

	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):2009-01 Siehe Anwendungsbeginn Elektrische Geräte für die Detektion und Messung von brennbaren oder toxischen Gasen und Dämpfen oder Sauerstoff – Anforderungen an die funktionale Sicherheit von Gaswarnsystemen; Deutsche Fassung EN 50402:2017 Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen – Requirements on the functional safety of gas detection systems; German version EN 50402:2017 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 de détection de gaz; Version allemande EN 50402:2017 Gesamtumfang 103 Seiten DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2017-02-04 angenommene Europäische Norm als DIN-Norm ist 2018-01-01.

Für **DIN EN 50402 (VDE 0400-70):2009-01** besteht eine Übergangsfrist bis 2020-02-04.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 50402 (VDE 0400-70):2015-12.

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

Änderungen

Gegenüber **DIN EN 50402 (VDE 0400-70):2009-01** wurden folgende Änderungen vorgenommen:

- a) Die Norm wurde allgemein aktualisiert, um die Änderungen in der zweiten Ausgabe der DIN EN 61508 (VDE 0803) bezüglich Hardware und Software zu berücksichtigen.
- b) Die Norm wurde aktualisiert zur Übereinstimmung der Anforderungen für SIL 1 mit der zweiten Ausgabe der **DIN EN 50271 (VDE 0400-21)**, die die Mindestanforderungen an die funktionale Sicherheit im Rahmen der messtechnischen Prüfung von Gasdetektoren, Gaswarngeräten und vollständigen Gaswarnsystemen festlegt.
- c) Die jüngsten Überarbeitungen der messtechnischen Normen wurden berücksichtigt.
- d) SIL 4 wurde gestrichen, weil es für die Gasdetektion unangemessen ist.
- e) Die **Abschnitte 4 und 5** wurden zwecks einer detaillierteren Spezifikation aktualisiert.
- f) Der **Abschnitt 6** für Software ist neu.
- g) Die **Abschnitte 7 bis 11** wurden umstrukturiert, um die Anforderungen und den Bezug zu DIN EN 61508 (VDE 0803) klarer zu fassen.
- h) **Abschnitt 10** beschreibt detaillierter die Informationen für den Anwender.
- i) Der vorherige normative **Anhang D** ist nun **Abschnitt 12**.
- j) Der vorherige informative **Anhang A** wurde gestrichen. Wichtige Textpassagen wurden in die **Abschnitte 7 bis 9** verschoben.
- k) Der neue informative **Anhang D** liefert Informationen über Ausfall-/Fehlermodi von Sensorelementen.

Frühere Ausgaben

DIN EN 50402 (VDE 0400-70): 2006-03, 2009-01

Nationaler Anhang NA (informativ)

Zusammenhang mit europäischen und internationalen Dokumenten

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

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

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

Tabelle NA.1 (1 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 45544 (alle Teile)	–	DIN EN 45544 (VDE 0400-22) (alle Teile)	VDE 0400-22
EN 45544-1	–	DIN EN 45544-1 (VDE 0400-22-1)	VDE 0400-22-1
EN 45544-2	–	DIN EN 45544-2 (VDE 0400-22-2)	VDE 0400-22-2
EN 45544-3	–	DIN EN 45544-3 (VDE 0400-22-3)	VDE 0400-22-3
EN 45544-4	–	DIN EN 45544-4 (VDE 0400-22-4)	VDE 0400-22-4
EN 50104	–	DIN EN 50104 (VDE 0400-20)	VDE 0400-20
EN 50159	–	DIN EN 50159 (VDE 0831-159)	VDE 0831-159
EN 50270	–	DIN EN 50270 (VDE 0843-30)	VDE 0843-30
EN 50271:2010	–	DIN EN 50271 (VDE 0400-21):2011-04	VDE 0400-21
EN 60079-29-1:2016	IEC 60079-29-1:2016, mod.	DIN EN 60079-29-1 (VDE 0400-1):2017-09	VDE 0400-1
EN 60079-29-2	IEC 60079-29-2	DIN EN 60079-29-2 (VDE 0400-2)	VDE 0400-2
EN 60079-29-3	IEC 60079-29-3	DIN EN 60079-29-3 (VDE 0400-3)	VDE 0400-3
EN 60079-29-4	IEC 60079-29-4, mod.	DIN EN 60079-29-4 (VDE 0400-40)	VDE 0400-40
EN 61326-3-1	IEC 61326-3-1	DIN EN 61326-3-1 (VDE 0843-20-3-1)	VDE 0843-20-3-1
EN 61326-3-2	IEC 61326-3-2	DIN EN 61326-3-2 (VDE 0843-20-3-2)	VDE 0843-20-3-2
EN 61508 (alle Teile)	IEC 61508 (alle Teile)	DIN EN 61508 (VDE 0803) (alle Teile)	VDE 0803
EN 61508-1:2010	IEC 61508-1:2010	DIN EN 61508-1 (VDE 0803-1):2011-02	VDE 0803-1
EN 61508-2:2010	IEC 61508-2:2010	DIN EN 61508-2 (VDE 0803-2):2011-02	VDE 0803-2

Tabelle NA.1 (2 von 2)

Europäisches Dokument	Internationales Dokument	Deutsches Dokument	Klassifikation im VDE-Vorschriftenwerk
EN 61508-3:2010	IEC 61508-3:2010	DIN EN 61508-3 (VDE 0803-3):2011-02	VDE 0803-3
EN 61508-4:2010	IEC 61508-4:2010	DIN EN 61508-4 (VDE 0803-4):2011-02	VDE 0803-4
EN 61508-5:2010	IEC 61508-5:2010	DIN EN 61508-5 (VDE 0803-5):2011-02	VDE 0803-5
EN 61508-6	IEC 61508-6	DIN EN 61508-6 (VDE 0803-6)	VDE 0803-6
EN 61508-7:2010	IEC 61508-7:2010	DIN EN 61508-7 (VDE 0803-7):2011-02	VDE 0803-7
EN 61784-3:2016	IEC 61784-3:2016	DIN EN 61784-3 (VDE 0803-500):2017-09	VDE 0803-500

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN 45544 (VDE 0400-22) (alle Teile), *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe*

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 direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 2: Anforderungen an das Betriebsverhalten von Geräten, die für Expositionsmessungen eingesetzt werden*

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, die für allgemeine Gaswarnanwendungen eingesetzt werden*

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 Wartung*

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

DIN EN 50159 (VDE 0831-159), *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in Übertragungssystemen*

DIN EN 50270 (VDE 0843-30), *Elektromagnetische Verträglichkeit – Elektrische Geräte für die Detektion und Messung von brennbaren Gasen, toxischen Gasen oder Sauerstoff*

DIN EN 50271 (VDE 0400-21):2011-04, *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; Deutsche Fassung EN 50271:2010*

DIN EN 60079-29-1 (VDE 0400-1):2017-09, Explosionsfähige Atmosphäre – Teil 29-1: Gasmessgeräte – Anforderungen an das Betriebsverhalten von Geräten für die Messung brennbarer Gase (IEC 60079-29-1:2016, modifiziert); Deutsche Fassung EN 60079-29-1:2016

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

DIN EN 60079-29-3 (VDE 0400-3), Explosionsfähige Atmosphäre – Teil 29-3: Gasmessgeräte – Leitfaden zur funktionalen Sicherheit von ortsfesten Gaswarnsystemen

DIN EN 60079-29-4 (VDE 0400-40), Explosionsfähige Atmosphäre – Teil 29-4: Gasmessgeräte – Anforderungen an das Betriebsverhalten von Geräten mit offener Messstrecke für die Messung brennbarer Gase

DIN EN 61326-3-1 (VDE 0843-20-3-1), Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Allgemeine industrielle Anwendungen

DIN EN 61326-3-2 (VDE 0843-20-3-2), Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-2: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Industrielle Anwendungen in spezifizierter elektromagnetischer Umgebung

DIN EN 61508 (VDE 0803) (alle Teile), Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

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 (safety integrity level) (IEC 61508-5:2010); Deutsche Fassung EN 61508-5:2010

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):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 61784-3 (VDE 0803-500):2017-09, Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile (IEC 61784-3:2016); Deutsche Fassung EN 61784-3:2016

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

Electrical apparatus for the detection and measurement of combustible or toxic gases or vapours or of oxygen –
Requirements on the functional safety of 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 de détection de gaz

Diese Europäische Norm wurde von CENELEC am 2017-02-04 angenommen. CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

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

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

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



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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brüssel

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

Ref. Nr. EN 50402:2017 D

Inhalt

Seite

Europäisches Vorwort.....	7
Einleitung	8
1 Anwendungsbereich	10
2 Normative Verweisungen	11
3 Begriffe	12
4 Allgemeine Anforderungen	17
4.1 Spezifikation der Sicherheitsfunktionen	17
4.2 Bestimmung der Sicherheitsfunktion	24
4.3 Merkmale der funktionalen Sicherheit von Modulen	26
5 Funktionale Module und Elemente – Merkmale und Anforderungen	27
5.1 Allgemeines	27
5.1.1 Aufbau funktionaler Module	27
5.1.2 Allgemeine Anforderungen	30
5.2 Messgaszuführung	31
5.2.1 Messgasförderung	31
5.2.2 Messgasaufbereitung	32
5.2.3 Probenahmeumschaltung	33
5.2.4 Messgaszuführung im Diffusionsbetrieb	33
5.2.5 Automatische Kalibrierung und Justierung	34
5.3 Sensor	34
5.4 Signalübertragung	36
5.4.1 Allgemeine Anforderungen	36
5.4.2 Signalübertragung zwischen räumlich voneinander getrennten Modulen	36
5.4.3 Signalübertragung zwischen nicht räumlich voneinander getrennten Modulen	38
5.5 Eingang der Steuereinheit	39
5.5.1 Allgemeines	39
5.5.2 Schnittstelle für Messsignal	39
5.5.3 Eingang Systemkommunikation	39
5.5.4 Benutzerschnittstelle	39
5.5.5 Eingang von Peripherie	40
5.5.6 Energieversorgung	40
5.6 Signalverarbeitung	41
5.6.1 Allgemeines	41
5.6.2 Messwertbildung	42
5.6.3 Sonderzustand	43
5.6.4 Signalbewertung	44
5.6.5 Diagnosemaßnahmen innerhalb der Steuereinheit	44
5.6.6 Eingeschränkter Messbetrieb	46

5.6.7	Steuerung der Messgasförderung	47
5.6.8	Steuerung Probenahmeumschaltung	47
5.6.9	Steuerung Automatische Kalibrierung	48
5.6.10	Steuerung Automatische Justierung	48
5.7	Ausgang der Steuereinheit.....	49
5.7.1	Optische Anzeige	49
5.7.2	Schaltausgang	50
5.7.3	Ausgang Systemkommunikation.....	51
5.7.4	Ausgang zur Peripherie.....	52
5.7.5	Datenarchivierung	52
6	Software	53
6.1	Allgemeine Anforderungen.....	53
6.2	Zusammenhang zwischen den Softwarenormen.....	53
6.3	Anforderungen aus EN 61508-3	54
6.4	Liste der ersetzten oder nicht zutreffenden Abschnitte der EN 61508-3:2010	54
6.5	Liste der Änderungen gegenüber Abschnitten der EN 61508-3:2010	55
6.6	EN 50402 Grade der Strenge	57
6.7	Tabellen der Verfahren und Maßnahmen aus EN 61508-3:2010, Anhang A.....	58
6.7.1	Erklärung der Begriffe	58
6.7.2	Schreibweise in den Tabellen der Verfahren und Maßnahmen.....	58
6.7.3	Spezifikation der Softwareanforderungen.....	58
6.7.4	Entwurf der Softwarearchitektur.....	61
6.7.5	Softwareentwurf und Softwareentwicklung – Werkzeuge und Programmiersprachen.....	64
6.7.6	Softwareentwurf	64
6.7.6.1	EN 50402 Softwareentwurf	64
6.7.7	Softwaremodultests und Softwareintegration	66
6.7.8	PE-Integration (Hardware + Software).....	68
6.7.9	Softwarevalidierung.....	69
6.7.10	Modifikation	69
6.7.11	Softwareverifikation.....	70
7	Kombination funktionaler Module zu Sicherheitsfunktionen	72
7.1	SIL-Fähigkeit	72
7.2	Ermittlung der SIL-Fähigkeiten für eine Sicherheitsfunktion.....	73
7.2.1	Allgemeines.....	73
7.2.2	Zusammenfassung serieller Ketten	73
7.2.3	Zusammenfassung paralleler Ketten	74
8	Ermittlung der Hardware Ausfallraten für jede Sicherheitsfunktion	75
9	Gasdetektion als Teil eines Gesamtsicherheitssystems.....	77
10	Informationspflicht	77

11	Validierung.....	78
12	Management der Funktionalen Sicherheit.....	79
13	Bewertung der Funktionalen Sicherheit	79
14	Dokumentation	79
	Anhang A (normativ) Umsetzung der SIL-Fähigkeiten von Gaswarnsystemen	80
A.1	Einleitung.....	80
A.2	Umsetzung von SIL-Fähigkeiten von Gaswarnsystemen auf die Sicherheits-Integritätslevel der EN 61508 (alle Teile).....	80
	Anhang B (normativ) Umsetzung der Anforderungen der Grundnormen auf Module.....	81
B.1	Allgemeines	81
B.2	SIL-Fähigkeit 1	81
B.3	SIL-Fähigkeit 2	81
B.4	SIL-Fähigkeit 3	82
	Anhang C (informativ) Bestimmung der SIL-Fähigkeit für eine Sicherheitsfunktion des Gaswarnsystems	83
C.1	Allgemeines	83
C.2	Verfahren zur Bestimmung der SIL-Fähigkeit	83
C.3	Beispiel: Bestimmung der SIL-Fähigkeit für ein Gaswarnsystem	88
C.3.1	Allgemeines	88
C.3.2	Beispiel: Zuordnung für Schaltausgänge der Steuereinheiten A und B.....	88
C.3.3	Beispiel: Zuordnung des Sammelalarm-Schaltausgangs	89
	Anhang D (informativ) Fehlermodi für spezifische Messprinzipien	92
D.1	Einleitung.....	92
D.2	Für die meisten oder alle Messprinzipien und Typen von Sensorelementen anwendbare Ausfall-/Fehlermodi.....	92
D.2.1	Allgemeine Ausfall-/Fehlermodi.....	92
D.2.2	In den messtechnischen Normen betrachtete Ausfall-/Fehlermodi	92
D.3	Wärmetönungs-Sensorelemente.....	93
D.4	Wärmeleitfähigkeits-Sensorelemente.....	93
D.5	Infrarot-Sensorelemente.....	93
D.5.1	Punktdetektoren	93
D.5.2	Detektoren mit offener Messstrecke.....	93
D.5.3	TDLAS (z. B. für Sauerstoff).....	94
D.6	Halbleiter-Sensorelemente	94
D.7	Elektrochemische-Sensorelemente.....	94
D.7.1	Galvanisch – Sauerstoff auf Bleibasis	94
D.7.2	Amperometrisch mit organischem oder wässrigem Elektrolyten	95
D.8	FID-Sensorelemente	95
D.9	FTA-Sensorelemente	95
D.10	Paramagnetische Sensorelemente	96

D.10.1 Allgemeines.....	96
D.10.2 Messprinzip unter Benutzung einer Hantel.....	96
D.10.3 Mikroströmungsmessprinzip	96
D.10.4 Messung der magnetischen Suszeptibilität.....	96
D.10.5 Paramagnetische Temperatureffekte.....	97
D.11 PID-Sensorelemente.....	97

Bilder

Bild 1 – Begriffe Messstelle, Messplatz und Messor.....	15
Bild 2a – Gaswarnsystem plus Aktor für Sicherheitsfunktion	19
Bild 2b – Gaswarnsystem plus Aktor für Sicherheitsfunktion	20
Bild 2c – Gasdetektor mit Relaisausgang plus Aktor für Sicherheitsfunktion.....	21
Bild 2d – Gaswarnsystem plus Aktor für Sicherheitsfunktion	22
Bild 2e – Gaswarnsystem plus Aktor für Sicherheitsfunktion	22
Bild 2f – Gaswarnsystem plus Aktor für Sicherheitsfunktion	23
Bild 2g – Gaswarnsystem plus Aktor für Sicherheitsfunktion.....	24
Bild 2 – Beispiele für die gesamte Sicherheitsfunktion von Gaswarnsystemen.....	24
Bild 3 – Überblick über ein sicherheitsbezogenes System	28
Bild 4 – Module eines Gaswarnsystems	30
Bild 5 – Architekturen für Datenkommunikation	38
Bild 6 – Serielle und parallele Ketten	73
Bild 7 – Behandlung komplexer Module in einer redundanten Anordnung.....	75
Bild C.1 – Schritt 1 – Verknüpfungen der Module	83
Bild C.2 – Schritt 2 – Ermittlung der für die Sicherheitsfunktion notwendigen Module	84
Bild C.3 – Schritt 3 – Eliminierung der für die Sicherheitsfunktion nicht benötigten Module und Verknüpfungen.....	84
Bild C.4 – Schritt 4 (1. Durchlauf) – Zusammenfassung serieller Ketten.....	84
Bild C.5 – Schritt 5 (1. Durchlauf) – Zusammenfassung paralleler Ketten.....	85
Bild C.6 – Schritt 6 (1. Durchlauf) – Anpassung der Struktur des Blockschaltbildes	86
Bild C.7 – Schritt 4 (2. Durchlauf) – Zusammenfassung serieller Ketten.....	87
Bild C.8 – Schritt 5 (2. Durchlauf) – Zusammenfassung paralleler Ketten.....	87
Bild C.9 – Schritt 6 (2. Durchlauf) – Anpassung der Struktur des Blockschaltbildes – <i>Keine Aktion erforderlich</i>	87
Bild C.10 – Schritt 4 (3. Durchlauf) – Zusammenfassung serieller Ketten.....	87
Bild C.11 – Schritt 5 (3. Durchlauf) – Zusammenfassung paralleler Ketten.....	87
Bild C.12 – Schritt 6 (3. Durchlauf) – Anpassung der Struktur des Blockschaltbildes – <i>Keine Aktion erforderlich</i>	87
Bild C.13 – Schritt (4. Durchlauf) – Zusammenfassung serieller Ketten – <i>Ende des Verfahrens</i>	88
Bild C.14 – Schritt 1 – Verknüpfungen der Module im Beispiel.....	88
Bild C.15 – Schritt 2 – Ermittlung der Module mit Einfluss auf die Sicherheitsfunktion	89
Bild C.16 – Schritt 3 – Eliminierung der Module und Verknüpfungen ohne Einfluss auf die	

	Seite
Sicherheitsfunktion	89
Bild C.17 – Schritt 4 – Zusammenfassung serieller Ketten	89
Bild C.18 – Schritt 5 – Zusammenfassung paralleler Ketten – <i>Ende des Verfahrens</i>	89
Bild C.19 – Schritt 2 – Ermittlung der Module mit Einfluss auf die Sicherheitsfunktion	90
Bild C.20 – Schritt 3 – Eliminierung der Module und Verknüpfungen ohne Einfluss auf die Sicherheitsfunktion	90
Bild C.21 – Schritt 4 (1. Durchlauf) – Zusammenfassung serieller Ketten	90
Bild C.22 – Schritt 5 (1. Durchlauf) – Zusammenfassung paralleler Ketten	91
Bild C.23 – Schritt 6 (1. Durchlauf) – Anpassung der Struktur des Blockschaltbildes – <i>Keine Aktion erforderlich</i>	91
Bild C.24 – Schritt 4 (2. Durchlauf) – Zusammenfassung serieller Ketten – <i>Ende des Verfahrens</i>	91
Tabellen	
Tabelle 1 – Fehlertoleranz für einfache Module nach EN 61508-2:2010, Tabelle 2	26
Tabelle 2 – Fehlertoleranz für komplexe Module nach EN 61508-2:2010, Tabelle 3	26
Tabelle 3 – Diagnoseverfahren für die Programmablauf-Überwachung aus EN 61508-2	44
Tabelle 4 – Diagnoseverfahren für Speicher aus EN 61508-2	45
Tabelle 5 – Liste der ersetzten oder nicht zutreffenden Abschnitte der EN 61508-3:2010	54
Tabelle 6 – Liste der Änderungen gegenüber Abschnitten der EN 61508-3:2010	55
Tabelle 7 – EN 50402 Grade der Strenge	57
Tabelle 8 – EN 50402 Spezifikation der Softwareanforderungen (aus EN 61508-3:2010, Tabelle A.1)	58
Tabelle 9 – Semiformale und formale Methoden (aus EN 61508-3:2010, Tabelle B.7) wie in Tabelle A.1 angewendet	59
Tabelle 10 – EN 50402 Entwurf der Softwarearchitektur (aus EN 61508-3:2010, Tabelle A.2)	61
Tabelle 11 – EN 50402 Softwareentwurf (aus EN 61508-3:2010, Tabelle A.3)	64
Tabelle 12 – EN 50402 Softwareentwurf (aus EN 61508-3:2010, Tabelle A.4)	64
Tabelle 13 – Semiformale Methoden (aus EN 61508-3:2010, Tabelle B.7) wie bei Tabelle A.4 angewendet	66
Tabelle 14 – EN 50402 Softwaremodultests und Softwareintegration (aus EN 61508-3:2010, Tabelle A.5) (1 von 2)	66
Tabelle 15 – EN 50402 PE-Integration (Hardware + Software) (aus EN 61508-3:2010, Tabelle A.6)	68
Tabelle 16 – EN 50402 Softwarevalidierung (aus EN 61508-3:2010, Tabelle A.7)	69
Tabelle 17 – EN 50402 Modifikation (aus EN 61508-3:2010, Tabelle A.8)	69
Tabelle 18 – EN 50402 Softwareverifikation (aus EN 61508-3:2010, Tabelle A.9)	70
Tabelle 19 – Für den Betrieb mit niedriger Anforderungsrate (low demand mode) (siehe EN 61508-1:2010, 7.6.2.9, Tabelle 2)	76
Tabelle 20 – Für den Betrieb mit hoher Anforderungsrate (high demand mode) oder für kontinuierlichen Betrieb (siehe EN 61508-1:2010, 7.6.2.9, Tabelle 3)	77
Tabelle A.1 – Umsetzung der SIL-Fähigkeiten nach EN 50402 in SIL nach EN 61508 (alle Teile)	80
Tabelle C.1 – Ermittlung der SIL-Fähigkeit für ein paralleles Kettenglied (anwendbar nur für Hardware)	86

Europäisches Vorwort

Dieses Dokument (EN 50402:2017) wurde ausgearbeitet von CLC/SC 31-9 „Elektrische Geräte für das Aufspüren und die Messung brennbarer Gase zur Verwendung in industriellen und gewerblichen explosionsgefährdeten Bereichen“ des CLC/TC 31 „Elektrische Betriebsmittel für explosionsgefährdete Bereiche“ und vom CLC/TC 216 „Gaswarngeräte“.

Nachstehende Daten wurden festgelegt:

- spätestes Datum, zu dem dieses Dokument auf nationaler Ebene durch Veröffentlichung einer identischen nationalen Norm oder durch Anerkennung übernommen werden muss (dop): 2018-02-04
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2020-02-04

Dieses Dokument ersetzt **EN 50402:2005**.

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

EN 50402:2017 enthält folgende wesentlichen technischen Änderungen gegenüber **EN 50402:2005**:

- Die Norm wurde allgemein aktualisiert, um die Änderungen in der zweiten Ausgabe der EN 61508 bezüglich Hardware und Software zu berücksichtigen. Pfad 2 der zweiten Ausgabe der EN 61508 wird für Gaswarneinrichtungen nicht erlaubt.
- Die Norm wurde aktualisiert zur Übereinstimmung der Anforderungen für SIL 1 mit der zweiten Ausgabe der **EN 50271**, die die Mindestanforderungen an die funktionale Sicherheit im Rahmen der messtechnischen Prüfung von Gasdetektoren, Gaswarngeräten und vollständigen Gaswarnsystemen festlegt.
- Die jüngsten Überarbeitungen der messtechnischen Normen wurden berücksichtigt.
- SIL 4 wurde gestrichen, weil es für die Gasdetektion unangemessen ist.
- Die **Abschnitte 4 und 5** wurden zwecks einer detaillierteren Spezifikation aktualisiert.
- Der **Abschnitt 6** für Software ist neu.
- Die **Abschnitte 7 bis 11** wurden umstrukturiert, um die Anforderungen und den Bezug zu EN 61508 klarer zu fassen.
- Der **Abschnitt 10** beschreibt detaillierter die Informationen für den Anwender.
- Der vorherige normative **Anhang D** ist nun **Abschnitt 12**.
- Der vorherige informative **Anhang A** wurde gestrichen. Wichtige Textpassagen wurden in die **Abschnitte 7 bis 9** verschoben.
- Der neue informative **Anhang D** liefert Informationen über Ausfall-/Fehlermodi von Sensorelementen.

Einleitung

Diese Europäische Norm stellt Anforderungen an die funktionale Sicherheit von Gaswarnsystemen auf. Sie umfasst Kriterien für Zuverlässigkeit, Fehlervermeidung und Fehlertoleranz. Funktionale Sicherheit ist der Teil der Gesamtsicherheit, der sich spezifisch auf die notwendigen Maßnahmen innerhalb des Gaswarnsystems zur Vermeidung und Beherrschung von Ausfällen bezieht, sodass die Sicherheitsfunktion sichergestellt wird. Dies schließt nicht nur Anforderungen an die Konstruktion und den Entwicklungsprozess des Gaswarnsystems, sondern auch Anforderungen an Informationen bezüglich Planung, Inbetriebnahme, Wartung und Reparatur ein.

Diese Europäische Norm richtet sich an den Hersteller. Wichtige Informationen für den sicheren Einsatz der Geräte (Gaswarnsysteme) werden in der Betriebsanleitung aufgeführt.

Die Funktion eines Gaswarnsystems fällt aus, wenn gefährbringende 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 der Betriebsanleitung ausgeführt werden. Diese Europäische Norm legt nicht die Platzierung von Messstellen/Messorten 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. Aus diesem Grund ist eine allgemeingültige Festlegung von Anforderungen 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 wird normalerweise nicht alle Module enthalten, die in dieser Europäischen Norm enthalten sind. 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 3 die höchste Stufe der funktionalen Sicherheit darstellt, um diese Europäische Norm zu erfüllen. Die SIL-Fähigkeit eines Moduls ist auf den höchsten Sicherheits-Integritätslevel bezogen, der für eine Sicherheitsfunktion unter Verwendung von Modulen dieser festgelegten SIL-Fähigkeit beansprucht werden kann. Module werden hinsichtlich ihrer SIL-Fähigkeit beschrieben. Es werden außerdem Informationen bezüglich der Ausfallraten der Module oder der zugehörigen physikalischen Komponenten benötigt, um dem Hersteller zu ermöglichen, die Stufe der funktionalen Sicherheit für das gesamte Gaswarnsystem bestimmen zu können. Auf diese Weise berücksichtigt der Hersteller sowohl zufällige Ausfälle der Hardware als auch systematische Ausfälle in Hard- und Software. Diese Europäische Norm legt ebenfalls die Anforderungen fest, die es ermöglichen zu bestimmen, ob das Gaswarnsystem in Verbindung mit anderen für die funktionale Sicherheit benötigten Geräten eine ausreichend niedrige Ausfallrate 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 ein spezifisches Modul bzw. eine Komponente nur ein einziges Mal erforderlich.

Abhängig von der Einstufung jedes Moduls und jeder Komponente werden die Eigenschaften für jede ausgewählte Sicherheitsfunktion des gesamten Gaswarnsystems 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. Unterschiedliche Kombinationen von gleichwertigen Modulen können zu Gaswarnsystemen mit unterschiedlichen SIL-Fähigkeiten führen.

Auf diese Weise wird eine flexible Anpassung der Gaswarnsysteme an verschiedene Anwendungen 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.

Diese Europäische Norm ist an Hersteller gerichtet und ist als Grundlage für die Prüfung der funktionalen Sicherheit anwendbar auf Gaswarnsysteme oder Teile davon (z. B. Gasmesstransmitter oder Gaswarn-Steuereinheiten). Sie ergänzt die Anforderungen der anwendbaren messtechnischen Normen. Sie sollte nicht mit der **EN 60079-29-3** verwechselt werden, die sich an Systemintegratoren richtet. **EN 60079-29-3** dient als Leitfaden für das Kombinieren von Gaswarngeräten mit anderen Einrichtungen (z. B. Gasaufbereitung, Filter, Ventile), die nicht vom Gaswarnhersteller geliefert werden, aber Teil einer Sicherheitsfunktion sind und im Verantwortungsbereich des Systemintegrators liegen.

1 Anwendungsbereich

Diese Europäische Norm ist anwendbar auf Geräte und Systeme zur Detektion und Messung von brennbaren oder toxischen Gasen oder Dämpfen oder Sauerstoff. Sie umfasst Geräte, die zur zuverlässigen Messung einer Gaskonzentration vorgesehen sind und ein Ausgangssignal (Alarm und/oder Messwertsignal) abgeben, um vor einer möglichen Gefahr zu warnen.

Diese Europäische Norm ist eine Produktnorm auf Grundlage der EN 61508 (alle Teile) und umfasst für Gaswarnsysteme sowohl Anwendungen mit niedriger als auch mit hoher Anforderungsrate ausschließlich für die SIL-Fähigkeiten 1, 2 oder 3. Gaswarngeräte und Gaswarnsysteme werden als generische Produkte entwickelt. Diese Europäische Norm deckt Teile der Phase 10 „Realisierung“ des in [EN 61508-1:2010, Bild 2](#) definierten Gesamt-Sicherheitslebenszyklus ab. Die Konfiguration und Integration für spezifische Anwendungen werden von dieser Europäischen Norm nicht behandelt.

Im Falle eines Widerspruchs zwischen den Anforderungen dieser Europäischen Norm und denen der EN 61508 hat EN 50402 Vorrang.

ANMERKUNG 1 Anwendungen, die eine SIL-Fähigkeit 4 für ein Gaswarnsystem erfordern, sind nicht praktikabel.

Diese Europäische Norm ist hauptsächlich auf ortsfeste Geräte und Systeme ausgerichtet. Sie kann aber ebenso auf transportable Gaswarngeräte angewendet werden, die als vorübergehender Ersatz für ortsfeste Geräte vorgesehen sind.

Diese Europäische Norm ergänzt die Anforderungen der Europäischen Normen an elektrische Geräte zur Detektion und Messung von brennbaren Gasen, Dämpfen (z. B. [EN 60079-29-1](#) oder [EN 60079-29-4](#)), toxischen Gasen (z. B. EN 45544) oder Sauerstoff (z. B. [EN 50104](#)).

ANMERKUNG 2 Diese Europäischen Normen werden im Text als „messtechnische Normen“ bezeichnet.

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.

[EN 50271](#) legt Mindestanforderungen für Geräte fest, die Software und/oder digitale Komponenten benutzen. Sie legt außerdem zusätzliche optionale Anforderungen zur Konformität mit SIL 1 im Betrieb mit niedriger Anforderungsrate fest. EN 50402 schließt alle Anforderungen der [EN 50271](#) ein.

EN 50402 ist ebenfalls für Geräte und Gaswarnsysteme und/oder Komponenten bestimmt und sollte in folgenden Fällen anstelle von [EN 50271](#) angewendet werden:

- für SIL 1, wenn das System Komponenten enthält, die nicht durch [EN 50271](#) abgedeckt sind;
- für SIL 1 im Betrieb mit hoher Anforderungsrate;
- für SIL 2 und SIL 3;
- für alle SIL's bei nicht auf Digitaltechnik basierenden Geräten.

Die Anwendung der oben genannten messtechnischen Normen stellt ein angemessenes messtechnisches Betriebsverhalten im Normalbetrieb des Gaswarnsystems sicher. Zusätzlich beziehen sich die Anforderungen dieser Europäischen Norm auf die funktionale Sicherheit von Gaswarnsystemen und umfassen Kriterien für Zuverlässigkeit, Fehlertoleranz und Vermeidung systematischer Ausfälle. Die Vermeidung und Beherrschung systematischer Ausfälle wird durch Anforderungen an Entwicklungsprozesse und Verfahren sowie während der Entwicklung gewählte Diagnosemaßnahmen abgedeckt. 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 Sicherheitsleveln wider. Dadurch wird es dem Anwender ermöglicht, das Gaswarnsystem in ein Gesamtsicherheitssystem nach den Sicherheits-Integritätsleveln der EN 61508 (alle Teile) einzubinden.

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

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

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

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

ANMERKUNG 3 Die für eine Anwendung erforderliche SIL-Fähigkeit wird vom Anwender festgelegt (siehe [Abschnitt 9](#) und [Anhang A](#)).

2 Normative Verweisungen

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

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

EN 45544-2, *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 2: Anforderungen an das Betriebsverhalten von Geräten, die für Expositionsmessungen eingesetzt werden*

EN 45544-3, *Arbeitsplatzatmosphäre – Elektrische Geräte für die direkte Detektion und direkte Konzentrationsmessung toxischer Gase und Dämpfe – Teil 3: Anforderungen an das Betriebsverhalten von Geräten, die für allgemeine Gaswarnanwendungen eingesetzt werden*

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

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

EN 50159, *Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante Kommunikation in Übertragungssystemen*

EN 50270, *Elektromagnetische Verträglichkeit – Elektrische Geräte für die Detektion und Messung von brennbaren Gasen, toxischen Gasen oder Sauerstoff*

EN 50271:2010, *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*

EN 60079-29-1:2016, *Explosionsfähige Atmosphäre – Teil 29-1: Gasmessgeräte – Anforderungen an das Betriebsverhalten von Geräten für die Messung brennbarer Gase (IEC 60079-29-1:2016, modifiziert)*

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

EN 60079-29-3, *Explosionsfähige Atmosphäre – Teil 29-3: Gasmessgeräte – Leitfaden zur funktionalen Sicherheit von ortsfesten Gaswarnsystemen (IEC 60079-29-3)*

EN 60079-29-4, *Explosionsfähige Atmosphäre – Teil 29-4: Gasmessgeräte – Anforderungen an das Betriebsverhalten von Geräten mit offener Messstrecke für die Messung brennbarer Gase (IEC 60079-29-4)*

EN 61326-3-1, *Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Allgemeine industrielle Anwendungen (IEC 61326-3-1)*

EN 61326-3-2, *Elektrische Mess-, Steuer-, Regel- und Laborgeräte – EMV-Anforderungen – Teil 3-2: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) – Industrielle Anwendungen in spezifizierter elektromagnetischer Umgebung (IEC 61326-3-2)*

EN 61508-1:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 1: Allgemeine Anforderungen (IEC 61508-1:2010)*

EN 61508-2:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010)*

EN 61508-3:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 3: Anforderungen an Software (IEC 61508-3:2010)*

EN 61508-4:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 4: Begriffe und Abkürzungen (IEC 61508-4:2010)*

EN 61508-5:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level) (IEC 61508-5: 2010)*

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

EN 61508-7:2010, *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 7: Anwendungshinweise über Verfahren und Maßnahmen (IEC 61508-7:2010)*

EN 61784-3:2016, *Industrielle Kommunikationsnetze – Profile – Teil 3: Funktional sichere Übertragung bei Feldbussen – Allgemeine Regeln und Festlegungen für Profile (IEC 61784-3: 2016)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach **EN 60079-29-1** und **EN 61508-4:2010** und die folgenden Begriffe.

Einige Begriffe werden zur Bequemlichkeit des Lesers wiederholt. Einige Begriffe aus **EN 61508-4:2010** sind für die Gasdetektion angepasst worden.

3.1

funktionale Sicherheit

Teil der Gesamtsicherheit, bezogen auf die EUC-Einrichtung (en: equipment under control – EUC) und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des elektrischen/elektronischen/programmierbaren elektronischen sicherheitsbezogenen Systems (E/E/PES) und anderer risikomindernder Maßnahmen abhängt

Anmerkung 1 zum Begriff: Das EUC ist die überwachte Einrichtung oder die Einrichtung oder Umgebung, die das Gaswarnsystem absichert (**EN 61508-4:2010, 3.2.1** modifiziert).

Anmerkung 2 zum Begriff: Das EUC-Leit- oder Steuerungssystem reagiert auf Eingangssignale und erzeugt Ausgangssignale, die die EUC in der gewünschten Art arbeiten lassen (**EN 61508-4:2010, 3.3.3** modifiziert).

Anmerkung 3 zum Begriff: Das Gaswarnsystem ist Teil des E/E/PES.

[QUELLE: EN 61508-4:2010, 3.1.12, Anmerkungen modifiziert]

3.2

Sicherheitsfunktion eines Gaswarnsystems

jede von dem Gaswarnsystem ausgeführte Funktion (von der Messgaszuführung bis zum Ausgang des Gaswarnsystems reichend), die nach Angaben des Herstellers sicherheitsbezogen ist

3.3

sicherheitsbezogenes Teil

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

3.4

Fehler

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

[QUELLE: EN 61508-4:2010, 3.6.1]

3.5

Fehlertoleranz

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

[QUELLE: EN 61508-4:2010, 3.6.3]

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. Im Sinne dieser Norm gibt es drei verschiedene SIL-Fähigkeiten, bezeichnet mit Nummern von 1 bis 3, wobei die SIL-Fähigkeit 3 für die höchste Stufe des sicheren Betriebsverhaltens steht. Jedem Modul oder der Kombination von Modulen wird nach der Klasse der Anteile sicherer Fehler (*SFF*) und der Fehleraten (λ) eine SIL-Fähigkeit zugeordnet.

3.7

entwickelt für SIL-Fähigkeit

spezielle Form des obigen Begriffs SIL-Fähigkeit. Er beschreibt die Klasse der Anteile ungefährlicher Ausfälle (*SFF*) ohne einen Bezug zu den Fehlerraten.

Der Begriff wird für funktionale Module benutzt, bei denen die Fehlermodi allgemein anwendbar sind, aber die Fehlerraten von den Anwendungen abhängig sind und deshalb nicht allgemein vom Hersteller bestimmt werden können.

3.8

Modul

der Begriff Modul wird in zwei verschiedenen Zusammenhängen benutzt.

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

Anmerkung 1 zum Begriff: Funktionale Module können einfach oder komplex sein (siehe 4.3).

Der Begriff Software-Modul wird in der Bedeutung der EN 61508-3:2010 benutzt.

3.9

Element

funktionale Untereinheit zu einem Modul

Anmerkung 1 zum Begriff: Die Software oder ein Teil von ihr dürfen als ein Element behandelt werden.

3.10

Komponente

der Hardwareaufbau des Gaswarnsystems besteht aus Komponenten als physikalisch trennbare Baugruppen

Anmerkung 1 zum Begriff: Abhängig von der jeweiligen Realisierung kann ein Element eines funktionalen Moduls zu verschiedenen Hardwarekomponenten gehören.

3.11

Peripherie

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

Anmerkung 1 zum Begriff: Siehe [Bild 3](#).

Anmerkung 2 zum Begriff: Die Peripherie liegt außerhalb des Anwendungsbereiches dieser Europäischen Norm.

3.12

Messstelle

Installationsort eines einzelnen Sensors im Diffusionsbetrieb oder einer Probenahmesonde

Anmerkung 1 zum Begriff: Siehe [Bild 1](#).

3.13

Messort

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

Anmerkung 1 zum Begriff: Siehe [Bild 1](#).

3.14

Messplatz

redundante Kombination zweier Messstellen eines Messortes

Anmerkung 1 zum Begriff: Siehe [Bild 1](#).

Anmerkung 2 zum Begriff: Bei Übereinstimmung mit den Begriffen 3.12 bis 3.14 ist es möglich, dass ein einzelner Sensor als redundanter Kombinationspartner für verschiedene andere Sensoren dient.

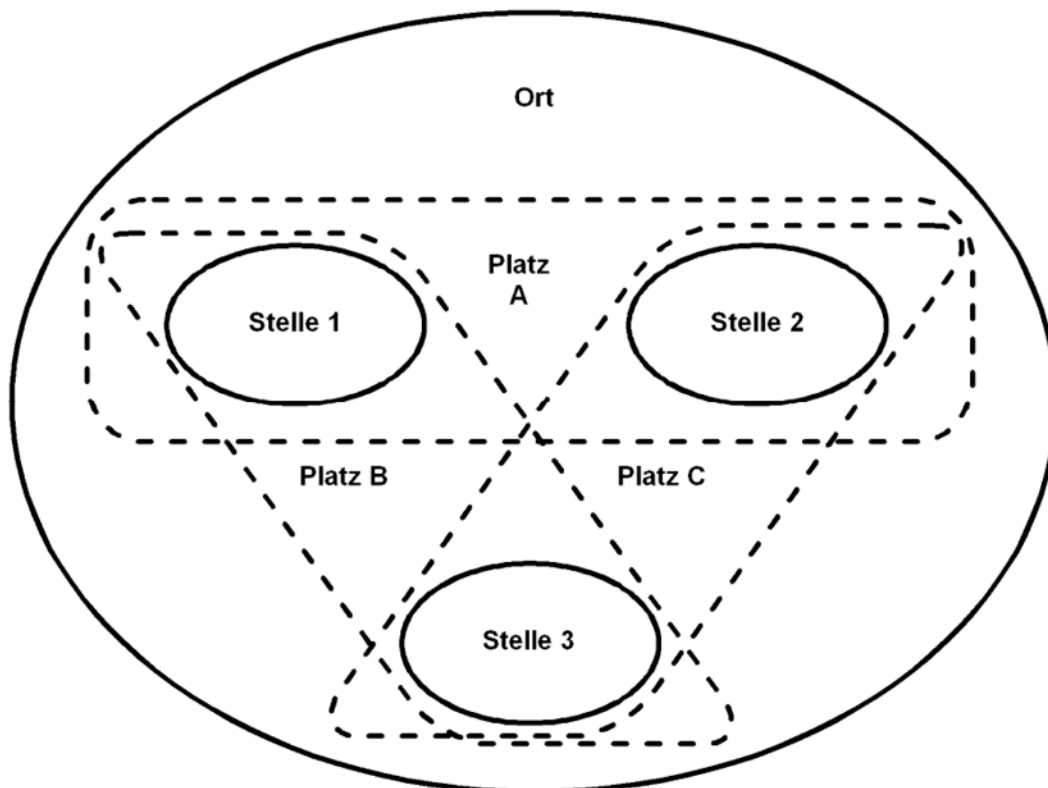


Bild 1 – Begriffe Messstelle, Messplatz und Messort

3.15

Messsignal

gegebenenfalls vorverstärktes Sensorsignal in analoger oder digitaler Form

3.16

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.

3.17

Statussignal

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

3.18

Alarmsignal

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

3.19

Sonderzustand

jeder Zustand des Gerätes, bei dem nicht die Überwachung der Gaskonzentration und/oder Alarmierung beabsichtigt ist

Anmerkung 1 zum Begriff: Sonderzustand umfasst Anwärmphase, Kalibriermodus oder Störung.

[QUELLE: EN 60079-29-1:2016, 3.5.4]

3.20

Parameter

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

3.21

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. Wenn der Hersteller kürzere Einstellzeiten angibt, müssen diese die Grundlage für die kleinste Einstellzeit darstellen.

3.22

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.

3.23

Selbsttestfunktionen

zyklisch wiederholte Testroutinen, die den Messbetrieb nicht unterbrechen. Testroutinen können auch vor Aufnahme des Betriebs während der Einschaltverzögerung eines Gaswarnsystems ausgeführt werden, bevor es den Messbetrieb aufnimmt, auf Benutzeranforderung ablaufen oder können im Kalibriermodus für einzelne Messstellen oder Teile des Gaswarnsystems ausgelöst werden. Diese Funktionen können innerhalb eines einzelnen Moduls oder einer Kombination von verbundenen Modulen ablaufen.

3.24

Kontrolle

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

3.25

Verifikation

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

[QUELLE: EN 61508-4:2010, 3.8.1]

3.26

Validierung

Bestätigen aufgrund einer Untersuchung und durch Bereitstellung eines Nachweises, dass die besonderen Anforderungen für eine spezielle beabsichtigte Verwendung erfüllt worden sind

[QUELLE: EN 61508-4:2010, 3.8.2]

3.27

Redundanz

Vorhandensein von mehr als einem Mittel zum Ausführen einer geforderten Funktion oder zur Darstellung von Informationen

Anmerkung 1 zum Begriff: Redundanz wird hauptsächlich verwendet, um die Zuverlässigkeit (Wahrscheinlichkeit der richtigen Funktion über einen gegebenen Zeitraum) oder die Verfügbarkeit (Wahrscheinlichkeit der Funktion zu einem gegebenen Moment) zu verbessern.

[QUELLE: EN 61508-4:2010, 3.4.6, Anmerkungen modifiziert]

3.28

Verfügbarkeit

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

3.29

Diffusionsbetrieb

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

3.30

Messgasförderung

Betrieb, bei dem der Transport des Gases aus der Atmosphäre zum Gassensorelement durch Ansaugen unter Benutzung von Komponenten, deren primärer Zweck darin besteht, einen Gasfluss zu erzeugen, z. B. durch eine Pumpe, erfolgt

3.31

spezifizierter Bereich von Eingangswerten

Bereich von analogen Eingangswerten, der mit dem digitalen Bereich von Ausgangswerten eines A/D-Umsetzers korrespondiert, oder Bereich von digitalen Eingangswerten, der mit dem analogen Bereich von Ausgangswerten eines D/A-Umsetzers korrespondiert. Die kleinsten und größten Digitalwerte des Umsetzers dürfen nicht als Werte innerhalb des spezifizierten Bereichs betrachtet werden, da Kleinst- und Größtwert mit stuck-at-Fehlern korrespondieren, die von dem Gerät erkannt werden müssen.

3.32

definierter Bereich von Eingangswerten

Bereich von Eingangswerten, der vom Hersteller des Geräts als gültig definiert wurde; der definierte Bereich ist ein Unterbereich des spezifizierten Bereichs von Eingangswerten

3.33

eingeschränkter Messbetrieb

Betriebsart des Gesamtsystems, bei der es nicht die ursprünglichen Anforderungen an das Betriebsverhalten erfüllt oder es einen Redundanzlevel verloren hat

3.34

Störungssignal

hörbares, sichtbares oder anderes Ausgangssignal, das sich vom Alarmsignal unterscheidet und das entweder direkt oder indirekt zu einer Warnung oder Anzeige führt, dass das Gerät nicht einwandfrei arbeitet

4 Allgemeine Anforderungen

4.1 Spezifikation der Sicherheitsfunktionen

Die Sicherheitsfunktion eines Gaswarnsystems ist sehr eng verwandt mit der in der einschlägigen messtechnischen Norm festgelegten Messfunktion. Die Grundnorm für funktionale Sicherheit, EN 61508, berücksichtigt, dass Umweltbedingungen, Messsignalabweichungen und EMV-Störungen einen wesentlichen Einfluss auf die funktionale Sicherheit eines Gerätes oder eines Gesamtsicherheitssystems besitzen. Deshalb muss ein Gaswarnsystem auch den einschlägigen messtechnischen Normen entsprechen, zum Beispiel EN 60079-29-1 oder EN 60079-29-4 für die Detektion und Messung brennbarer Gase, EN 45544-1, EN 45544-2 und EN 45544-3 für toxische Gase und EN 50104 für Sauerstoff.

Gaswarneinrichtungen müssen EN 50270 entsprechen, die die EMV-Anforderungen für alle Arten von Gaswarneinrichtungen festlegt, ebenfalls unter Berücksichtigung der funktionalen Sicherheit. Im Fall eines Widerspruchs zwischen den Anforderungen der EN 50270 und denen der EN 61326-3-1 und/oder der EN 61326-3-2 hat EN 50270 Vorrang.

Die funktionale Sicherheit von Gaswarnsystemen hängt außerdem von ordnungsgemäßer Installation, Betrieb und Wartung ab, die in der Verantwortung des Anwenders liegen. Anleitungen zu Auswahl, Installation, sicherem Gebrauch und Instandhaltung werden in [EN 60079-29-2](#) und [EN 45544-4](#) gegeben.

Der Hersteller der jeweiligen Gaswarneinrichtung muss weitere Informationen in der Betriebsanleitung/in dem Sicherheitshandbuch angeben (siehe Abschnitt 10).

Das gesamte Gaswarnsystem kann sowohl Sicherheitsfunktionen als auch nicht sicherheitsgerichtete Funktionen wahrnehmen. Für die Sicherheitsfunktionen kann das gesamte Gaswarnsystem Kombinationen verschiedener SIL-Fähigkeiten für unterschiedliche Sicherheitsfunktionen enthalten. Die SIL-Fähigkeit kann für eine oder mehrere Sicherheitsfunktionen bestimmt werden. Der Prozess der Zuweisung von Funktionen beginnt an der Messstelle bzw. dem Messort und endet bei der zugehörigen sicherheitsbezogenen Ausgangsfunktion (siehe [Bild 2](#)).

Die Sicherheitsfunktionen eines Gaswarnsystems müssen getrennt voneinander und von den nicht sicherheitsgerichteten bewertet werden.

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 allgemeingültige Festlegung von Anforderungen ist auf dieser Grundlage nicht möglich.

[Abschnitt 5](#) enthält die für Gaswarnsysteme spezifischen funktionalen Anforderungen und ist hauptsächlich auf die Hardware ausgerichtet. Dieser Abschnitt legt die Hardwareanforderungen von [EN 61508-2](#) für Gaswarnsysteme fest.

ANMERKUNG Die EN 50402 ist der empfohlene Weg der [EN 61508-2](#) für Gaswarneinrichtungen einschließlich Gaswarn-Steuereinheiten (siehe [Bild 2](#)) zu entsprechen.

Gaswarnsysteme werden für die Bewertung in funktionale Module aufgeteilt, um sicherzustellen, dass Systeme unterschiedlichen Aufbaus mittels geeigneter Verfahren behandelt werden können. Ein Gaswarnsystem wird normalerweise nicht alle Module enthalten, die in dieser Europäischen Norm enthalten sind. 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-Fähigkeiten bezeichnet, wobei die SIL-Fähigkeit 1 die niedrigste und die SIL-Fähigkeit 3 die höchste Stufe für das Betriebsverhalten darstellt, um diese Europäische Norm zu erfüllen.

[Abschnitt 6](#) spezifiziert gaswarnspezifische Anforderungen an Software auf Grundlage der [EN 50271:2010](#) und gaswarnspezifische Auslegungen und Ergänzungen zu [EN 61508-3:2010](#).

In [Abschnitt 7](#) werden funktionale Module zum Erreichen einer SIL-Fähigkeit für eine oder mehrere Sicherheitsfunktionen miteinander kombiniert.

In [Abschnitt 8](#) wird eine Berechnung der Hardware-Fehlerraten (*PFD* und/oder *PFH*) für eine oder mehrere Sicherheitsfunktionen durchgeführt.

Falls die Bestimmungen nach [Abschnitt 7](#) und [Abschnitt 8](#) zu verschiedenen SIL-Fähigkeiten führen, gilt die niedrigere SIL-Fähigkeit für die zugehörige Sicherheitsfunktion.

[Abschnitt 9](#) betrachtet das Gaswarnsystem als Teil eines Gesamtsicherheitssystems.

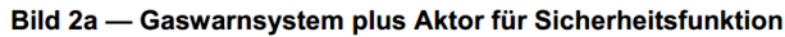
[Abschnitt 10](#) spezifiziert die Informationspflichten in Bezug auf die Betriebsanleitung.

[Abschnitt 11](#) betrachtet die Validierung des Gaswarnsystems.

[Abschnitte 12 bis 14](#) betrachten die zugehörigen Anforderungen an das Management der funktionalen Sicherheit, an die Beurteilung der funktionalen Sicherheit und an die Dokumentation.

Das gesamte Gaswarnsystem besteht aus einem oder mehreren Gasdetektoren und einer Gaswarn-Steuereinheit, die sicherheitsgerichtete Ausgangsfunktionen (z. B. Schaltausgänge) ansteuert. Die Gaswarn-Steuereinheit könnte auch als getrenntes Gerät ausgeführt werden (z. B. eine SPS). Das gesamte

Die Bilder 2a bis 2g zeigen sieben verschiedene Beispiele für Gaswarnsysteme.



Der vom Schaltausgang des Gaswarnsystems angesteuerte Aktor gehört zum Anwendungsbereich der EN 61508 (alle Teile).

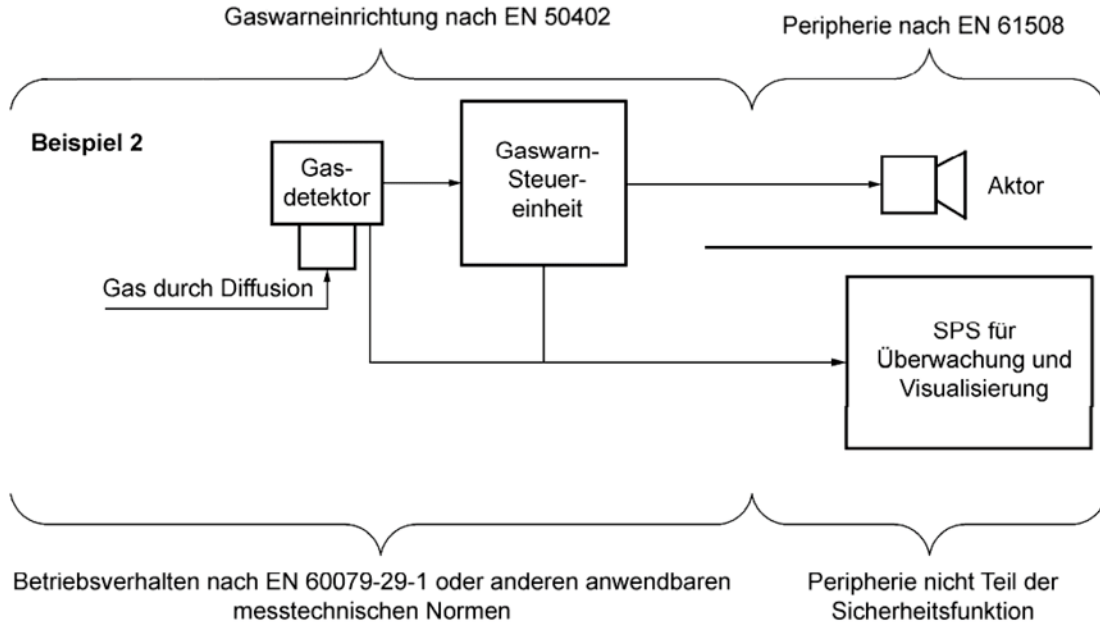


Bild 2b — Gaswarnsystem plus Aktor für Sicherheitsfunktion

Beschreibung der Sicherheitsfunktion:

Im Beispiel 2 in Bild 2b ist der Gasdetektor ein Gasmessstransmitter mit

- einem genormten Ausgangssignal (z. B. 4 – 20 mA),
- einer digitalen Übertragung von Messwert und Statusinformationen.

Gasmesstransmitter und separate Gaswarn-Steuereinheit einschließlich des Schaltausgangs gehören zum Anwendungsbereich der anwendbaren messtechnischen Norm sowie der EN 50402.

Der vom Schaltausgang des Gaswarnsystems angesteuerte Aktor gehört zum Anwendungsbereich der EN 61508 (alle Teile).

Beschreibung der nicht sicherheitsbezogenen Signale:

Die SPS gehört zur „Peripherie“ und ist nicht Bestandteil der Sicherheitsfunktion. Sie liegt deshalb außerhalb des Anwendungsbereiches dieser Europäischen Norm. Es gibt keine Anforderungen an das Betriebsverhalten für die SPS solange sie nicht Bestandteil der Sicherheitsfunktion ist. Die SPS empfängt Daten vom Gasmessstransmitter (4 – 20 mA einschließlich Statussignalen) und/oder von der separaten Gaswarn-Steuereinheit (verarbeitete Messwerte einschließlich ihrer physikalischen (wissenschaftlichen) Einheiten sowie Alarm- und Status-Signale). Diese Daten dürfen zur Visualisierung und Überwachung der Gaskonzentration benutzt werden. Es ist zulässig, dass die SPS zusätzliche Maßnahmen unabhängig von der Sicherheitsfunktion auslöst. Das schließt auch Maßnahmen bei Auftreten von hohen Gaskonzentrationen mit ein. Die SPS kann eine Sicherheits-SPS (EN 61508 zertifiziert) sein oder auch nicht.

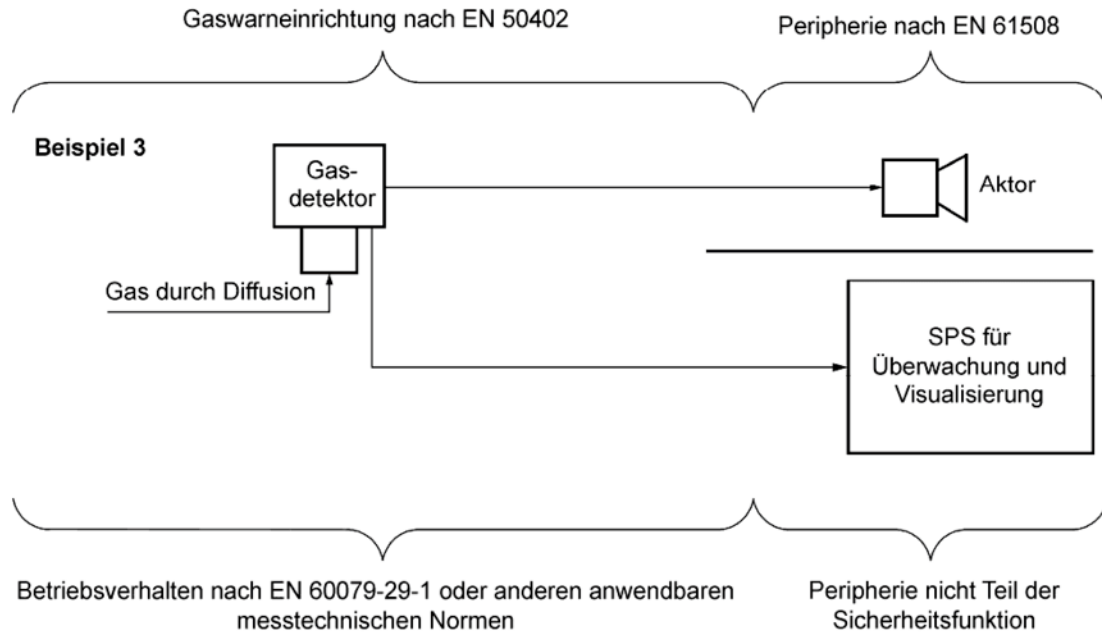


Bild 2c — Gasdetektor mit Relaisausgang plus Aktor für Sicherheitsfunktion

Beschreibung der Sicherheitsfunktion:

Im Beispiel 3 in Bild 2c enthält der Gasdetektor auch die funktionalen Module der Gaswarn-Steuereinheit zur Erzeugung von Alarmen und Ausgangssignalen zur Ansteuerung von Aktoren. Der Gasdetektor arbeitet als komplettes Gaswarnsystem im Anwendungsbereich der EN 50402 und der messtechnischen Normen.

Der vom Schaltausgang des Gasdetektors angesteuerte Aktor gehört zum Anwendungsbereich der EN 61508 (alle Teile).

Beschreibung der nicht sicherheitsbezogenen Signale:

Die SPS gehört zur „Peripherie“ und ist nicht Bestandteil der Sicherheitsfunktion. Sie liegt deshalb außerhalb des Anwendungsbereiches dieser Europäischen Norm. Es gibt keine Anforderungen an das Betriebsverhalten für die SPS solange sie nicht Bestandteil der Sicherheitsfunktion ist. Die SPS empfängt Daten vom Gasmessstransmitter (4 – 20 mA einschließlich Statussignalen) und/oder von der separaten Gaswarn-Steuereinheit (verarbeitete Messwerte einschließlich ihrer physikalischen (wissenschaftlichen) Einheiten sowie Alarm- und Status-Signale). Diese Daten dürfen zur Visualisierung und Überwachung der Gaskonzentration benutzt werden. Es ist zulässig, dass die SPS zusätzliche Maßnahmen unabhängig von der Sicherheitsfunktion auslöst. Das schließt auch Maßnahmen bei Auftreten von hohen Gaskonzentrationen mit ein. Die SPS kann eine Sicherheits-SPS (EN 61508 zertifiziert) sein oder auch nicht.

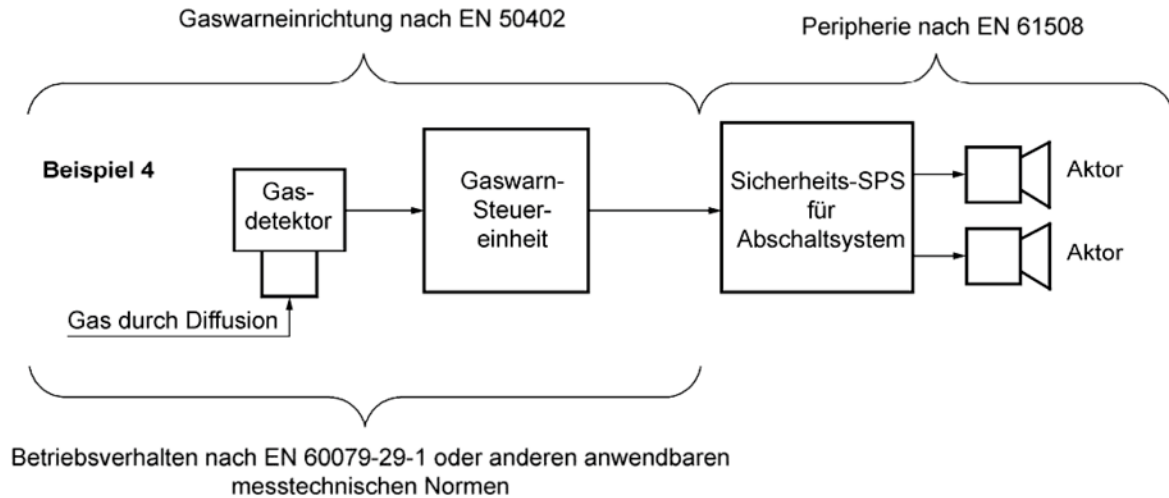


Bild 2d — Gaswarnsystem plus Aktor für Sicherheitsfunktion

Im Beispiel 4 in Bild 2d ist der Gasdetektor ein Gasesstransmitter mit

- einem genormten Ausgangssignal (z. B. 4 – 20 mA),
- einer digitaler Übertragung von Messwert und Statusinformationen.

Gasesstransmitter und separate Gaswarn-Steuereinheit einschließlich des Schaltausgangs gehören zum Anwendungsbereich der anwendbaren messtechnischen Norm sowie der EN 50402. Es gibt keine eins zu eins Beziehung zwischen Alarmausgang und Aktor. Es wird vorausgesetzt, dass die SPS keinen negativen Einfluss auf die sicherheitsbezogenen Ausgänge der Gaswarn-Steuereinheit haben kann.

Die Schaltausgänge des Gaswarnsystems sind sicherheitsbezogene Alarめingänge in die Sicherheits-SPS, die hier als Abschaltssystem arbeitet. Sie korreliert ihre Alarめingänge mit den zugehörigen Aktoren (z. B. durch ein Voting). Die Sicherheits-SPS und die Aktoren gehören zum Anwendungsbereich der EN 61508 (alle Teile).

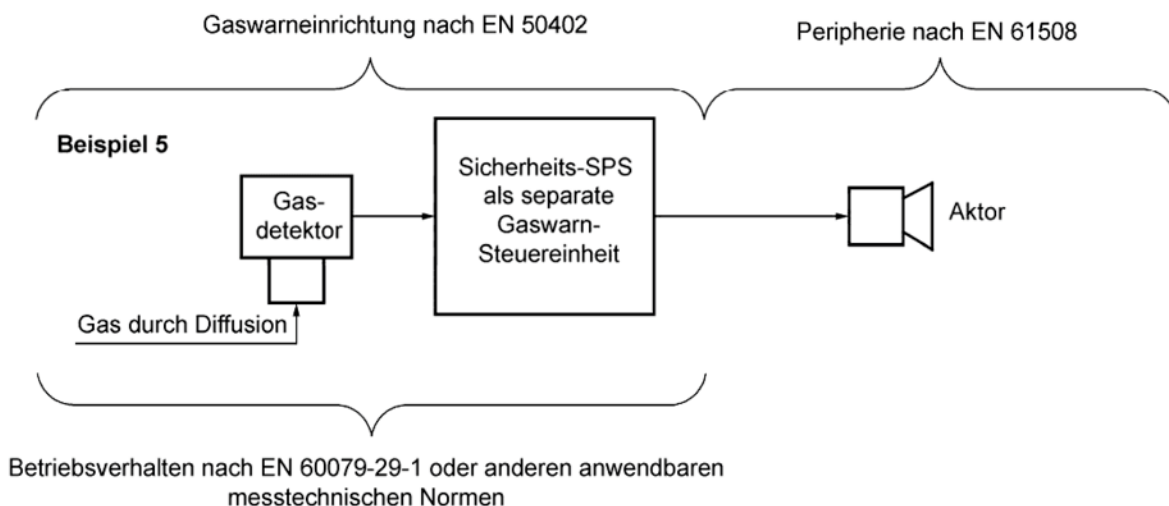


Bild 2e — Gaswarnsystem plus Aktor für Sicherheitsfunktion

Im Beispiel 5 in Bild 2e ist der Gasdetektor ein Gasesstransmitter mit einem genormten Ausgangssignal (z. B. 4 – 20 mA).

Gasmesstransmitter und die als separate Gaswarn-Steuereinheit eingesetzte Sicherheits-SPS einschließlich des Schaltausgangs gehören zum Anwendungsbereich der anwendbaren messtechnischen Norm sowie der EN 50402. Deshalb muss die Sicherheits-SPS **EN 60079-29-1** (brennbare Gase) oder **EN 50104** (Sauerstoff) oder eine andere anwendbare messtechnische Norm, z. B. EN 45544 für toxische Gase, erfüllen.

Der vom Schaltausgang der Sicherheits-SPS angesteuerte Aktor gehört zum Anwendungsbereich der EN 61508 (alle Teile).

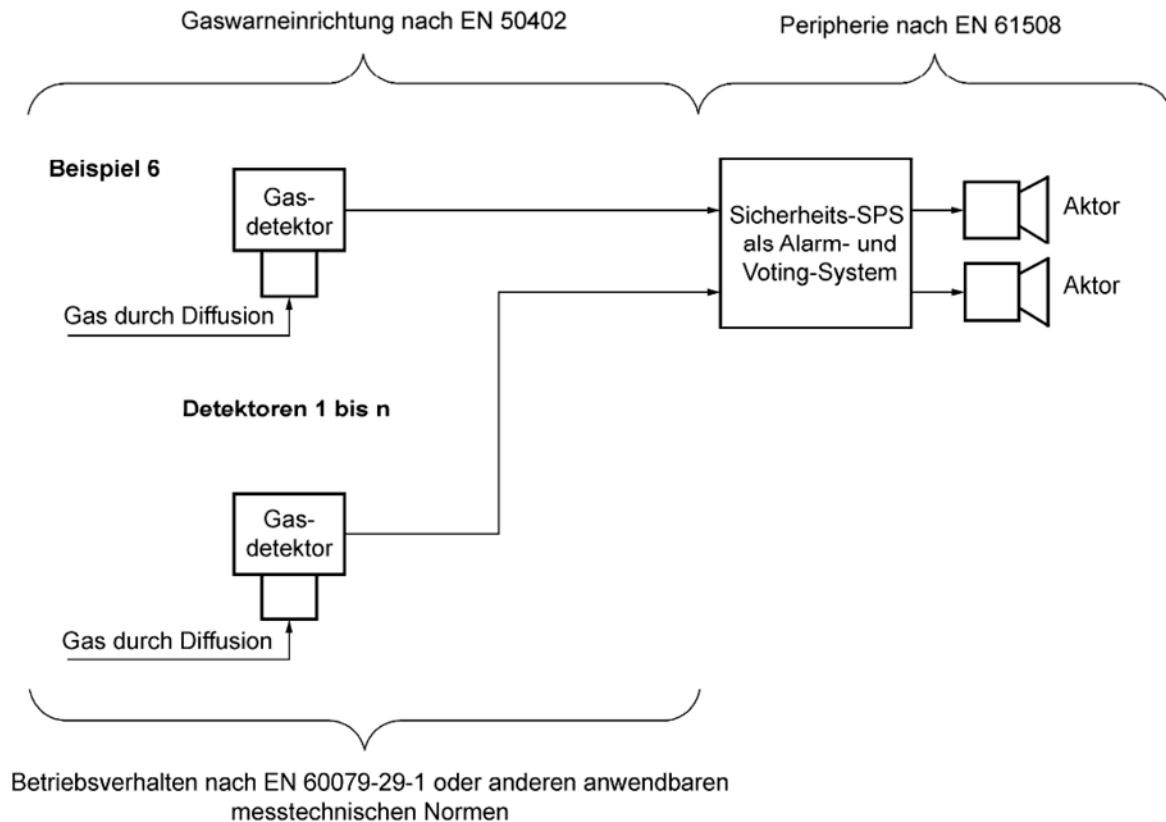


Bild 2f — Gaswarnsystem plus Aktor für Sicherheitsfunktion

Im Beispiel 6 in Bild 2f enthält der Gasdetektor auch die funktionalen Module der Gaswarn-Steuereinheit zur Erzeugung von Alarmen und Ausgangssignalen zur Ansteuerung von Aktoren. Der Gasdetektor arbeitet als komplettes Gaswarnsystem im Anwendungsbereich der EN 50402 und der messtechnischen Normen. Es gibt keine eins zu eins Beziehung zwischen Alarmausgang und Aktor. Es wird vorausgesetzt, dass die SPS keinen negativen Einfluss auf den sicherheitsbezogenen Ausgang des Gasdetektors haben kann.

Die Schaltausgänge einer Anzahl von Gasdetektoren sind sicherheitsbezogene Alarmeingänge in die Sicherheits-SPS, die hier als Lüftungssteuerungssystem arbeitet. Sie korreliert ihre Alarmeingänge mit den zugehörigen Aktoren (z. B. durch ein Voting). Die Sicherheits-SPS und die Aktoren gehören zum Anwendungsbereich der EN 61508 (alle Teile).

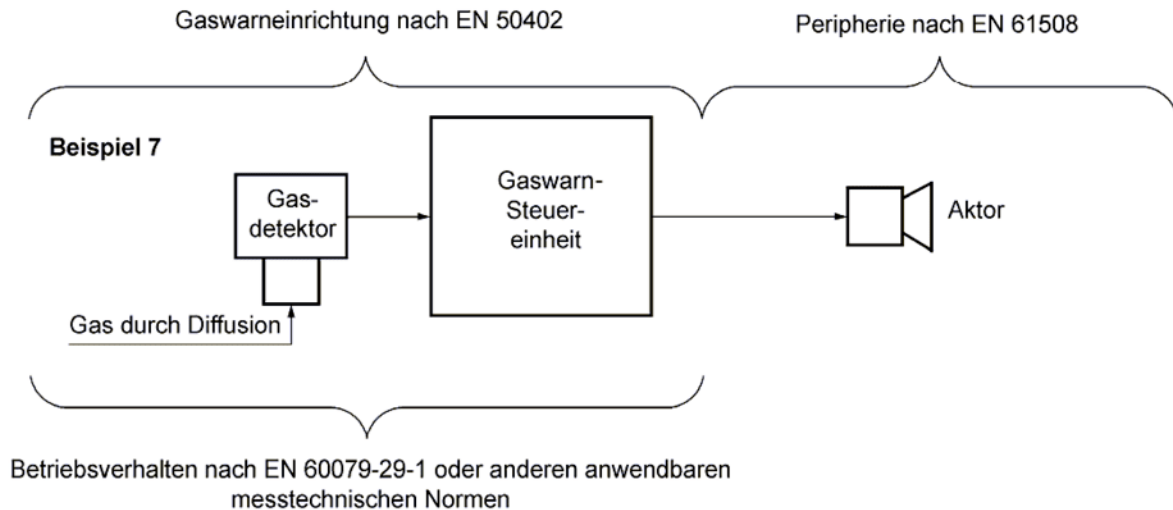


Bild 2g – Gaswarnsystem plus Aktor für Sicherheitsfunktion

Bild 2 – Beispiele für die gesamte Sicherheitsfunktion von Gaswarnsystemen

Im Beispiel 7 in Bild 2g ist der Gasdetektor ein an eine Gaswarn-Steuereinheit angeschlossener externer Sensor.

Externer Sensor und Gaswarn-Steuereinheit einschließlich des Schaltausgangs gehören zum Anwendungsbereich der anwendbaren messtechnischen Norm sowie der EN 50402.

Der vom Schaltausgang des Gaswarnsystems angesteuerte Aktor gehört zum Anwendungsbereich der EN 61508 (alle Teile).

4.2 Bestimmung der Sicherheitsfunktion

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

Die SIL-Fähigkeit eines Moduls wird durch die Maßnahmen und Techniken zur Fehlervermeidung und Fehlerbeherrschung sowohl bei 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.

Diese Europäische Norm fordert außerdem eine Bestimmung der Hardwareausfallraten für jede Sicherheitsfunktion nach Aufteilung eines Gaswarnsystems in physikalische Komponenten, die abweichend von den funktionalen Modulen sein kann.

Anwender sollten in der Lage sein, das Betriebsverhalten einer Sicherheitsfunktion eines übergeordneten sicherheitsbezogenen Systems, das ein Gaswarnsystem enthält, in Begriffen von Sicherheits-Integritätsleveln (SIL) nach EN 61508 (alle Teile) 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 [Abschnitt 9](#)).

Die SIL-Fähigkeit und Hardwareausfallraten einer Sicherheitsfunktion eines Gaswarnsystems können aus der SIL-Fähigkeit der funktionalen Module und Hardwareausfallraten der Komponenten ermittelt werden (siehe [Abschnitt 7](#) und [Anhang C](#)).

Die Software aller Module, die Bestandteil der Sicherheitsfunktion sind, muss in einem Prozess nach der SIL-Fähigkeit entwickelt werden, die von der Sicherheitsfunktion erreicht werden soll. Falls redundante Hardware eingesetzt wird, um eine höhere SIL-Fähigkeit zu erreichen, muss die Software die höhere SIL-Fähigkeit erfüllen (siehe [Bild 6](#)) oder es muss nachgewiesen werden, dass die Software der redundanten Ketten diversitär ist (siehe [EN 61508-7:2010, C.3.5](#)).

Wenn ein Gaswarnsystem mehrere Sicherheitsfunktionen mit unterschiedlichen SIL-Fähigkeiten besitzt, gibt es zwei Möglichkeiten:

- a) die gesamte Software erfüllt die höhere SIL-Fähigkeit, oder
- b) es muss nachgewiesen werden, dass die Software mit der niedrigeren SIL-Fähigkeit die Sicherheitsfunktion der höheren SIL-Fähigkeit nicht beeinträchtigt.

Software von Modulen, die nicht Bestandteil der Sicherheitsfunktion sind, aber auf einem Mikroprozessor laufen, der Bestandteil der Sicherheitsfunktion ist, muss mindestens in einem SIL 1-konformen Prozess entwickelt werden. Wenn diese Software einem niedrigeren SIL entspricht als die Sicherheitsfunktion, muss nachgewiesen werden, dass diese Software die Sicherheitsfunktion der höheren SIL-Fähigkeit nicht beeinträchtigt.

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

ANMERKUNG 2 Unterschiedliche Kombinationen von Modulen können zu einer unterschiedlichen SIL-Fähigkeit für die ausgewählte Sicherheitsfunktion führen.

ANMERKUNG 3 Eine separate Gaswarn-Steuereinheit mit einer bestimmten SIL-Fähigkeit von X kann mit einem oder mehreren Messorten verbunden sein, die unterschiedliche SIL-Fähigkeiten besitzen (von X oder geringer), abhängig von ihren angeschlossenen Transmittern und Schaltausgängen. Es ist daher möglich, dass das gesamte Gaswarnsystem (bestehend aus der Steuereinheit und mehreren Messorten) für verschiedene Sicherheitsfunktionen mehrere unterschiedliche SIL-Fähigkeiten (von X oder geringer) realisieren kann.

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 C](#)).

Die Feststellung, ob eine bestimmte Sicherheitsfunktion eines Gaswarnsystems in Verbindung mit anderen Einrichtungen eine festgelegte Sicherheitsintegrität erfüllt, erfordert auch die Einbeziehung der Eigenschaften der funktionalen Sicherheit der anderen Anlagenteile (Peripherie), die für die funktionale Sicherheit benötigt werden. Geeignete Verfahren werden in [Abschnitt 9](#) beschrieben.

Wenn die SIL-Fähigkeit eines Moduls und die Hardware-Fehlerraten einer Komponente einmal bestimmt worden sind, können das Modul bzw. die Komponente in verschiedenen Systemkonfigurationen eingesetzt werden ohne die Notwendigkeit, die SIL-Fähigkeit und Hardwarefehlerrate erneut zu bestimmen.

Die Bestimmung der SIL-Fähigkeit und der Hardwareausfallrate für eine spezifische Sicherheitsfunktion eines Gaswarnsystems muss für jede neue Kombination von Modulen und zugehörigen Komponenten wiederholt werden. Der Einfluss aller zum Gaswarnsystem gehörenden Module und Komponenten muss berücksichtigt werden. Module, die nicht Bestandteil der Sicherheitsfunktion sind, dürfen keinen negativen Einfluss auf die Sicherheitsfunktion haben.

Diese Europäische Norm legt Anforderungen an Maßnahmen fest, die ausgeführt werden, wenn Ausfälle in den Modulen erkannt werden. Das Gaswarnsystem muss einen vorbestimmten Zustand einnehmen, nachdem Ausfälle erkannt wurden. Wenn die Sicherheitsfunktion durch den erkannten Ausfall verloren gegangen ist, muss der zugehörige Teil des Systems in einen Sonderzustand übergehen. Wenn die Sicherheitsfunktion noch verfügbar ist (sicherer erkannter Ausfall), wird empfohlen, dass eine Wartungsanforderung angezeigt wird (siehe [5.6.6](#)). Die Reaktion auf solch eine Anzeige und die notwendige Reparaturmaßnahme müssen in der Betriebsanleitung beschrieben 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.

Sind Mittel zur Steigerung der Verfügbarkeit vorhanden (z. B. zusätzliche Hard- oder Software), müssen diese Funktionen als Bestandteil der zugehörigen Sicherheitsfunktion berücksichtigt werden und müssen derselben SIL-Fähigkeit entsprechen.

4.3 Merkmale der funktionalen Sicherheit von Modulen

Diese Europäische Norm legt Module und spezifische Anforderungen für jede SIL-Fähigkeit (benannt mit 1, 2 und 3) fest. SIL-Fähigkeiten höher als 1 schließen die Anforderungen der niedrigeren SIL-Fähigkeiten ein, es sei denn, es ist etwas anderes festgelegt.

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

Bei einigen Modulen bestimmt ihre technische Ausführung und ihre Implementierung, ob sie einfach oder komplex sind.

Auf Analogtechnik basierende Module werden als einfach vorausgesetzt. Alle anderen Module sind als komplex zu behandeln. Die Fehlertoleranz für alle einfachen Module muss der Tabelle 1 entsprechen. Die Fehlertoleranz für alle komplexen Module muss der Tabelle 2 entsprechen.

Tabelle 1 – Fehlertoleranz für einfache Module nach EN 61508-2:2010, Tabelle 2

SIL-Fähigkeit	Minimale Hardware-Fehlertoleranz (siehe EN 61508-2:2010, 7.4.4.2.2)		
	Anteil ungefährlicher Ausfälle (<i>SFF</i>) 60 % bis < 90 %	Anteil ungefährlicher Ausfälle (<i>SFF</i>) 90 % bis < 99 %	Anteil ungefährlicher Ausfälle (<i>SFF</i>) ≥ 99 %
1	0	0	0
2	0	0	0
3	1	0	0

Tabelle 2 – Fehlertoleranz für komplexe Module nach EN 61508-2:2010, Tabelle 3

SIL-Fähigkeit	Minimale Hardware-Fehlertoleranz (siehe EN 61508-2:2010, 7.4.4.2.2)		
	Anteil ungefährlicher Ausfälle (<i>SFF</i>) 60 % bis < 90 %	Anteil ungefährlicher Ausfälle (<i>SFF</i>) 90 % bis < 99 %	Anteil ungefährlicher Ausfälle (<i>SFF</i>) ≥ 99 %
1	0	0	0
2	1	0	0
3	2 (nicht anwendbar für Gaswarntechnik)	1	0

Die spezifischen Anforderungen in [Abschnitt 5](#) sind aus den allgemeinen Anforderungen in EN 61508-2:2010 und zusätzlich aus speziellen Anforderungen für Gaswarnsysteme abgeleitet.

Die Anforderungen der messtechnischen Normen sind hinreichend, um eine *SFF* von mindestens 60 % sicherzustellen. Deshalb berücksichtigt diese Europäische Norm keine technische Lösung mit einer *SFF* unterhalb von 60 %.

Für einfache Module stellen die in [Abschnitt 5](#) festgelegten spezifischen Anforderungen sicher, dass eine *SFF* von 60 % bis 90 % erreicht wird.

Für komplexe Module stellen die in [Abschnitt 5](#) festgelegten spezifischen Anforderungen für Hardware-Fehler-Toleranzen 0 und 1 sicher, dass die geforderte *SFF* erreicht wird. Architekturen mit Hardware-Fehler-Toleranz 2 (en: hardware fault tolerance, HFT) werden in [Abschnitt 5](#) nicht beschrieben, weil sie in der Gaswarntechnik nicht praktisch anwendbar sind.