

	DIN EN 50402 (VDE 0400-70)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE
ICS 13.320 Ersatz für DIN EN 50402 (VDE 0400-70):2006-03 Siehe jedoch Beginn der Gültigkeit Elektrische Geräte für die Detektion und Messung von brennbaren oder toxischen Gasen und Dämpfen oder Sauerstoff – Anforderungen an die funktionale Sicherheit von ortsfesten Gaswarnsystemen; Deutsche Fassung EN 50402:2005 + A1:2008 Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen – Requirements on the functional safety of fixed gas detection systems; German version EN 50402:2005 + A1:2008 Matériel électrique pour la détection et la mesure des gaz ou vapeurs combustibles ou toxiques, ou de l'oxygène – Exigences relatives à la fonction de sécurité des systèmes fixes de détection de gaz; Version allemande EN 50402:2005 + A1:2008 Gesamtumfang 73 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE		

Beginn der Gültigkeit

Die von CENELEC am 2005-07-01 angenommene EN 50402 gilt zusammen mit der am 2008-03-01 angenommenen Änderung A1 als DIN-Norm ab 2009-01-01.

Daneben darf **DIN EN 50402 (VDE 0400-70):2006-03** noch bis 2011-03-01 angewendet werden.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 50402/A1 (VDE 0400-70/A1):2007-10.

Für diese Norm ist das nationale Arbeitsgremium UK 966.1 „Mess- und Warngeräte für gefährliche Gase“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (www.dke.de) zuständig.

Die CENELEC-Abänderungen sind im Norm-Text mit einem Randstrich gekennzeichnet.

Änderungen

Gegenüber **DIN EN 50402 (VDE 0400-70):2006-03** wurden folgende Änderungen vorgenommen:

- a) in 5.1 Text bezüglich Störungsmeldung ergänzt;
- b) in 5.4.1, 5.4.2, 5.6 und 5.7.2 Fehler in den hierarchischen Abstufungen der Anforderungen behoben.

Frühere Ausgaben

DIN EN 50402 (VDE 0400-70): 2006-03

Nationaler Anhang NA (informativ)

Zusammenhang mit Europäischen und Internationalen Normen

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

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

Eine Information über den Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen ist in Tabelle NA.1 wiedergegeben.

Tabelle NA.1

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN ISO 13849-1:2006	—	DIN EN ISO 13849-1:2007-07	—
EN 45544-1:1999	—	DIN EN 45544-1 (VDE 0400-22-1):2000-10	VDE 0400-22-1
EN 45544-2:1999	—	DIN EN 45544-2 (VDE 0400-22-2):2000-10	VDE 0400-22-2

Tabelle NA.1 (fortgesetzt)

Europäische Norm	Internationale Norm	Deutsche Norm	Klassifikation im VDE-Vorschriftenwerk
EN 45544-3:1999	—	DIN EN 45544-3 (VDE 0400-22-3):2000-10	VDE 0400-22-3
EN 45544-4:1999	—	DIN EN 45544-4 (VDE 0400-22-4):2000-10	VDE 0400-22-4
EN 50073:1999 ^{*)}	—	—	—
EN 50104:2002	—	DIN EN 50104 (VDE 0400-20):2002-10	VDE 0400-20
EN 50241-1:1999	—	DIN EN 50241-1 (VDE 0400-40-1):2000-04	VDE 0400-40-1
EN 50241-2:1999	—	DIN EN 50241-2 (VDE 0400-40-2):2000-04	VDE 0400-40-2
EN 50271:2001	—	DIN EN 50271 (VDE 0400-21):2002-05	VDE 0400-21
EN 61508-1:2001	IEC 61508-1:1998 + Corrigendum:1999	DIN EN 61508-1 (VDE 0803-1):2002-11	VDE 0803-1
EN 61508-2:2001	IEC 61508-2:2000	DIN EN 61508-2 (VDE 0803-2):2002-12	VDE 0803-2
EN 61508-3:2001	IEC 61508-3:1998 + Corrigendum:1999	DIN EN 61508-3 (VDE 0803-3):2002-12	VDE 0803-3
EN 61508-4:2001	IEC 61508-4:1998 + Corrigendum:1999	DIN EN 61508-4 (VDE 0803-4):2002-11	VDE 0803-4
EN 61508-5:2001	IEC 61508-5:1998 + Corrigendum:1999	DIN EN 61508-5 (VDE 0803-5):2002-11	VDE 0803-5
EN 61508-6:2001	IEC 61508-6:2000	DIN EN 61508-6 (VDE 0803-6):2003-06	VDE 0803-6
EN 61508-7:2001	IEC 61508-7:2000	DIN EN 61508-7 (VDE 0803-7):2003-06	VDE 0803-7
EN 61511-1:2004	IEC 61511-1:2003 + Corrigendum:2004	DIN EN 61511-1 (VDE 0810-1):2005-05	VDE 0810-1
EN 60079-29-1:2007	IEC 60079-29-1:2007, modifiziert	DIN EN 60079-29-1 (VDE 0400-1):2008-07	VDE 0400-1
EN 60079-29-2:2007	IEC 60079-29-2:2007	DIN EN 60079-29-2 (VDE 0400-2):2008-07	VDE 0400-2
EN 61779-1:2000 ^{**)}	—	—	—
EN 61779-2:2000 ^{**)}	—	—	—
EN 61779-4:2000 ^{**)}	—	—	—
EN 61779-5:2000 ^{**)}	—	—	—

^{*)} Ersetzt durch EN 60079-29-2:2007.

^{**)} Ersetzt durch EN 60079-29-1:2007.

Nationaler Anhang NB (informativ)

Literaturhinweise

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

DIN EN 45544-1 (VDE 0400-22-1), *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 1: Allgemeine Anforderungen und Prüfverfahren*

DIN EN 45544-2 (VDE 0400-22-2), *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und die direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 2: Anforderungen an das Betriebsverhalten von Geräten für Konzentrationsmessungen im Bereich von Grenzwerten*

DIN EN 45544-3 (VDE 0400-22-3), *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 3: Anforderungen an das Betriebsverhalten von Geräten für Konzentrationsmessungen weit oberhalb von Grenzwerten*

DIN EN 45544-4 (VDE 0400-22-4), *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 4: Leitfaden für Auswahl, Installation, Einsatz und Instandhaltung*

DIN EN 50104 (VDE 0400-20), *Elektrische Geräte für die Detektion und Messung von Sauerstoff – Anforderungen an das Betriebsverhalten und Prüfverfahren*

DIN EN 50241-1 (VDE 0400-40-1), *Anforderungen an Geräte mit offener Messstrecke für die Detektion brennbarer oder toxischer Gase und Dämpfe – Teil 1: Allgemeine Anforderungen und Prüfverfahren*

DIN EN 50241-2 (VDE 0400-40-2), *Anforderungen an Geräte mit offener Messstrecke für die Detektion brennbarer oder toxischer Gase und Dämpfe – Teil 2: Anforderungen an das Betriebsverhalten von Geräten für die Detektion brennbarer Gase*

DIN EN 50271 (VDE 0400-21), *Elektrische Geräte für die Detektion und Messung von brennbaren Gasen, giftigen Gasen oder Sauerstoff - Anforderungen und Prüfungen für Warngeräte, die Software und/oder Digitaltechnik nutzen*

DIN EN 61508-1 (VDE 0803-1), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen*

DIN EN 61508-2 (VDE 0803-2), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme*

DIN EN 61508-3 (VDE 0803-3), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software*

DIN EN 61508-4 (VDE 0803-4), *Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen*

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

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

DIN EN 61508-7 (VDE 0803-7), *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen*

DIN EN 61511-1 (VDE 0810-1), *Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware*

DIN EN 60079-29-1 (VDE 0400-1), *Explosionsfähige Atmosphäre – Teil 29-1: Gasmessgeräte – Anforderungen an das Betriebsverhalten von Geräten für die Messung brennbarer Gase*

DIN EN 60079-29-2 (VDE 0400-2), *Explosionsfähige Atmosphäre – Teil 29-2: Gasmessgeräte – Auswahl, Installation, Einsatz und Wartung von Geräten für die Messung von brennbaren Gasen und Sauerstoff*

– Leerseite –

**Elektrische Geräte für die Detektion und Messung von brennbaren oder
toxischen Gasen und Dämpfen oder Sauerstoff –
Anforderungen an die funktionale Sicherheit von ortsfesten Gaswarnsystemen**

Electrical apparatus for the detection and
measurement of combustible or toxic gases or
vapours or of oxygen –
Requirements on the functional safety of fixed
gas detection systems

Matériel électrique pour la détection et la
mesure des gaz ou vapeurs combustibles ou
toxiques, ou de l'oxygène –
Exigences relatives à la fonction de sécurité des
systèmes fixes de détection de gaz

Diese Änderung A1 modifiziert die Europäische Norm EN 50402:2005; sie wurde von CENELEC am 2008-03-01 angenommen. Die CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Zentralsekretariat oder bei jedem CENELEC-Mitglied auf Anfrage erhältlich.

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

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

CENELEC

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

Zentralsekretariat: rue de Stassart 35, B-1050 Brüssel

© 2008 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 50402:2005 + A1:2008 D

Vorwort

Diese Europäische Norm wurde ausgearbeitet von SC 31-9 „Elektrische Geräte für das Aufspüren und die Messung brennbarer Gase zur Verwendung in industriellen und gewerblichen explosionsgefährdeten Bereichen“ des Technischen Komitees CENELEC/TC 31 „Elektrische Betriebsmittel für explosionsgefährdete Bereiche“ und vom Technischen Komitee CENELEC/TC 216 „Gaswarngeräte“.

Der Text des Entwurfs wurde der formellen Abstimmung unterworfen und von CENELEC am 2005-07-01 als EN 50402 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die EN auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2006-07-01
- spätestes Datum, zu dem nationale Normen, die der EN entgegenstehen, zurückgezogen werden müssen (dow): 2008-07-01

Vorwort zu A1

Diese Änderung wurde von SC 31-9 „Elektrische Geräte für das Aufspüren und die Messung brennbarer Gase zur Verwendung in industriellen und gewerblichen explosionsgefährdeten Bereichen“ des Technischen Komitees CENELEC/TC 31 „Elektrische Betriebsmittel für explosionsgefährdete Bereiche“ ausgearbeitet.

Der Text des Entwurfs wurde dem Einstufigen Annahmeverfahren unterworfen und von CENELEC am 2008-03-01 als Änderung A1 zu EN 50402:2005 angenommen.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem die Änderung auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2009-03-01
- spätestes Datum, zu dem nationale Normen, die der Änderung entgegenstehen, zurückgezogen werden müssen (dow): 2011-03-01

Inhalt

	Seite
Vorwort.....	2
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	8
3 Begriffe	9
4 Allgemeine Anforderungen	13
4.1 Einleitung	13
4.2 Merkmale der funktionalen Sicherheit von Modulen	14
5 Module und Elemente: Merkmale und Anforderungen.....	17
5.1 Allgemeine Anforderungen	21
5.2 Messgaszuführung	24
5.3 Sensor	27
5.4 Signalübertragung	27
5.5 Eingang der Auswerteeinheit.....	31
5.6 Signalverarbeitung in der Auswerteeinheit.....	33
5.7 Ausgang der Auswerteeinheit.....	37
6 Bestimmung der Sicherheitsanforderung	40
6.1 Allgemeines	40
6.2 Bestimmung der Sicherheitsfunktion.....	41
6.3 Bestimmung der Sicherheitsintegrität.....	42
6.4 Ermittlung der SIL-Fähigkeit für eine Sicherheitsfunktion	43
6.5 Bestimmung der Hardwareausfallraten für eine Sicherheitsfunktion	46
6.6 Anforderungen an das sichere Betriebsverhalten	47
7 Informationserfordernisse.....	47
7.1 Vom Hersteller des Gaswarnsystems beizustellende Informationen.....	47
7.2 Vom Anwender des Gaswarnsystems beizustellende Informationen	48
8 Validierung.....	48
Anhang A (informativ) Gaswarnsysteme als Teil eines sicherheitsbezogenen Systems.....	49
Anhang B (normativ) Umsetzung von SIL-Fähigkeiten des Gaswarnsystems.....	54
Anhang C (normativ) Umsetzung der Anforderungen der Grundnormen auf Module.....	55
Anhang D (normativ) Management für funktionale Sicherheit.....	58
Anhang E (informativ) Bestimmung der SIL-Fähigkeit für eine Sicherheitsfunktion des Gaswarnsystems	60
 Bilder	
Bild 1 – Begriffe Messstelle, Messplatz und Messort	11
Bild 2 – Überblick über ein sicherheitsbezogenes System.....	18
Bild 3a – Module eines Gaswarnsystems (Messgaszuführung, Sensoren)	19

	Seite
Bild 3b – Module eines Gaswarnsystems (Auswerteeinheit).....	20
Bild 4 – Einbindung eines Gaswarnsystems in den Gesamt-Sicherheitslebenszyklus	41
Bild 5 – Serielle und parallele Kette	43
Bild 6 – Behandlung komplexer Module in einer redundanten Anordnung	46
Bild A.1 – Funktionale Sicherheit von Modulen und Systemen (Intervalle von Wiederholungsprüfungen und mittlere Reparaturzeit (MTTR) sind in dem Bild nicht dargestellt, obwohl sie in die Überlegungen einbezogen werden müssen)	53
Bild E.1 – Schritt 1 – Verknüpfungen der Module	60
Bild E.2 – Schritt 2 – Ermittlung der für die Sicherheitsfunktion notwendigen Module	60
Bild E.3 – Schritt 3 – Eliminierung der für die Sicherheitsfunktion nicht benötigten Module und Verknüpfungen.....	61
Bild E.4 – Schritt 4 (1. Durchlauf) – Zusammenfassung serieller Ketten.....	61
Bild E.5 – Schritt 5 (1. Durchlauf) – Zusammenfassung paralleler Ketten	61
Bild E.6 – Schritt 6 (1. Durchlauf) – Anpassung der Struktur des Blockschaltbildes	62
Bild E.7 – Schritt 4 (2. Durchlauf) – Zusammenfassung serieller Ketten.....	63
Bild E.8 – Schritt 5 (2. Durchlauf) – Zusammenfassung paralleler Ketten	63
Bild E.9 – Schritt 6 (2. Durchlauf) – Anpassung der Struktur des Blockschaltbildes – <i>Keine Aktion erforderlich</i>	63
Bild E.10 – Schritt 4 (3. Durchlauf) – Zusammenfassung serieller Ketten.....	64
Bild E.11 – Schritt 5 (3. Durchlauf) – Zusammenfassung paralleler Ketten	64
Bild E.12 – Schritt 6 (3. Durchlauf) – Anpassung der Struktur des Blockschaltbildes – <i>Keine Aktion erforderlich</i>	64
Bild E.13 – Schritt 4 (4. Durchlauf) – Zusammenfassung serieller Ketten – <i>Ende des Verfahrens</i>	64
Bild E.14 – Schritt 1 – Verknüpfungen der Module im Beispiel	65
Bild E.15 – Schritt 2 – Ermittlung der Module mit Einfluss auf die Sicherheitsfunktion	65
Bild E.16 – Schritt 3 – Eliminierung der Module und Verknüpfungen ohne Einfluss auf die Sicherheitsfunktion.....	65
Bild E.17 – Schritt 4 – Zusammenfassung serieller Ketten.....	66
Bild E.18 – Schritt 5 – Zusammenfassung paralleler Ketten – <i>Ende des Verfahrens</i>	66
Bild E.19 – Schritt 2 – Ermittlung der Module mit Einfluss auf die Sicherheitsfunktion	66
Bild E.20 – Schritt 3 – Eliminierung der Module und Verknüpfungen ohne Einfluss auf die Sicherheitsfunktion.....	66
Bild E.21 – Schritt 4 (1. Durchlauf) – Zusammenfassung serieller Ketten.....	67
Bild E.22 – Schritt 5 (1. Durchlauf) – Zusammenfassung paralleler Ketten	67
Bild E.23 – Schritt 6 (1. Durchlauf) – Anpassung der Struktur des Blockschaltbildes – <i>Keine Aktion erforderlich</i>	67
Bild E.24 – Schritt 4 (2. Durchlauf) – Zusammenfassung serieller Ketten – <i>Ende des Verfahrens</i>	67
 Tabellen	
Tabelle 1 – Fehlertoleranz für komplexe Module nach EN 61511-1, Tabelle 5.....	15
Tabelle 2 – Fehlertoleranz für komplexe Module nach EN 61508-2, Tabelle 3.....	15
Tabelle 3 – Minimale Hardware-Fehlertoleranz für einfache Module gemäß EN 61511-1, Tabelle 6.....	16

	Seite
Tabelle 4 – Fehlertoleranz für einfache Module gemäß EN 61508-2, Tabelle 2.....	16
Tabelle 5 – Diagnoseverfahren für die Programmablauf-Überwachung aus EN 61508-2	22
Tabelle 6 – Diagnoseverfahren für Speicher aus EN 61508-2	23
Tabelle 7 – Ermittlung der SIL-Fähigkeit für ein paralleles Kettenglied.....	44
Tabelle B.1 – Umsetzung von SIL-Fähigkeit der EN 50402 in SIL der EN 61508	54
Tabelle B.2 – Umsetzung von SIL-Fähigkeit der EN 50402 in Kategorien der EN ISO 13849-1	54
Tabelle E.1 – Ermittlung der SIL-Fähigkeit für ein paralleles Kettenglied	62

Einleitung

Diese Europäische Norm stellt Anforderungen an die funktionale Sicherheit von Gaswarnsystemen auf und umfasst Kriterien für Zuverlässigkeit, Fehlervermeidung und Fehlertoleranz. Funktionale Sicherheit ist der Teil der Gesamtsicherheit, der mit den für das Gaswarnsystem getroffenen Maßnahmen zur Vermeidung und Beherrschung von Ausfällen verbunden ist, so dass die Sicherheitsfunktion sichergestellt wird. Dies schließt nicht nur Anforderungen an die Konstruktion des Gaswarnsystems, sondern auch Anforderungen an Informationen bezüglich Planung, Inbetriebnahme, Wartung und Reparatur ein.

Die Funktion eines Gaswarnsystems fällt aus, wenn Gefahr bringende Ausfälle in den verwendeten Geräten auftreten. Funktionsausfälle treten ebenfalls auf, wenn solche Systeme nicht in geeigneter Weise installiert oder gewartet werden. In einigen Anwendungen sind diese Ausfallarten bestimmend für die erreichbare funktionale Sicherheit. Diese Europäische Norm zielt ausschließlich darauf ab, Geräteausfälle auf ein für die Anwendung geeignetes Maß zu reduzieren. Deshalb ist es erforderlich, dass Anwender von Gaswarnsystemen sicherstellen, dass die Installation und Wartung solcher Systeme entsprechend den Erfordernissen ausgeführt werden. Diese Europäische Norm legt nicht die Platzierung von Sensoren fest.

Gaswarnsysteme können sich in ihrem Aufbau, ihrer Komplexität und ihrem Betriebsverhalten sehr stark voneinander unterscheiden. Sie können nicht wie Geräte von geringer Komplexität in einheitlicher Weise behandelt werden. Eine allgemein gültige Festlegung von Anforderungen ist auf dieser Grundlage nicht möglich.

Deshalb müssen Gaswarnsysteme für die Bewertung in funktionale Module aufgeteilt werden, um sicherzustellen, dass Systeme unterschiedlichen Aufbaus mittels geeigneter Verfahren behandelt werden können. Ein Gaswarnsystem muss nicht alle Module enthalten, die durch diese Europäische Norm abgedeckt werden. Es werden für jedes dieser Module in Form von hierarchischen Stufen Anforderungen festgelegt, die Bestandteil des Betriebsverhaltens bezüglich der funktionalen Sicherheit sind. Diese hierarchischen Stufen werden als SIL-Fähigkeit bezeichnet, wobei die SIL-Fähigkeit 1 die niedrigste und die SIL-Fähigkeit 4 die höchste Stufe für das Betriebsverhalten darstellt, um diese Norm zu erfüllen. Die SIL-Fähigkeit eines Moduls ist mit dem größten Sicherheits-Integritätslevel verbunden, der für eine Sicherheitsfunktion unter Verwendung von Modulen dieser festgelegten SIL-Fähigkeit beansprucht werden kann. Module werden hinsichtlich ihrer SIL-Fähigkeit eingestuft. Es werden ebenfalls die Informationen bezüglich der Ausfallraten der Module oder der mit ihnen verbundenen physikalischen Komponenten benötigt, um das Betriebsverhalten des Gaswarnsystems in seiner Gesamtheit bestimmen zu können. Dadurch werden sowohl zufällige Ausfälle der Hardware als auch systematische Ausfälle in Hard- und Software berücksichtigt. Die Norm legt ebenfalls die Anforderungen fest, die es ermöglichen zu bestimmen, ob das Gaswarnsystem in Verbindung mit anderen für die funktionale Sicherheit benötigten Geräten ausreichend niedrige Ausfallraten aufweist.

Diese Europäische Norm ermöglicht die Bestimmung der funktionalen Sicherheitsmerkmale eines Gaswarnsystems, ausgehend von Eigenschaften seiner Module und Komponenten (siehe [Anhang C](#)). Dies ermöglicht die Verwendung eines Gaswarnsystems als Teil eines Gesamtsicherheitssystems.

Die Einstufung einschließlich der Bestimmung von SIL-Fähigkeit und Ausfallraten ist für jede individuelle Ausführung nur ein einziges Mal erforderlich.

Nach der Einstufung jedes Moduls und jeder Komponente werden die Eigenschaften des gesamten Gaswarnsystems in Abhängigkeit von der ausgewählten Sicherheitsfunktion festgelegt. Das Verfahren zur Bestimmung der SIL-Fähigkeit für die Sicherheitsfunktion eines Gaswarnsystems muss nur für jede neue Kombination von Modulen und Komponenten wiederholt werden. Aus unterschiedlichen Kombinationen von Modulen können Gaswarnsysteme resultieren, die unterschiedliche SIL-Fähigkeiten erreichen.

Eine flexible Anpassung der Gaswarnsysteme an verschiedene Anwendungen wird möglich, ohne für jede neue Konfiguration alle Stufen des Validierungs-Verfahrens erneut zu durchlaufen.

Diese Europäische Norm enthält keine Anforderungen an die Verfügbarkeit. Diese sind getrennt zu betrachten.

1 Anwendungsbereich

Diese Europäische Norm gilt für ortsfeste Gaswarnsysteme zur Detektion und Messung von brennbaren oder toxischen¹⁾ Gasen oder Dämpfen oder Sauerstoff.

Diese Europäische Norm ergänzt die Anforderungen der Europäischen Normen an elektrische Geräte zur Detektion und Messung von brennbaren Gasen, Dämpfen (z. B. EN 61779 oder EN 50241), toxischen Gasen (z. B. EN 45544) oder Sauerstoff (z. B. [EN 50104](#)).

ANMERKUNG 1 Auf diese Europäischen Normen wird im Text als „messtechnische Normen“ Bezug genommen.

ANMERKUNG 2 Die oben genannten Beispiele stellen den Stand der Normung für industrielle Anwendungen zum Zeitpunkt der Veröffentlichung dieser Europäischen Norm dar. Es können weitere messtechnische Normen für andere Anwendungsfelder bestehen, auf die diese Norm ebenfalls anwendbar ist.

ANMERKUNG 3 Für ortsfeste Geräte zum Einsatz in sicherheitsgerichteten Anwendungen mit einer SIL-Anforderung bis Level 1 und für tragbare Geräte darf anstelle dieser Europäischen Norm die Europäische Norm [EN 50271](#) angewendet werden.

Die Anwendung der oben genannten messtechnischen Normen stellt ein angemessenes messtechnisches Betriebsverhalten im Normalbetrieb des Gaswarnsystems sicher. Die Anforderungen dieser Europäischen Norm richten sich ergänzend auf die funktionale Sicherheit von Gaswarnsystemen und umfassen Kriterien für Zuverlässigkeit, Fehlertoleranz und Vermeidung systematischer Fehler.

Diese Europäische Norm führt zu einer Einstufung des Gaswarnsystems in Form einer SIL-Fähigkeit und von damit verbundenen Hardwareausfallraten. Sie spiegelt eine hierarchische Anordnung von Sicherheitsstufen wider. Dadurch wird es dem Anwender ermöglicht, das Gaswarnsystem in ein Gesamtsicherheitssystem gemäß den Sicherheits-Integritätsleveln der EN 61508 oder den Kategorien der EN ISO 13849-1 einzubinden (siehe [Anhang B](#)).

Diese Europäische Norm stellt eine Produktnorm auf Grundlage der EN 61508 dar und schließt zusätzliche Anforderungen der EN ISO 13849-1 ein. Sie deckt Teile der Phase 9 „Realisierung“ des in [EN 61508-1](#) definierten Gesamt-Sicherheitslebenszyklus ab.

Diese Europäische Norm ist auf Gaswarnsysteme anwendbar, die aus folgenden funktionalen Einheiten bestehen können:

- Gasprobenentnahme;
- Sensor;
- Signal-Übertragung;
- Eingang der Auswerteeinheit;
- Signalverarbeitung in der Auswerteeinheit;
- Ausgang der Auswerteeinheit.

Diese Europäische Norm legt keine Anforderungen an die Installation und Wartung von Gaswarnsystemen fest. Sie legt auch nicht die Platzierung von Sensoren fest.

Diese Europäische Norm legt nicht fest, welche SIL-Fähigkeit für welche Anwendung ausreichend ist.

ANMERKUNG 4 Die für eine Anwendung erforderliche SIL-Fähigkeit wird vom Anwender festgelegt (siehe [Anhänge A und B](#)).

¹⁾ Für die Anwendung dieser Norm schließt der Begriff „toxisch“ folgende Eigenschaften ein: „sehr giftig“, „giftig“, „gesundheitsschädlich“, „ätzend“, „reizend“, „sensibilisierend“, „krebserzeugend“, „erbgutverändernd“ und „teratogen“.

2 Normative Verweisungen

Die folgenden zitierten Dokumente 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).

EN ISO 13849-1²⁾, *Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsgrundsätze (ISO 13849-1:1999)*

EN 45544-1:1999, *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 1: Allgemeine Anforderungen und Prüfverfahren*

EN 45544-2:1999, *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 2: Anforderungen an das Betriebsverhalten von Geräten für Konzentrationsmessungen im Bereich von Grenzwerten*

EN 45544-3:1999, *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 3: Anforderungen an das Betriebsverhalten von Geräten für Konzentrationsmessungen weit oberhalb von Grenzwerten*

EN 45544-4:1999, *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 4: Leitfaden für Auswahl, Installation, Einsatz und Instandhaltung*

EN 50073:1999, *Leitfaden für Auswahl, Installation, Einsatz und Wartung von Geräten für die Detektion und die Messung von brennbaren Gasen oder Sauerstoff*^{N1)}

EN 50104:2002, *Elektrische Geräte für die Detektion und Messung von Sauerstoff – Anforderungen an das Betriebsverhalten und Prüfmethoden*

EN 50241-1:1999, *Anforderungen an Geräte mit offener Messstrecke für die Detektion brennbarer oder toxischer Gase und Dämpfe – Teil 1: Allgemeine Anforderungen und Prüfverfahren*

EN 50241-2:1999, *Anforderungen an Geräte mit offener Messstrecke für die Detektion brennbarer oder toxischer Gase und Dämpfe – Teil 2: Anforderungen an das Betriebsverhalten von Geräten für die Detektion brennbarer Gase*

EN 61508-1:2001, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:1998)*

EN 61508-2:2001, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/ programmierbare elektronische Systeme (IEC 61508-2:2000)*

EN 61508-3:2001, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:1998)*

EN 61508-4:2001, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:1998)*

EN 61508-5:2001, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5:1998)*

EN 61508-6:2001, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 6: Anwendungsrichtlinie für IEC 61508-2 und IEC 61508-3 (IEC 61508-6:2000)*

²⁾ Im Entwurfsstadium.

^{N1)} Nationale Fußnote: Ersetzt durch EN 60079-29-2:2007.

EN 61508-7:2001, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (IEC 61508-7:2000)

EN 61511-1:2004, Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie – Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware (IEC 61511-1:2003)

EN 60079-29-1:2007, Explosionsfähige Atmosphäre – Teil 29-1: Gasmessgeräte – Anforderungen an das Betriebsverhalten von Geräten für die Messung brennbarer Gase

EN 60079-29-2:2007, Explosionsfähige Atmosphäre – Teil 29-2: Gasmessgeräte – Auswahl, Installation, Einsatz und Wartung von Geräten für die Messung von brennbaren Gasen und Sauerstoff

EN 61779-1:2000, Elektrische Geräte für die Detektion und Messung brennbarer Gase – Teil 1: Allgemeine Anforderungen und Prüfverfahren (IEC 61779-1:1998, mod.)^{N2)}

EN 61779-2:2000, Elektrische Geräte für die Detektion und Messung brennbarer Gase – Teil 2: Anforderungen an das Betriebsverhalten von Geräten der Gruppe I mit einem Messbereich bis zu 5 % Volumenanteil Methan in Luft (IEC 61779-2:1998, mod.)^{N2)}

EN 61779-4:2000, Elektrische Geräte für die Detektion und Messung brennbarer Gase – Teil 4: Anforderungen an das Betriebsverhalten von Geräten der Gruppe II mit einem Messbereich bis zu 100 % der unteren Explosionsgrenze (IEC 61779-4:1998, mod.)^{N2)}

EN 61779-5:2000, Elektrische Geräte für die Detektion und Messung brennbarer Gase – Teil 5: Anforderungen an das Betriebsverhalten von Geräten der Gruppe II mit einem Messbereich bis zu 100 % Volumenanteil Gas (IEC 61779-5:1998, mod.)^{N2)}

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 61779 und EN 61508-4. Einige Begriffe werden zweckmäßigerweise wiederholt. Einige Begriffe aus der EN 61508-4 sind für Gaswarnsysteme angepasst worden.

3.1

funktionale Sicherheit (EN 61508-4, 3.1.9)

Teil der Gesamtsicherheit, bezogen auf das sicherheitsbezogene System (en: equipment under control – EUC) und das EUC-Leit- und Steuerungssystem, der von der korrekten Funktion des elektrischen/elektronischen/programmierbaren elektronischen sicherheitsbezogenen Systems (E/E/PES), sicherheitsbezogenen Systemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt

ANMERKUNG 1 Das EUC (EN 61508-4, 3.2.3) ist die überwachte Einrichtung oder der überwachte Prozess, die bzw. der das Gaswarnsystem absichert.

ANMERKUNG 2 Das EUC-Leit- und Steuerungssystem reagiert auf Eingangssignale aus dem Prozess und erzeugt Ausgangssignale, die die EUC in der gewünschten Art arbeiten lassen (EN 61508-4, 3.3.4).

ANMERKUNG 3 Das Gaswarnsystem ist Teil des E/E/PES.

3.2

Sicherheitsfunktion eines Gaswarnsystems

von dem Gaswarnsystem ausgeführte Funktion (Messgaszuführung bis Ausgang des Gaswarnsystems einschließend), die es dem sicherheitsbezogenen System erlaubt, einen sicheren Zustand zu erreichen

3.3

sicherheitsbezogenes Teil

jedes Teil, z. B. Modul oder Element, das für die Ausführung der geforderten Sicherheitsfunktion eines Gaswarnsystems benötigt wird

^{N2)} Nationale Fußnote: Ersetzt durch EN 60079-29-1:2007.

3.4

Fehler (EN 61508-4, 3.6.1)

nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen

3.5

Fehlertoleranz (EN 61508-4, 3.6.3)

Fähigkeit einer Funktionseinheit, eine geforderte Funktion bei Bestehen von Fehlern oder Abweichungen weiter auszuführen

3.6

SIL-Fähigkeit

wird durch die Maßnahmen und Techniken zur Fehlervermeidung und -beherrschung sowohl in Hard- als auch in Software bestimmt. Die Nummer der SIL-Fähigkeit stellt eine Eigenschaft eines Elements, eines Moduls, einer Kombination von Modulen oder von einer oder mehreren Sicherheitsfunktion(en) eines Gaswarnsystems dar. Es gibt vier verschiedene SIL-Fähigkeiten, bezeichnet mit Nummern von 1 bis 4, wobei die SIL-Fähigkeit 4 für die höchste Stufe des sicheren Betriebsverhaltens steht.

3.7

Modul

Module bilden die Funktionseinheiten eines Gaswarnsystems. Ein Modul führt einen festgelegten Teil der Funktionalität innerhalb des Gaswarnsystems aus. Es besteht aus einem oder mehreren Elementen.

ANMERKUNG Module können einfach oder komplex sein (siehe 4.2).

3.8

Element

funktionale Untereinheit zu einem Modul

ANMERKUNG Die Software oder ein Teil von ihr können als ein Element behandelt werden.

3.9

Komponente

der Hardwareaufbau des Gaswarnsystems besteht aus Komponenten als physikalisch trennbare Baugruppen

ANMERKUNG Abhängig von der jeweiligen Realisierung kann ein Element eines funktionalen Moduls deshalb zu verschiedenen Hardwarekomponenten gehören.

3.10

Peripherie

Komponenten des Gesamtsystems, die nicht zum Gaswarnsystem gehören, aber mit ihm in Verbindung stehen

ANMERKUNG 1 Siehe Bild 2.

ANMERKUNG 2 Die Peripherie liegt außerhalb des Anwendungsbereiches dieser Norm.

3.11

Messstelle

Installationsort eines einzelnen Sensors im Diffusionsbetrieb oder einer Probenahmesonde

ANMERKUNG Siehe Bild 1.

3.12

Messplatz

redundante Kombination zweier Messstellen eines Messortes

ANMERKUNG Siehe Bild 1.

3.13

Messort

Bereich, der mehrere Messstellen umfasst, in dem annähernd gleiche Gaskonzentrationen zu erwarten sind

ANMERKUNG 1 Siehe Bild 1.

ANMERKUNG 2 Bei Übereinstimmung mit den Begriffen 3.11 bis 3.13 ist es möglich, dass ein einzelner Sensor als redundanter Kombinationspartner für verschiedene andere Sensoren dient.

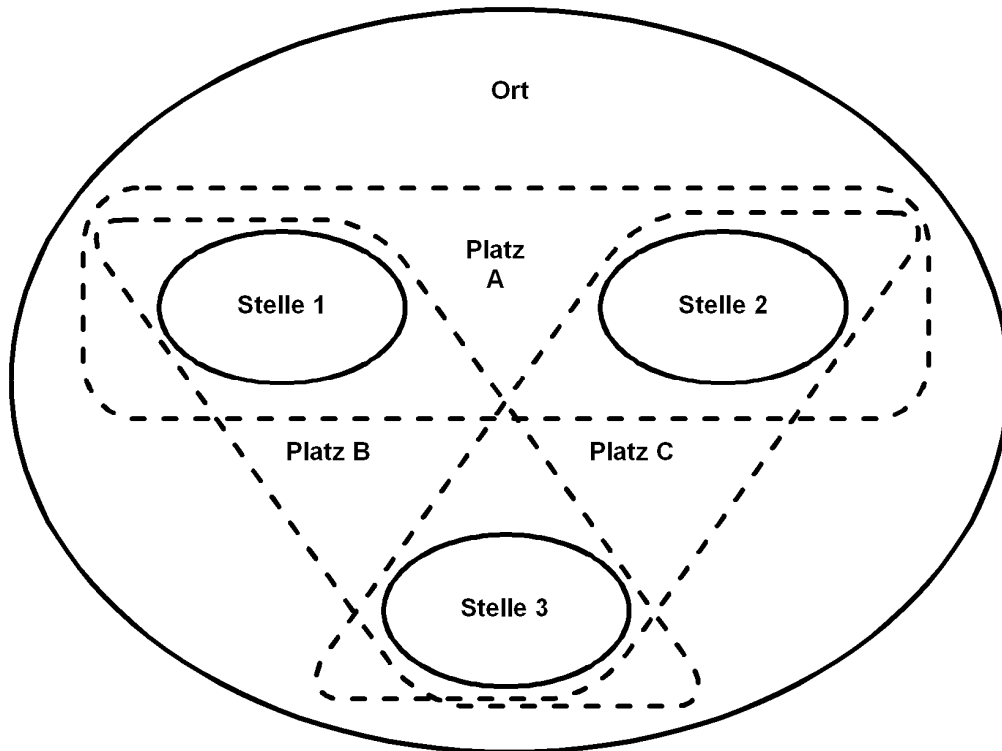


Bild 1 – Begriffe Messstelle, Messplatz und Messort

3.14

Messsignal

gegebenenfalls vorverstärktes Sensorsignal in analoger oder digitaler Form

3.15

Messwert

verarbeitetes Messsignal einschließlich physikalischer Einheit (z. B. % der UEG). Ein Messwert kann aus einem einzelnen Signal oder einer Kombination mehrerer Messsignale gebildet werden. Die kombinierten Messsignale können unterschiedliche physikalische Größen, z. B. Gaskonzentration und Temperatur, darstellen.

3.16

Statussignal

elektrisches Signal, mit dem Betriebszustände, Schaltzustände von Geräten, Einhaltung von Rahmenbedingungen (z. B. zulässiger Temperaturbereich oder Durchfluss) innerhalb eines Moduls oder an ein anderes Modul des Gaswarnsystems gemeldet werden

3.17

Alarmsignal

elektrisches Signal, das einen Alarmzustand von einer oder mehreren Messstellen meldet. Das Alarmsignal wird entweder im Gaswarnsystem verarbeitet (z. B. zur Auslösung von Schaltvorgängen) oder an die Peripherie weitergeleitet.

ANMERKUNG Alarmsignale werden von anderen Signalen getrennt behandelt, da sie allgemein mit höherer Priorität behandelt werden.

3.18

Sonderzustand

jeder Zustand einer Messstelle, eines Moduls, einer Auswerteeinheit oder des gesamten Gaswarnsystems, in dem die Überwachung der Gaskonzentration nicht erfolgt, z. B. Inbetriebnahme, Kalibrierung oder Störung

3.19

Parameter

Einstellung durch den Hersteller oder Anwender, der das Betriebsverhalten der Software beeinflusst, z. B. Änderung der Alarmschwellen oder der Messbereiche. Parametriermöglichkeiten werden während der Konstruktion des Gaswarnsystems in die Software eingebunden. Veränderungen von Parametereinstellungen sind keine Änderungen der Software. Die Software kann verschiedene Stufen der Zugangsberechtigung für das Lesen und Ändern von Parametern beinhalten.

3.20

kleinste Einstellzeit

Wert, der durch die anwendbaren messtechnischen Normen bestimmt wird. In den messtechnischen Normen werden zulässige Einstellzeiten für die Baumusterprüfung angegeben. Enthalten verschiedene anwendbare messtechnische Normen unterschiedliche Anforderungen an die Einstellzeit, dann stellt der kleinste Wert die „kleinste Einstellzeit“ dar.

3.21

kleinste Anzeigeabweichung

Wert, der durch die anwendbaren messtechnischen Normen bestimmt wird. In den messtechnischen Normen werden Toleranzspannen als zulässige Anzeigeabweichungen für die Baumusterprüfung angegeben. Enthalten verschiedene anwendbare messtechnische Normen unterschiedlich große Toleranzspannen, dann stellt die kleinste Toleranzspanne die „kleinste Anzeigeabweichung“ dar.

Die kleinste Anzeigeabweichung wird als Grundlage für die notwendige Auflösung von Messsignalen bei digitaler Datenübertragung und Datenverarbeitung benutzt, damit bei Einsatz digitaler Technik die Anforderungen der messtechnischen Normen erfüllt werden.

3.22

Selbsttestfunktionen

Testroutinen, z. B. Speichertests, die innerhalb des Gaswarnsystems automatisch und zyklisch wiederholt ablaufen. Diese Funktionen können innerhalb eines einzelnen Moduls ablaufen oder können die Verbindung oder das Zusammenwirken von Modulen überprüfen.

Zu Selbsttestfunktionen zählen sowohl zyklisch wiederholte Testroutinen, die den Messbetrieb nicht unterbrechen, als auch Testroutinen, die bei der Inbetriebnahme oder während der Einschaltverzögerung eines Gaswarnsystems ablaufen, bevor es den Messbetrieb aufnimmt. Ebenso zählen dazu Testroutinen, die auf Benutzeranforderung ablaufen oder die im Kalibriermodus für einzelne Messstellen oder Teile des Gaswarnsystems ausgelöst werden.

3.23

Kontrolle

die Kontrolle beinhaltet zusätzlich zu Selbsttestfunktionen, die auf Benutzeranforderung ablaufen, organisatorische Maßnahmen, z. B. manuelle Kalibrierung

3.24

Verifikation (EN 61508-4, 3.8.1)

Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die Anforderungen erfüllt worden sind

3.25

Redundanz

Vorhandensein von Einrichtungen zusätzlich zu den Einrichtungen, die für die Ausführung einer geforderten Funktion ausreichen

ANMERKUNG Redundanz dient der Verbesserung von Zuverlässigkeit und Fehlertoleranz, kann aber auch zur Verbesserung der Verfügbarkeit genutzt werden.

3.26

Verfügbarkeit

der Zeitanteil des Messbetriebes an der Gesamtzeit, während der sich das Gaswarnsystem im Messbetrieb oder in einem Sonderzustand einschließlich Reparatur befindet. Sie wird in Prozent angegeben.

3.27

Diffusionsbetrieb

Betrieb, bei dem der Transport des Gases aus der Atmosphäre in den Sensor durch Diffusion erfolgt, d. h., es ist keine Messgasförderung vorhanden

3.28

Messgasförderung

Betrieb, bei dem der Transport des Gases aus der Atmosphäre in den Sensor durch Ansaugung, z. B. eine Pumpe, erfolgt

4 Allgemeine Anforderungen

4.1 Einleitung

Das gesamte Gaswarnsystem kann sowohl Sicherheitsfunktionen als auch nicht sicherheitsgerichtete Funktionen wahrnehmen. Die SIL-Fähigkeit kann für eine oder mehrere Sicherheitsfunktionen ermittelt werden.

Die Spezifikation der Sicherheitsanforderungen eines Moduls oder eines Gaswarnsystems besteht aus drei Teilen: Sicherheitsfunktion, SIL-Fähigkeit und Hardwareausfallrate. Dies wird in den Abschnitten 4 bis 6 behandelt.

[Anhang A](#) enthält eine Anleitung, wie aus der Gesamtspezifikation der Sicherheitsanforderungen die Spezifikation der Sicherheitsanforderungen an das Gaswarnsystem abgeleitet wird.

In [Abschnitt 5](#) werden Module des Gaswarnsystems ausgehend von ihrer Funktion definiert und die Anforderungen für jede SIL-Fähigkeit festgelegt.

Die in [Abschnitt 5](#) beschriebenen Module geben die üblicherweise anzutreffende Bandbreite wieder, können aber eventuell nicht alle technischen Lösungen abdecken. Anforderungen an neue, von dieser Europäischen Norm nicht abgedeckte Module müssen gemäß [Anhang D](#) dieser Europäischen Norm aufgestellt werden.

Die SIL-Fähigkeit eines Moduls wird durch die Maßnahmen und Technologien zur Fehlervermeidung und -beherrschung sowohl in Hard- als auch Software bestimmt. Die Stufe der SIL-Fähigkeit stellt eine Eigenschaft eines Elements, eines Moduls, einer Kombination von Modulen oder von einer oder mehreren Sicherheitsfunktion(en) eines Gaswarnsystems dar. Es gibt vier verschiedene SIL-Fähigkeiten, bezeichnet mit Nummern von 1 bis 4, wobei die SIL-Fähigkeit 4 für die höchste Stufe des sicheren Betriebsverhaltens steht.

Die Ermittlung der Hardwareausfallraten nach Aufteilung eines Gaswarnsystems in physikalische Komponenten wird ebenfalls von dieser Europäischen Norm gefordert.

Anwenden sollte es möglich sein, das Betriebsverhalten einer Sicherheitsfunktion eines übergeordneten sicherheitsbezogenen Systems, das ein Gaswarnsystem enthält, in Begriffen von Sicherheits-Integritätsleveln (SIL) gemäß EN 61508 zu ermitteln. Dies ist möglich, wenn die SIL-Fähigkeit und zugehörigen Hardwareausfallraten für die Sicherheitsfunktion des Gaswarnsystems sowie die entsprechenden Angaben für die weiteren für die funktionale Sicherheit erforderlichen Einrichtungen (Peripherie) bekannt sind (siehe auch [A.3.2](#)).

Die SIL-Fähigkeit eines Moduls bestimmt weiterhin die Übereinstimmung eines Moduls mit den Kategoriebegriffen gemäß EN ISO 13849-1.

Es besteht im Allgemeinen keine Beziehung zwischen den Sicherheits-Integritätsleveln in EN 61508 und den Kategorien in EN ISO 13849-1. Die Anforderungen an Module in dieser Europäischen Norm wurden unter Berücksichtigung der Anforderungen beider oben genannten Europäischen Normen ermittelt. Hinweise zur Beziehung zwischen der in dieser Europäischen Norm verwendeten SIL-Fähigkeit und den Sicherheits-Integritätsleveln der EN 61508 und den Kategorien der EN ISO 13849-1 werden in [Anhang B](#) gegeben.

Die SIL-Fähigkeit und Hardwareausfallraten einer Sicherheitsfunktion eines Gaswarnsystems können aus der SIL-Fähigkeit der Module und Hardwareausfallraten der Komponenten ermittelt werden (siehe [Abschnitt 6](#) und [Anhang E](#)).

ANMERKUNG 1 Die Zuweisung einer SIL-Fähigkeit zu einem einzelnen Modul beinhaltet nicht automatisch, dass die gleiche SIL-Fähigkeit für das gesamte Gaswarnsystem gilt.

ANMERKUNG 2 Unterschiedliche Kombinationen von Modulen können zu unterschiedlichen SIL-Fähigkeiten für die ausgewählte Sicherheitsfunktion des gesamten Gaswarnsystems führen.

ANMERKUNG 3 Ein und dasselbe Gaswarnsystem kann abhängig von der für die Anwendung ausgewählten Sicherheitsfunktion den Anforderungen unterschiedlicher SIL-Fähigkeiten entsprechen.

ANMERKUNG 4 Alternativ kann die für jedes Modul erforderliche SIL-Fähigkeit aus der SIL-Fähigkeit für die ausgewählte Sicherheitsfunktion des Gaswarnsystems ermittelt werden, abhängig davon, auf welche Weise die Module kombiniert werden (siehe [Anhang A](#)).

Die Feststellung, ob eine bestimmte Sicherheitsfunktion eines Gaswarnsystems in Verbindung mit anderen Einrichtungen eine festgelegte Sicherheitsintegrität erfüllt, erfordert auch die Einbeziehung der funktionalen Sicherheits-Eigenschaften der anderen Einrichtungen (Peripherie), die für die funktionale Sicherheit benötigt werden. Geeignete Verfahren werden in [Abschnitt 6](#) beschrieben.

Die Bestimmung der SIL-Fähigkeit für ein Modul und der Hardwareausfallrate einer Komponente sind nur ein einziges Mal erforderlich.

Die Bestimmung der SIL-Fähigkeit und der Hardwareausfallrate für die Sicherheitsfunktion eines Gaswarnsystems muss für jede neue Kombination von Modulen und mit diesen verbundenen Komponenten wiederholt werden. Der Einfluss aller zum Gaswarnsystem gehörenden Module und Komponenten muss berücksichtigt werden.

Ergänzend zur funktionalen Sicherheit des Gaswarnsystems sind die Verfügbarkeit und die Vermeidung von Fehlalarmen die wichtigsten Auswahlkriterien für den Anwender, um ein geeignetes System für eine bestimmte Anwendung auszuwählen.

Diese Europäische Norm stellt Anforderungen an Maßnahmen, die ausgeführt werden, wenn Ausfälle in den Modulen erkannt werden. Das Gaswarnsystem muss einen vorbestimmten Zustand einnehmen, nachdem Ausfälle erkannt wurden.

BEISPIEL 1 Zur Erfüllung dieser Forderung kann eine Abschaltung der von den Fehlern betroffenen Teile des Gaswarnsystems vorgenommen werden. Dies kann die Verfügbarkeit mindern oder zu fälschlichen Auslösungen führen.

BEISPIEL 2 Bei Funktionsstörung oder Ausfall in einem redundanten Element kann es zulässig sein, für einen begrenzten Zeitraum in einen Notbetrieb ohne Redundanz umzuschalten, wenn das betroffene Teil ermittelt und der Redundanzverlust innerhalb des Gaswarnsystems gemeldet wird.

Sind Mittel zur Steigerung der Verfügbarkeit vorhanden (z. B. zusätzliche Hard- oder Software), müssen diese im Gaswarnsystem enthaltenen Funktionen entsprechend ihrer Bedeutung für die Sicherheit in die Prüfungen einbezogen werden.

4.2 Merkmale der funktionalen Sicherheit von Modulen

Diese Europäische Norm legt für eine Reihe von Modulen die Eigenschaften der sicherheitsbezogenen Teile eines Gaswarnsystems bezüglich deren Widerstandsfähigkeit gegen Fehler und ihr Verhalten im Fehlerfall fest. Dies geschieht in Abhängigkeit von der beanspruchten SIL-Fähigkeit. Es gibt vier Stufen von SIL-Fähig-

keiten (mit den Nummern 1, 2, 3 und 4). SIL-Fähigkeiten höher als 1 schließen die Anforderungen für die niedrigeren SIL-Fähigkeiten mit ein, sofern nichts anderes festgelegt wird.

In [Abschnitt 5](#) werden die Module des Gaswarnsystems als einfach oder komplex eingestuft und es werden die Anforderungen den SIL-Fähigkeiten entsprechend festgelegt.

Die meisten Module sind entweder als einfach oder komplex eingestuft. Ist dies nicht der Fall oder weicht die technische Lösung von der Einstufung in [Abschnitt 5](#) ab, muss die Einstufung nach folgenden Kriterien vorgenommen werden:

Module mit analoger Datenverarbeitung werden als einfach angenommen. Dies gilt auch für Module mit digitaler Signalverarbeitung, wenn der Anwender die Softwarefunktion nicht ändern kann oder nur einige wenige Parameter (bis zu 10) einstellen kann. Alle anderen Module werden als komplex behandelt, z. B. Module, die programmierbare Systeme mit beschränkt oder unbeschränkt änderbarer Software enthalten. Die Fehlertoleranz muss für alle komplexen Module mit den Anforderungen in Tabelle 1 oder Tabelle 2 übereinstimmen.

Tabelle 1 – Fehlertoleranz für komplexe Module nach EN 61511-1, Tabelle 5

SIL-Fähigkeit	Minimale Hardware-Fehlertoleranz (siehe EN 61511-1, 11.4.2)		
	Anteil ungefährlicher Ausfälle < 60 %	Anteil ungefährlicher Ausfälle 60 % bis 90 %	Anteil ungefährlicher Ausfälle > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Es gelten besondere Anforderungen – siehe EN 61508		

Sehr ähnlich ist der in Tabelle 2 wiedergegebene Ansatz der EN 61508-2.

Tabelle 2 – Fehlertoleranz für komplexe Module nach EN 61508-2, Tabelle 3

SIL-Fähigkeit	Minimale Hardware-Fehlertoleranz (siehe EN 61508-2, 7.4.3.1)			
	Anteil ungefährlicher Ausfälle < 60 %	Anteil ungefährlicher Ausfälle 60 % bis < 90 %	Anteil ungefährlicher Ausfälle 90 % bis < 99 %	Anteil ungefährlicher Ausfälle ≥ 99 %
1	1	0	0	0
2	2	1	0	0
3	Nicht behandelt in EN 61508-2	2	1	0
4	Nicht anwendbar	Es gelten besondere Anforderungen – siehe EN 61508	2	1

Die minimale Hardware-Fehlertoleranz nach EN 61511-1 von einfachen Modulen muss den Angaben in [Tabelle 3](#) entsprechen, vorausgesetzt, der überwiegende Ausfallmodus führt in den sicheren Zustand oder Gefahr bringende Ausfälle werden erkannt. Anderenfalls muss die Fehlertoleranz um eins erhöht werden.

ANMERKUNG Um festlegen zu können, ob die überwiegende Art der Ausfälle in den sicheren Zustand führt, ist es erforderlich, Folgendes in die Überlegungen einzubeziehen:

- die Prozessanbindung des Gerätes;
- Nutzung von Diagnoseinformation des Gerätes, um die Prozesssignale zu bewerten;

- Nutzung von eigenem fehlersicherem Verhalten des Gerätes (z. B. Signal mit lebendem Nullpunkt, Übergang in sicheren Zustand bei Ausfall der Spannungsversorgung).

Für alle einfachen Module darf die minimale Hardware-Fehlertoleranz (wie in der rechten Spalte von Tabelle 3 gezeigt) um eins gemindert werden, wenn die verwendeten Module allen nachfolgenden Punkten entsprechen:

- Die Hardware der Module wird auf Grundlage der Betriebsbewährung ausgewählt (siehe [EN 61511-1, 11.5.3](#));
- die Module erlauben lediglich die Einstellung prozessbezogener Parameter, z. B. Messbereich, Ausfallrichtung aufwärts oder abwärts usw.;
- die Einstellung prozessbezogener Parameter des Moduls ist geschützt, z. B. Jumper, Passwort;
- die Funktion besitzt eine SIL-Anforderung kleiner als 4.

Tabelle 3 – Minimale Hardware-Fehlertoleranz für einfache Module gemäß [EN 61511-1, Tabelle 6](#)

SIL-Fähigkeit	Minimale Hardware-Fehlertoleranz (siehe EN 61511-1, 11.4.3 und 11.4.4)	Minimale Hardware-Fehlertoleranz um eins gemindert (siehe Text oben)
1	0	0
2	1	0
3	2	1
4	Es gelten besondere Anforderungen – siehe EN 61508	Nicht anwendbar

Den Ansatz der [EN 61508-2](#) gibt Tabelle 4 unter Berücksichtigung der verschiedenen Anteile ungefährlicher Fehler wieder.

Tabelle 4 – Fehlertoleranz für einfache Module gemäß [EN 61508-2, Tabelle 2](#)

SIL-Fähigkeit	Minimale Hardware-Fehlertoleranz (siehe EN 61508-2, 7.4.3.1)			
	Anteil ungefährlicher Ausfälle < 60 %	Anteil ungefährlicher Ausfälle 60 % bis < 90 %	Anteil ungefährlicher Ausfälle 90 % bis < 99 %	Anteil ungefährlicher Ausfälle ≥ 99 %
1	0	0	0	0
2	1	0	0	0
3	2	1	0	0
4	Nicht behandelt in EN 61508-2	2	1	1

Es wird vorausgesetzt, dass durch die Erfüllung der Anforderungen an einfache und komplexe Module, die in [Abschnitt 5](#) beschrieben sind, ein Anteil ungefährlicher Ausfälle von 60 % bis 90 % erreicht wird. Für bestimmte in [Abschnitt 5](#) beschriebene Module wird vorausgesetzt, dass ein Anteil ungefährlicher Ausfälle von 90 % bis 99 % oder ≥ 99 % erreicht wird. Andere Zusammenstellungen sind zulässig, vorausgesetzt, die Anforderungen der EN 61508 werden eingehalten.

Die Anforderungen für eine bestimmte SIL-Fähigkeit wurden mit Bezug auf die systematischen Anforderungen des zugehörigen SIL aus den Anforderungen in EN 61508 abgeleitet. Die Anforderungen an die Fehlertoleranz wurden aus [EN 61511-1](#) für den zugehörigen Sicherheits-Integritätslevel abgeleitet. Die Anforderungen der EN ISO 13849-1 wurden ebenfalls berücksichtigt und an geeigneten Stellen in [Abschnitt 5](#) eingebunden.