemeine Sicherheit nicht verringert und erfüllt oder übertrifft die vorgesehenen Anforderungen der Reihe ISO 13577.

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

ANMERKUNG 4 Die Verifizierung und Validierung des SIL/PL wird in der Regel mit einem unabhängigen Prüfverfahren durchgeführt, ähnlich wie bei der Überprüfung durch Dritte.

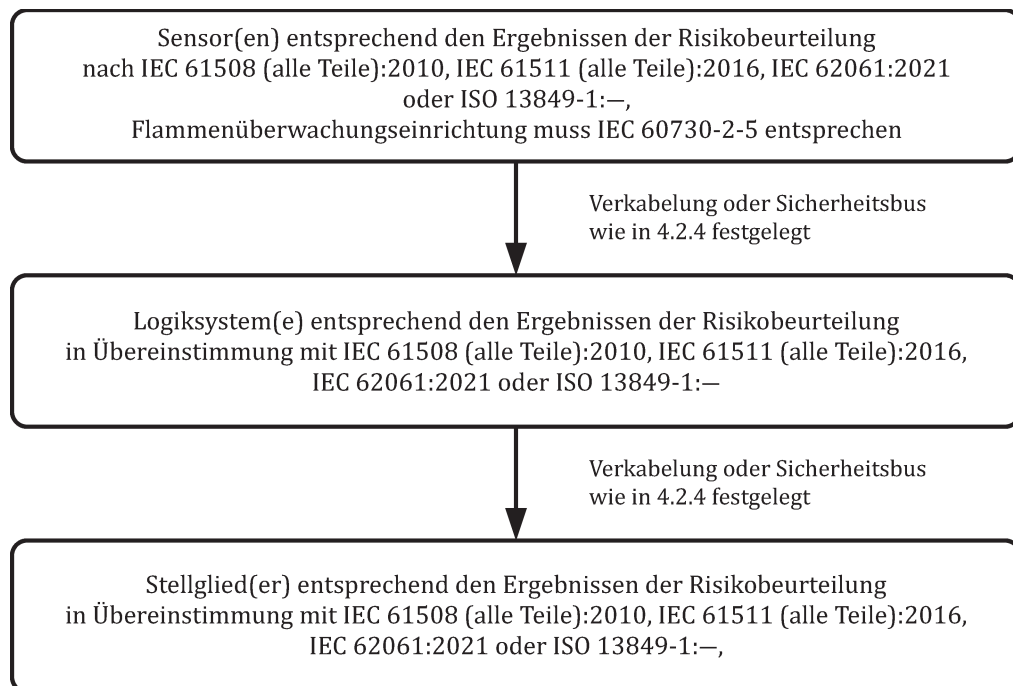


Bild 6 — Hardwarekonfiguration bei Methode D

4.3 Fehlerbeurteilung für den verkabelten Teil von Schutzsystemen

Das Schutzsystem muss so ausgelegt sein, dass die nach der Reihe ISO 13577 erforderlichen Geräte 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 Geräte müssen in Übereinstimmung mit den Gebrauchsanleitungen der Hersteller verkabelt werden.
- c) Wenn bei Methode BC Zeitsteuergeräte, die nicht, wie in der Reihe 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 Gerätekontaktleistung zu begrenzen.

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 Methode D gestattet, muss an Geräten, 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 vor keiner Sicherheitsfunktion Vorrang haben.

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

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

Die Gebrauchsanleitung 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 Gebrauchsanleitung enthalten sein.

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, welche die Schutzmaßnahmen und den Betrieb detailliert beschreibt, muss in der Anlagendokumentation enthalten sein.

³ In Vorbereitung. Die zweite Ausgabe von 13577-2 soll im Jahr 2022 veröffentlicht 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 menschlichen Fehlern in den Festlegungen und der Auslegung des Schutzsystems. Systematische Fehler können verborgen sein, bis bestimmte Bedingungen auftreten, und könnten unter Umständen lange nicht entdeckt werden. Diese spezifischen Bedingungen führen dazu, dass alle Geräte, die innerhalb dieses Systems hergestellt wurden, in gleicher Weise ausfallen. Daher ist es sehr 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, kompetent für die jeweiligen Aktivitäten, für die sie verantwortlich sind, sein. 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) technisches Wissen, Schulung und Erfahrung im Hinblick auf
 - 1) die Prozessanwendung,
 - 2) die jeweilige verwendete Technologie (z. B. Elektrik, Elektronik, Programmierung) und
 - 3) die Sensoren und Stellglieder;
- b) sicherheitstechnisches Wissen (z. B. Prozesssicherheitsanalyse);
- c) Kenntnisse der gesetzlichen und regulatorischen funktionalen Sicherheitsanforderungen;
- d) angemessene Management- und Führungskompetenzen, die für die jeweilige Rolle in der Auslegung geeignet sind;
- e) Verständnis der potenziellen Folgen 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 unterstützen, auszuwählen:

- a) Transparenz, Modularität und andere Merkmale, die Komplexität beherrschbar machen;
- b) eindeutiger und präziser Ausdruck von
 - Funktionalität,
 - Teilsystem- und Elementschnittstellen,
 - ablauf- und zeitbezogenen Informationen und
 - Gleichzeitigkeit und Synchronisation;
- c) eindeutige und präzise Dokumentation und Kommunikation von Informationen;
- d) Überprüfung und Validierung.

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

Während der Auslegung sind die Aktivitäten, die im Entwicklungsbereich durchgeführt werden können, von denen, die einen Zugang zur Anlage des Anwenders erfordern, zu unterscheiden und zu bestimmen.

Wartungsanforderungen müssen während der Auslegungsphase fixiert werden, um sicherzustellen, dass die Anforderungen an die Sicherheitsintegrität der Schutzsysteme über ihre Lebenszyklen hinweg dauerhaft 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 auszulegen, und die Prüfplandokumentation, einschließlich der folgenden Punkte, ist zu erstellen:

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

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

Anhang B (normativ)

Verkabelung von Schutzsystemen

B.1 Allgemeines

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

Dieser Anhang beschreibt, wie das Schutzsystem verkabelt werden muss, sodass das Sicherheitsniveau nicht verringert wird.

Dieser Anhang gilt für die Verkabelung innerhalb des Logiksystems und für die Verkabelung zwischen dem Logiksystem und den Geräten, die direkt oder indirekt die Stellglieder steuern. Darüber hinaus gilt er für die Feldverkabelung zwischen Geräten wie Sensoren, Verriegelungen, Aktoren, Stellgliedern, Flammenwächtern, Zündvorrichtungen, usw.

Um das Sicherheitsniveau des verkabelten Schutzsystems aufrecht zu erhalten, 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 beherrschen.

Die Fehlerbeurteilung 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 Wirksamkeit des Schutzsystems durch Fehlervermeidungsmethoden beeinträchtigen könnten, wie in den Beispielen in Bild B.2 bis Bild B.8 dargestellt, minimiert werden müssen; oder

ANMERKUNG 1 Beispiele UNZULÄSSIGER Verkabelung sind in Bild B.10 bis Bild 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 Beherrschung von Fehlern).

Das gleichzeitige Auftreten von zwei unabhängigen Fehlern in unterschiedlichen Geräten 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 nach 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 intermittierenden Betrieb ist der Betrieb nicht zulässig, wenn beim Anfahren ein Fehler festgestellt wird.

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

ANMERKUNG 2 24 h ist eine Angabe zur MTTR (mittlere Dauer bis 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 Geräten und
- c) die Überprüfung von Funktionen und Verbindungen durch Tests.

Bei anwendungsspezifischen integrierten Schaltkreisen muss besonders auf Vorbeugungsmaßnahmen zur Fehlervermeidung geachtet werden.

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 Schutzfunktionen 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 Fehlerbeurteilung nach Bild B.1 zum Abbruch führt.

Bei der Fehlerbeurteilung 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 Geräte einen sicheren Zustand erreichen (z.B. Ruhestrombetrieb bei Binärkreisen), kann abgesehen von den folgenden Maßnahmen eine einkanalige Ausführung des jeweiligen Teiles ausreichend sein. Kann diese Annahme nicht getroffen werden (z. B. beim Arbeitsstrombetrieb in Binärkreisen), so würde ein zweiter, üblicherweise bestromter, unabhängiger Auslösekanal vorgesehen werden (z. B. Ruhestrombetrieb bei Binärkreisen), damit die Wirksamkeit des Schutzsystems (einschließl. aller pneumatischen, hydraulischen und mechanischen Stellglieder) für diese Funktion sichergestellt wird.

Bei Ausgangsschaltungen müssen mindestens zwei überwachte Abschaltglieder, d. h. Schütze oder Relais, vorgesehen werden, um eine Sicherheitsabschaltung der gesamten Brennstoffzufuhr zu gewährleisten.

Reed-Relais dürfen nicht für Schutzfunktionen verwendet werden.

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

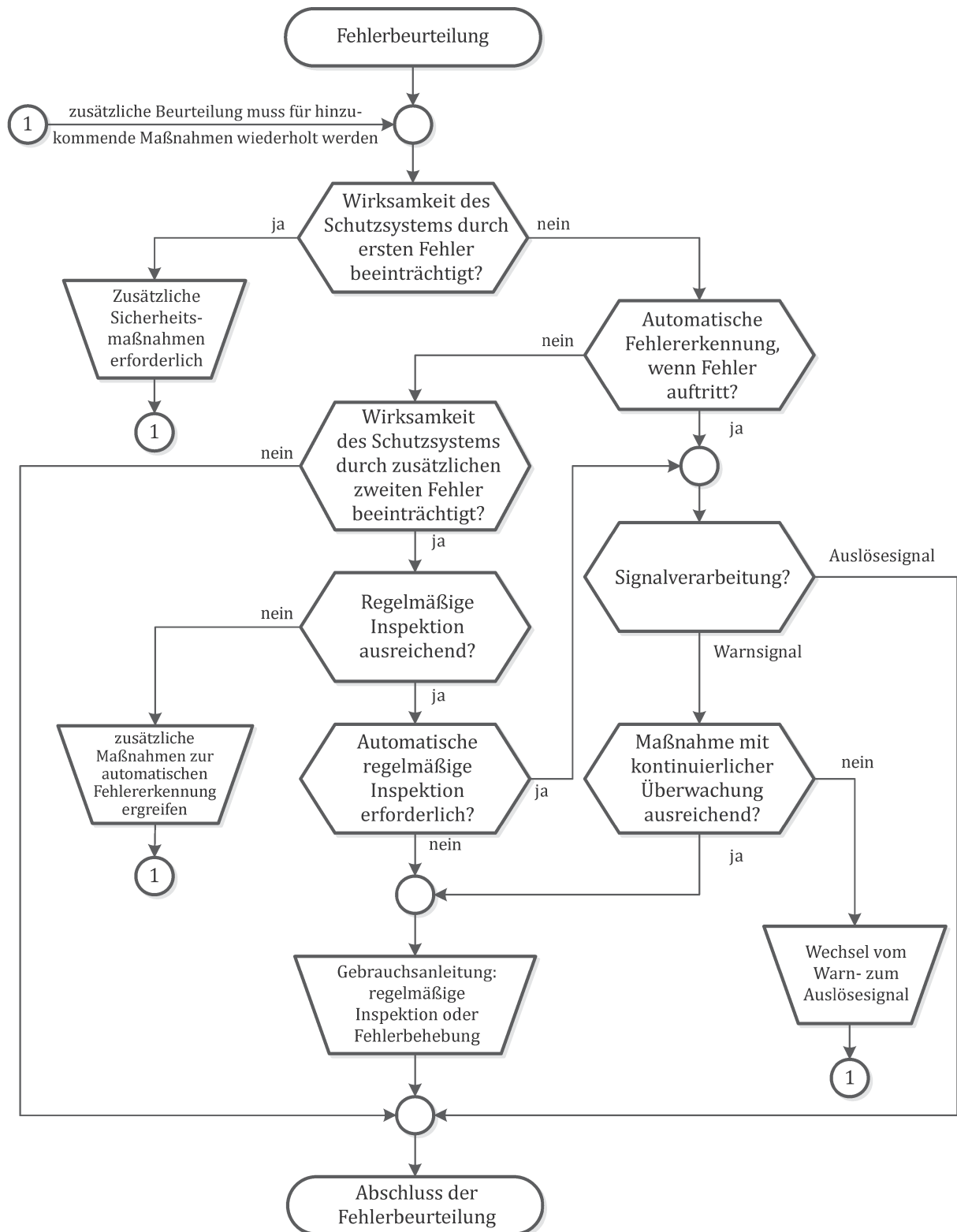
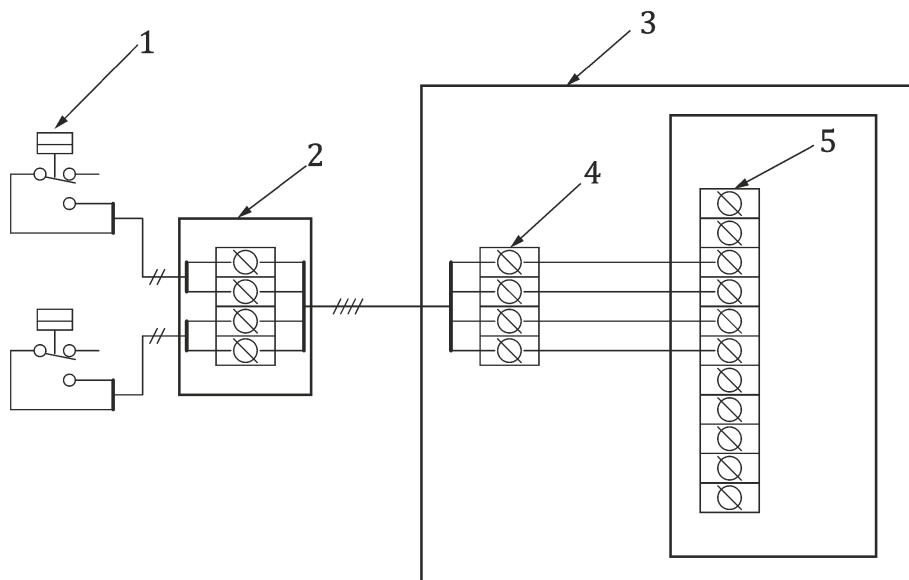


Bild B.1 — Fehlerbeurteilung für den verkabelten Teil eines Schutzsystems

B.5 Ordnungsgemäße Eingangsverkabelung

Dieser Abschnitt enthält Beispiele für Techniken zur Vermeidung von Fehlern durch die externe Verkabelung.

Bild B.2 zeigt eine Technik, die bei Verwendung der Schutzsystemmethoden 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 der Sensoren auf.

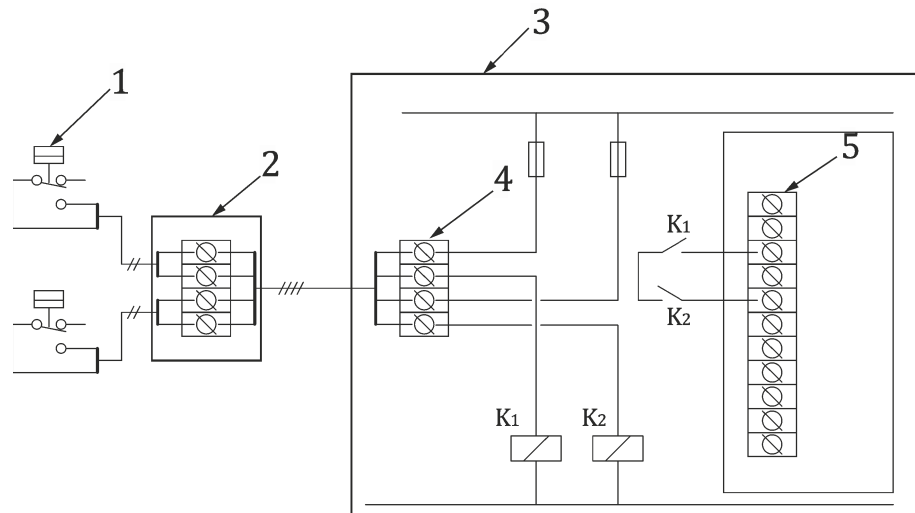


Legende

- | | |
|--|-----------------------------|
| 1 digitaler Sensor (z. B. Drucksensor) | 4 Gehäuseanschlüsse |
| 2 Feldanschlusskasten | 5 digitale Logik-Anschlüsse |
| 3 Gehäuse mit Logik | |

Bild B.2 — Geschützte Verkabelung

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

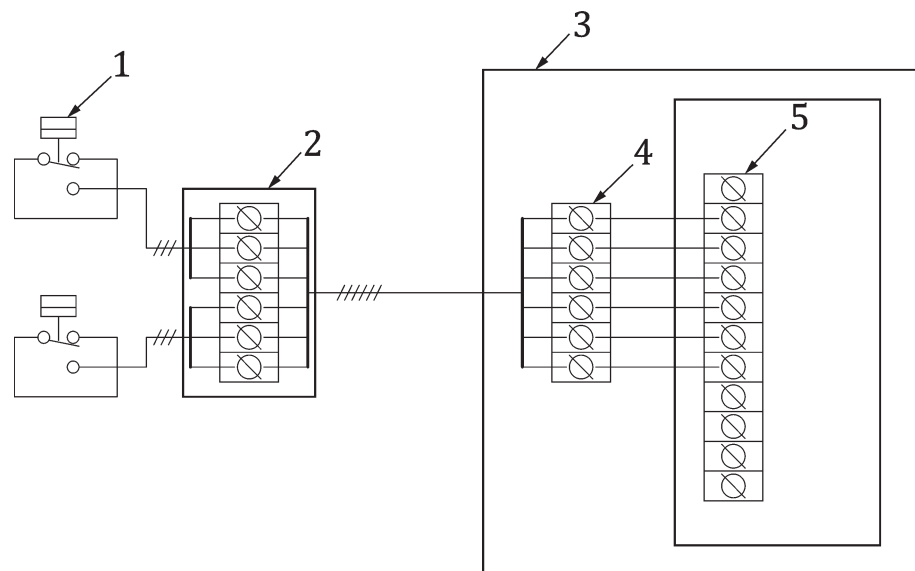


Legende

- | | | | |
|---|--------------------------------------|---------------------------------|-------------------------------|
| 1 | digitaler Sensor (z. B. Drucksensor) | 4 | Gehäuseanschlüsse |
| 2 | Feldanschlusskasten | 5 | digitale Logik-Anschlüsse |
| 3 | Gehäuse mit Logik | K ₁ , K ₂ | Zusatzrelais (siehe Bild B.9) |

Bild B.3 — Geschützte Verkabelung mit zusätzlichen Relais

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

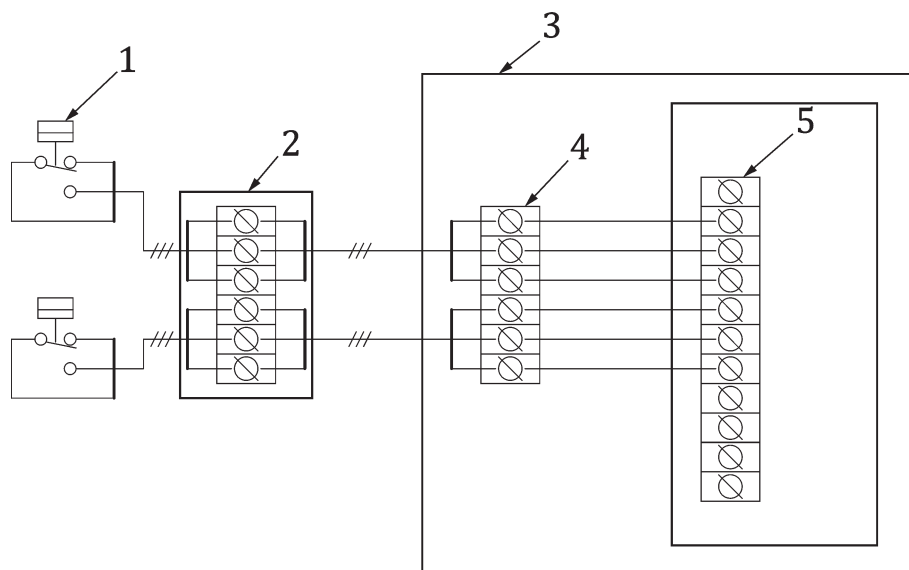


Legende

- | | | | |
|---|--------------------------------------|---|---------------------------|
| 1 | digitaler Sensor (z. B. Drucksensor) | 4 | Gehäuseanschlüsse |
| 2 | Feldanschlusskasten | 5 | digitale Logik-Anschlüsse |
| 3 | Gehäuse mit Logik | | |

Bild B.4 — Überwachung beider Zustände

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

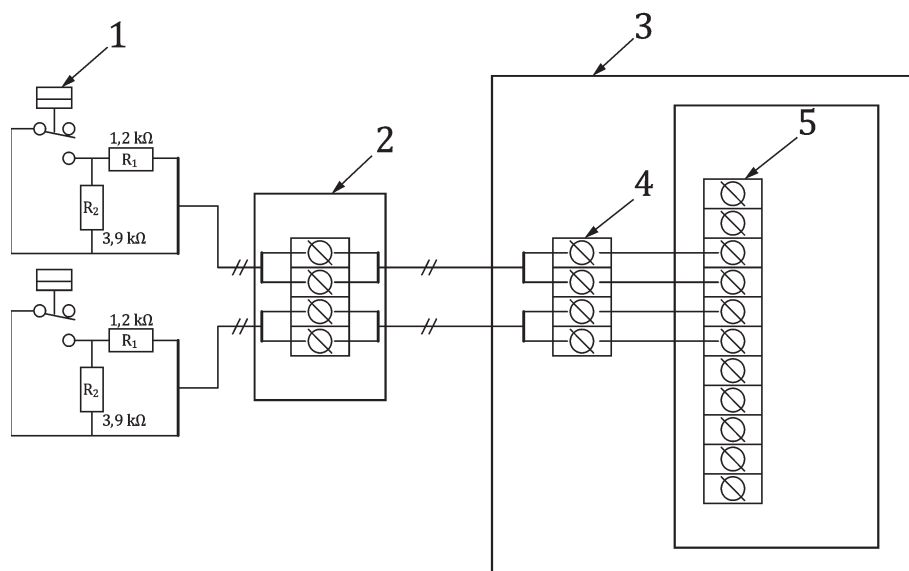


Legende

- | | |
|--|-----------------------------|
| 1 digitaler Sensor (z. B. Drucksensor) | 4 Gehäuseanschlüsse |
| 2 Feldanschlusskasten | 5 digitale Logik-Anschlüsse |
| 3 Gehäuse mit Logik | |

Bild B.5 — Überwachung beider Zustände, mehrere Kabel

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



Legende

- | | |
|--|--------------------------------------|
| 1 digitaler Sensor (z. B. Drucksensor) | 5 analoge Logik-Anschlüsse |
| 2 Feldanschlusskasten | R ₁ Widerstand 1 (1,2 kΩ) |
| 3 Gehäuse mit Logik | R ₂ Widerstand 2 (3,9 kΩ) |
| 4 Gehäuseanschlüsse | |

Die Eingangskarte sollte in der Lage sein, Unterbrechungen und Kurzschlüsse zu erkennen.

ANMERKUNG Die in dem Bild angegebenen Werte sind nur Beispiele für 4 mA bis 20 mA.

Bild B.6 — Überwachung durch Analogwert