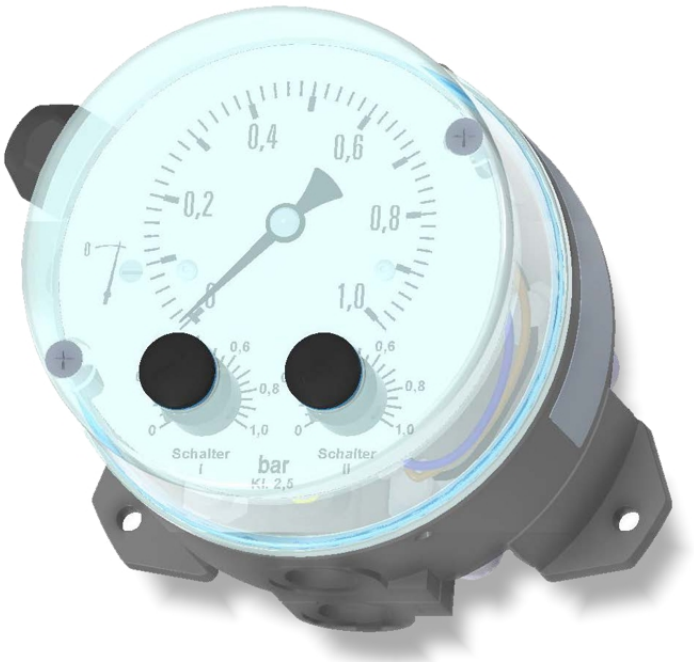
developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL



Sicherheitshandbuch

DS11

Differenzdruck Mess- und Schaltgerät

09015242 • SHB_DE_DS11 • Rev. ST4-E • 06/26

Inhaltsverzeichnis

1 Geltungsbereich und Standards 3
2 Gerätebeschreibung und Einsatzbereich 4
2.1 Aufbau und Wirkungsweise 4
2.2 Funktionsbild 4
2.3 Sicherer Zustand 4
3 Hinweise zur Projektierung 5
3.1 Bestimmungsgemäßer Gebrauch 5
3.2 Betriebsart 5
3.3 Gerätetyp 5
3.4 Prüfintervall 5
3.5 Gebrauchsdauer 5
3.6 Montage und Installation 6
4 Wiederkehrende Prüfungen 7
4.1 Wartung 7
4.2 Funktionsprüfung 7
4.3 Reparatur 8
5 Sicherheitstechnische Kenngrößen 9
6 Anhang 10
6.1 SIL Zertifikat 10
6.2 Glossar 12
6.3 Fehlerraten 16
6.4 Gerätetypen 17

1 Geltungsbereich und Standards

HINWEIS

Sicherheitshinweise

Dieses Sicherheitshandbuch ist nur in Verbindung mit der Betriebsanleitung des betreffenden Gerätes zu benutzen. Beachten Sie die Sicherheitshinweise der Betriebsanleitung.

Das Sicherheitshandbuch gilt für alle Ausführungen des Differenzdruck Mess- und Schaltgerät DS11.

Das DS11 wurde vom TÜV NORD CERT GmbH, Prüflabor Produktsicherheit entsprechend folgender Norm geprüft und ein Zertifikat mit der Nummer 44 7999 13759902 ausgestellt.

IEC 61508: 2010
Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer/programmierbarer elektronischer Systeme

Teile 1 bis 7

2 Gerätebeschreibung und Einsatzbereich

2.1 Aufbau und Wirkungsweise

Als Messsystem wird ein robustes und unempfindliches Membranmesswerk verwendet, dass sich gleichermaßen für Differenzdruck, Über- und Unterdruck-Messungen eignet. In allen drei Messanwendungen arbeitet das Gerät nach dem gleichen Messprinzip.

In Ruhelage sind die Federkräfte beiderseits der Membrane ausgeglichen. Durch den zu messenden Druck entsteht an der Membrane eine einseitige Kraft, die das Membransystem bis zum Ausgleich der Federkräfte gegen die Messbereichsfedern verschiebt. Bei Überlastung stützt sich die Membrane gegen metallische Anlageflächen ab.

Ein zentrisch angeordneter Stößel überträgt die Bewegung des Membransystems auf das Zeigerwerk und die Betätigungselemente der Mikroschalter.

2.2 Funktionsbild

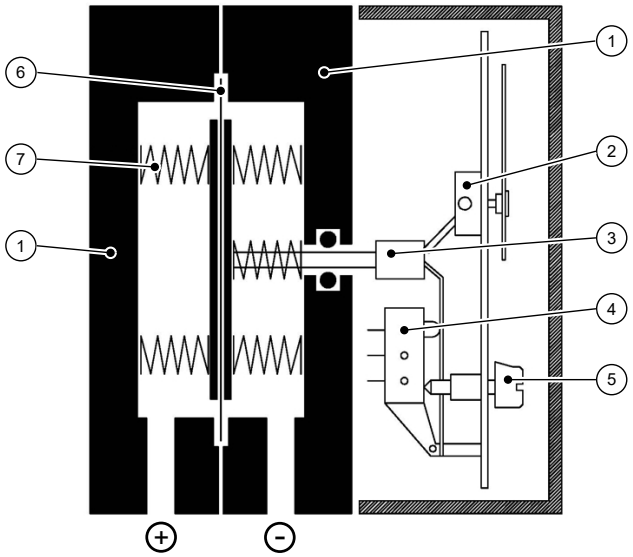


Abb. 1: Funktionsbild

1	Druck-Kammer	**2**	Zeigerwerk
3	Stößel	**4**	Mikroschalter
5	Schaltpunkteinstellung	**6**	Messmembran
7	Messfedern		

2.3 Sicherer Zustand

Die sichere Funktion des Kontaktmanometers ist die Funktion der beiden Schaltkontakte und der Anzeige innerhalb des im Datenblatt angegeben Toleranzbereichs.

3 Hinweise zur Projektierung

3.1 Bestimmungsgemäßer Gebrauch

Das DS11 wurde vom TÜV NORD CERT GmbH auf der Basis ‚betriebsbewährte Komponente' geprüft. Die Geräte können mit einer geeigneten Testung (Proof Test) in SIL2 Anwendungen eingesetzt werden.

HINWEIS

SIL2 wird mit einem Kontakt erreicht.

3.2 Betriebsart

High Demand Mode

3.3 Gerätetyp

Das Gerät ist vom Typ-A (einfaches Betriebsmittel).

3.4 Prüfintervall

Ein Proof-Test ist nach Inbetriebnahme und danach spätestens nach Ablauf von 1 Jahr durchzuführen.

3.5 Gebrauchsdauer

Das DS11 hat eine Gebrauchsdauer von 15 Jahren bei einer Begrenzung auf maximal 250 000 Schaltspiele.

3.6 Montage und Installation

Beachten Sie die Montageanleitung der Betriebsanleitung.

Die Sicherheitskennzahlen wurden anhand von FMEAs ermittelt. Diese gelten unter der Bedingung, dass die Ausgangsignale von einer nachgeschalteten Steuerung überwacht und ausgewertet werden.

HINWEIS

SIL2 Anwendung

SIL2 wird bereits durch die Verwendung eines Wechselkontaktes erreicht. Der zweite Kontakt kann für eine andere Funktion verwendet werden.

Für die nachfolgenden Anschlussbilder gilt die folgende Legende:

Legende

i_m	Verbindungsmittel
c	Kreuzvergleich
S	Wechselkontakt
L1, L2	Logik
m	Überwachung
O1, O2	Ausgabeeinheiten
SF	Sicherheitsfunktion

3.6.1 Architektur 1001 (HFT=0)

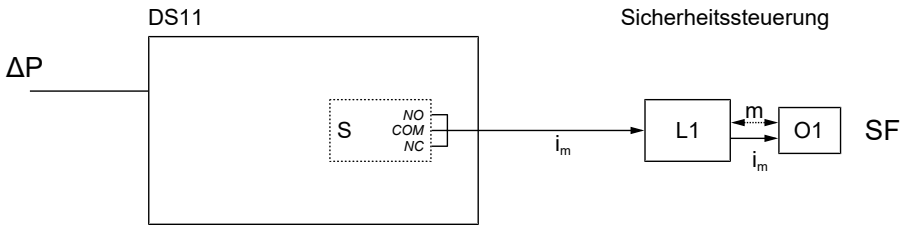


Abb. 2: Architektur 1001

3.6.2 Architektur 1002 (HFT=1)

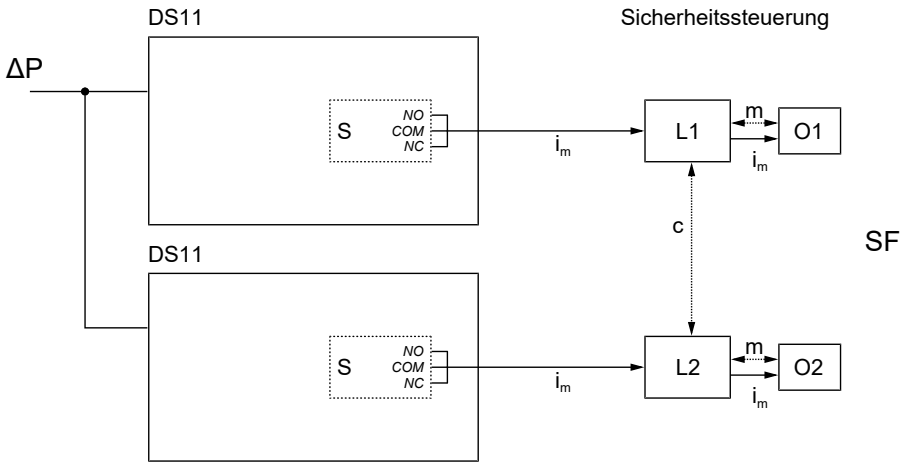


Abb. 3: Architektur 1002

4 Wiederkehrende Prüfungen

4.1 Wartung

Um einen gefährlichen unentdeckten Ausfall aufzudecken sind Proof-Tests ein notwendiger Bestandteil des Sicherheitskonzeptes. Bei einem Proof-Test werden folgende Aspekte einer sicherheitskritischen Komponente überprüft:

- Funktionalität
- erfüllt die Komponente die vorherrschenden Einsatzbedingungen
- sind die Schnittstellen zu weiteren Komponenten in Ordnung

Alle kritischen Teile müssen mit dem Proof-Test getestet werden. Für Nichtsicherheitskritische Teile genügt hingegen ein stichprobenartiger Test.

4.2 Funktionsprüfung

HINWEIS

Anzeigewert

Gem. DIN 837 ist ein leichtes Klopfen auf das Gerät zum ‚Einstellen' des Anzeigewertes zugelassen.

Folgende Funktionen sind für das DS11 zu prüfen:

1. Prüfung der Schaltpunkte im drucklosen Zustand
2. Prüfung der Schaltpunkte durch Änderung des Betriebsdrucks.

Die Funktionsprüfung sollte möglichst mit dem Sicherheitstechnischen System (SIS) durchgeführt werden. Andernfalls muss das DS11 ausgebaut und mit einem Druckkalibrator verschaltet werden. Werden die angegebenen Grenzwerte überschritten, so darf das betreffende Gerät nicht wieder in Betrieb genommen werden und muss durch ein neues Gerät ersetzt werden.

Prüfschaltung

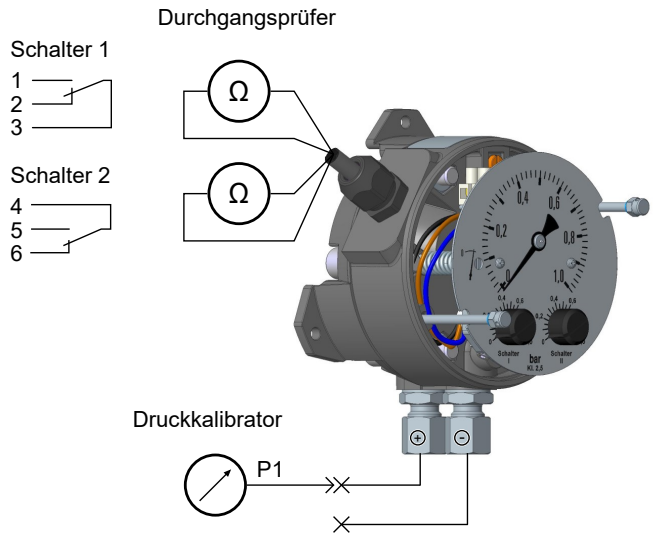


Abb. 4: Funktionstest

Prüffolge

- Öffnen Sie das Gerät, indem Sie (abhängig von der Ausführung) entweder die Haube oder den Bajonettring der Frontscheibe entfernen.
- Prüfung im drucklosen Zustand
  - Drehen Sie den Schalter 1 in Richtung Nullpunkt bis der Mikroschalter schaltet. Prüfen Sie den Zustand des Schaltausgangs mit einem Durchgangsprüfer.
  - Drehen Sie den Schalter 2 in Richtung Nullpunkt bis der Mikroschalter schaltet. Prüfen Sie den Zustand des Schaltausgangs mit einem Durchgangsprüfer.
- Prüfung der Messgenauigkeit (±2,5% vom Messbereichsendwert)
  - Stellen Sie am Druckkalibrator einen Differenzdruck ein, der dem Messbereichsanfang entspricht. Prüfen Sie den Anzeigewert.
  - Stellen Sie am Druckkalibrator einen Differenzdruck ein, der dem Messbereichende entspricht. Prüfen Sie den Anzeigewert.
  - Stellen Sie am Druckkalibrator einen Differenzdruck ein, der der Mitte des Messbereichs entspricht. Prüfen Sie den Anzeigewert.
- Prüfung durch Änderung des Betriebsdrucks
  - Stellen Sie mit den Schaltern 1 und 2 die Schaltpunkte ein.
  - Erhöhen Sie nun den Differenzdruck mit dem Druckkalibrator bis der erste Schaltpunkt erreicht ist und Überprüfen Sie den Zustand des Schaltausgangs mit einem Durchgangsprüfer. Notieren Sie den Druckwert bei dem der erste Schalter schaltet.
  - Erhöhen Sie nun den Differenzdruck mit dem Druckkalibrator bis der zweite Schaltpunkt erreicht ist und Überprüfen Sie den Zustand des Schaltausgangs mit einem Durchgangsprüfer. Notieren Sie den Druckwert bei dem der zweite Schalter schaltet.
  - Verringern Sie nun den Differenzdruck und ermitteln Sie die Druckwerte, bei denen die Schalter abfallen. Notieren Sie die Werte und ermitteln Sie die Hysterese der Schaltpunkte. Diese darf den Grenzwert von 2,5% vom Messbereichsendwert nicht überschreiten.
- Schließen Sie das Gerät.

4.3 Reparatur

Die Reparatur eines Gerätes kann nur der Hersteller durchführen.

Alle defekten oder mit Mängeln behafteten Geräte sind direkt an unsere Reparaturabteilung zu senden. Wir bitten darum alle Geräterücksendungen mit unserer Verkaufsabteilung abzustimmen.

⚠ WARNUNG

Messstoffreste

Messstoffreste in und an ausgebauten Messgeräten können zur Gefährdung von Menschen, Umwelt und Einrichtungen führen. Ausreichende Vorsichtsmaßnahmen sind zu ergreifen. Gegebenenfalls sind die Geräte gründlich zu reinigen.

Zur Rücksendung des Gerätes die Originalverpackung oder eine geeignete Transportverpackung verwenden.

5 Sicherheitstechnische Kenngrößen

Die Geräte können mit einer geeigneten Testung in SIL2 Anwendungen eingesetzt werden. SIL2 wird mit einem Kontakt erreicht.

Safe Failure Fraction	**SFF**	70 %
Probability of dangerous Failure per Hour	**PFH**	$3{,}3 * 10^{-11}$ 1/h
Hardware Fault Tolerance	**HFT**	0
Gerätetyp		Typ-A Teilsystem
Prüfintervall	$\mathbf{T_1}$	1 Jahr

Verwendung im Low Demand Mode

In Übereinstimmung mit der Norm EN 61508 kann der PFD Wert wie folgt bestimmt werden. Der berechnete Wert gilt für ein einzelnes Gerät.

$$\lambda_{du} = PFH$$
$$T_1 = 1\ Jahr = 365 * 24\ h$$

$$PFD = \lambda_{du} * \frac{T_1}{2}$$
$$= 33 * 10^{-11} [\frac{1}{h}] * \frac{365 * 24\ [\ h\ ]}{2}$$
$$= 1{,}45 * 10^{-7}$$

Abb. 5: Berechnung des PFD Wertes

6 Anhang

6.1 SIL Zertifikat

TÜVNORD

ZERTIFIKAT
CERTIFICATE

Hiermit wird bescheinigt, dass das unten beschriebene Produkt der Firma
This certifies that the product mentioned below from company

Fischer Mess- und Regeltechnik
Bielefelder Straße 37a
32107 Bad Salzuflen
Deutschland

die Anforderungen der folgenden Prüfunterlage(n) erfüllt.
fulfills the requirements of the following test regulations.

Geprüft nach: *Tested in accordance with:*	**EN 61508:2010 Teile/Parts 1-7**
Zertifizierungsprogramm: *Certification program:*	**P14.1VA001**
Beschreibung des Produktes: (Details s. Anlage 1) *Description of product:* *(Details see Annex 1)*	**Differenzdruck Mess- und Schaltgerät** / *Differental Presure Switch* **Kontaktmanometer** / *Contact Pressure Gauge*
Typenbezeichnung: *Type Designation:*	**DS11, DS13 und DS21** **MS11**
Bemerkungen: *Remarks:*	**Die Geräte können mit einer geeigneten Testung in SIL2 Anwendungen eingesetzt werden.** *The components can be used with an appropriate testing in SIL2 applications.*

Dieses Zertifikat bescheinigt das Ergebnis der Prüfung an dem vorgestellten Prüfgegenstand. Eine allgemein gültige Aussage über die Qualität der Produkte aus der laufenden Fertigung kann hieraus nicht abgeleitet werden.

Registrier-Nr. / *Registered No.* 44 799 13759902
Prüfbericht Nr. / *Test Report No.* 35392078
Aktenzeichen / *File reference* 8003081893

Gültigkeit / Validity
von / *from* 2025-03-24
bis / *until* 2030-03-23

F. Hegenfeld

Zertifizierungsstelle der
TÜV NORD CERT GmbH

Essen, 2025-03-24

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de machinery@tuev-nord.de

Bitte beachten Sie auch die umseitigen Hinweise
Please also pay attention to the information stated overleaf

Abb. 6: 4479913759902_SIL_2030-03-23_Seite_1

TÜVNORD

ANLAGE
ANNEX

Anlage 1, Seite 1 von 1
Annex 1, page 1 of 1

zum Zertifikat Registrier-Nr. / *to Certificate Registration No.* 44 799 13759902

Produktbeschreibung: *Product description:*	**Differnzdruck Mess- und Schaltgerät** / *Differental Presure Switch* **Kontaktmonometer** / *Contact Pressure Gauge*
Typenbezeichnung: *Type designation:*	**DS11, DS13 und DS21** **MS11**
Technische Daten: *Technical data:*	**Sicherheitsparameter** / *Safety Parameter* SFF = 70% PFH = 3,3 10^{-11} 1/h HFT = 0 Typ-A-Teilkomponente / *Type*

Zertifizierungsstelle der
TÜV NORD CERT GmbH

Essen, 2025-03-24

TÜV NORD CERT GmbH Am TÜV 1 45307 Essen www.tuev-nord-cert.de machinery@tuev-nord.de

Abb. 7: 4479913759902_SIL_2030-03-23_Seite_2

6.2 Glossar

Abk. (A-Z)	Definition
β	*(en)* **Common Cause Factor** *(de)* Beta-Faktor Proportionalitätsfaktor zwischen der CCF-Rate (Ausfalls infolge gemeinsamer Ursache) und der gefährlichen Ausfallrate des einzelnen Kanals.
DC	*(en)* **Diagnostic Coverage Factor** *(de)* Diagnosedeckungsgrad Der DC Parameter gibt das Verhältnis der Anzahl aller entdeckbaren gefährlichen Fehler (λ_{DD}) zur gesamten Anzahl der gefährlichen Fehler (λ_D) an. $DC = \frac{\sum \text{erkannter gefährlicher Fehler}}{\sum \text{gesamter gefährlicher Fehler}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
FIT	*(en)* **Failure in Time** *(de)* Ausfälle pro Zeit Ausfallrate bezogen auf das Zeitintervall 10^9 Stunden. $1\ FIT = 1 \times 10^{-9} \frac{1}{h}$
FMEDA	*(en)* **Failure Mode Effect and Diagnostic Analysis** *(de)* Gefährdung und Risikoanalyse Verfahren zur Ermittlung von Fehlerursachen und deren Auswirkung auf das System.
HDM	*(en)* **High Demand Mode** *(de)* Betriebsart mit hoher Anforderungsstufe Betriebsart mit hoher oder kontinuierlicher Anforderung der Sicherheitsfunktion. Die Anforderungsrate an das sicherheitsbezogene System beträgt mehr als einmal pro Jahr.
HFT	*(en)* **Hardware Fault Tolerance** *(de)* Hardware-Fehlertoleranz Die Hardware-Fehlertoleranz gibt an, wie viele gefährliche Fehler aufgrund der Architektur möglich sind, ohne dass die Ausführung der Sicherheitsfunktion gefährdet ist. • HFT = 0 Der Eintritt eines gefährlichen Fehlers führt bereits zum Ausfall der Sicherheitsfunktion. • HFT = 1 Erst der Eintritt von zwei gefährlichen Fehlern führt zum Ausfall der Sicherheitsfunktion.

LDM	*(en)* **Low Demand Mode** *(de)* Betriebsart mit niedriger Anforderungsstufe
	Die Sicherheitsfunktion wird nur auf Anforderung ausgeführt, um das System in einen festgelegten sicheren Zustand zu überführen. Die Häufigkeit von Anforderungen beträgt nicht mehr als einmal pro Jahr.
MooN	*(en)* **Architecture with M out of N channels** *(de)* Systemarchitektur mit M aus N Kanälen
	Systemarchitektur MooN mit den Variablen M und N: Klassifizierung und Beschreibung des sicherheitsbezogenen Systems hinsichtlich der Redundanz und den angewandten Auswahlverfahren. • N - gibt die gesamte Anzahl der redundanten Kanäle einer sicherheitsbezogenen Architektur bzw. eines Sicherheitskreises an. • M – bestimmt, wie viele Kanäle korrekt arbeiten müssen, um die Sicherheitsfunktion auszuführen.
MTBF	*(en)* **Mean Time Between Failures** *(de)* Mittlere Brauchbarkeitsdauer
	Mittlere Betriebsdauer zwischen zwei Ausfällen.
$MTTF_d$	*(en)* **Mean Time To Dangerous Failures** *(de)* Mittlere Zeit bis zum gefahrbringenden Ausfall
	Betriebsdauer bis zu einem gefahrbringenden Fehler.
MRT	*(en)* **Mean Repair Time** *(de)* Mittlere Reparaturdauer
	Mittlere Zeitdauer für die Reparatur.
MTTR	*(en)* **Mean Time To Repair** *(de)* Mittlere Instandsetzungszeit
	Mittlere Zeitdauer zwischen dem Auftreten eines Fehlers und der Widerherstellung des Systems.
PFD	*(en)* **Probability of Failure on Demand** *(de)* Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall
	Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion für eine Betriebsart mit niedriger Anforderungsrate (Low Demand).
PFH	*(en)* **Probability of a dangerous Failure per Hour** *(de)* Ausfallwahrscheinlichkeit pro Stunde für die Sicherheitsfunktion
	Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion für eine Betriebsart mit hoher oder kontinuierlicher Anforderungsrate (High Demand).

PFS	*(en)* **Probability of Failure Spurious** *(de)* Ausfallwahrscheinlichkeit aufgrund einer nicht beabsichtigten Prozessabschaltung Häufigkeit eines Ausfalls aufgrund eines Fehlalarms, der zu einer nicht beabsichtigten Prozessabschaltung durch das sicherheitstechnische-System führt. Je kleiner der Wert ist umso verfügbarer ist das System.
SC	*(en)* **systematic capability** *(de)* systematische Eignung Maß des Vertrauens (ausgedrückt auf einer Skala von SC 1 bis SC 4), dass die systematische Sicherheitsintegrität eines Elements den Anforderungen des festgelegten SILs hinsichtlich der festgelegten Element-Sicherheitsfunktion entspricht, wenn das Element in Übereinstimmung mit dem Sicherheitshandbuch für konforme Objekte für das Element festgelegten Anweisungen angewendet wird.
SFF	*(en)* **Safe Failure Fraction** *(de)* Anteil der ungefährlichen Ausfälle Ergibt sich aus der Rate der ungefährlichen Fehler plus der diagnostizierten bzw. erkannten Fehler im Verhältnis zur gesamten Ausfallrate des Systems.[(1)]
SIF	*(en)* **Safety Instrumented Function** *(de)* Sicherheitstechnische Funktion Die Sicherheitsfunktion (SIF) ist eine Schutzmaßnahme, die nur im Störfall aktiviert wird und dann verhindert, dass Personen, Umwelt und Sachwerte Schaden nehmen.
SIL	*(en)* **Safety Integrity Level** *(de)* Sicherheits-Integritätslevel Eine von vier diskreten Stufen, um die Anforderungen an die Zuverlässigkeit der Sicherheitsfunktionen in Sicherheitstechnischen-Systemen zu beurteilen. SIL 4 bezeichnet die höchste und SIL1 die niedrigste Stufe der Sicherheitsintegrität. Jeder Level entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion.
SIS	*(en)* **Safety Instrumented System** *(de)* Sicherheitstechnisches-System Sicherheitstechnisches-System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein solches System besteht mindestens aus einem Sensor, einer übergeordneten Sicherheitssteuerung und einem Aktor.
T_1	*(en)* **Proof Test Interval** *(de)* Prüfintervall Das Sicherheitstechnische-System muss sich stets in einem Zustand befinden, der die festgelegte Sicherheits-Integrität garantiert. Der Proof-Test ist die durchzuführende Prüfung, die dies bestätigt. Das Prüfintervall gibt an in welchen Zeitabständen ein Proof-Test durchzuführen ist, um die Sicherheitsfunktion zu garantieren.

[(1)] Aufgrund der fehlenden Diagnose und den vernachlässigbar wenigen Fehlern bei mechanischen Komponenten ist die Methode bei Ventilen, Antrieben und anderen mechanischen Komponenten nur bedingt anwendbar. Es obliegt daher dem Endanwender durch geeignete Diagnosemaßnahmen und eigensichere Konstruktion eine entsprechende SFF sicherzustellen.

6.3 Fehlerraten

Die Fehlerraten unterscheiden sich grundsätzlich wie folgt:

1. sichere Fehler
2. gefährliche Fehler
3. Fehler ohne Auswirkung

Die ersten beiden Fehlertypen werden nochmals unterschieden in entdeckbare und unentdeckbare Fehler.

Die Fehler ohne Auswirkung und die sicheren Fehler, egal ob entdeckt oder unentdeckt, haben auf die Sicherheitsfunktion keinen Einfluss. Gefährliche Fehler führen hingegen zu einem gefährlichen Zustand des Systems. Eine Übersicht gibt das nachfolgende Diagramm.

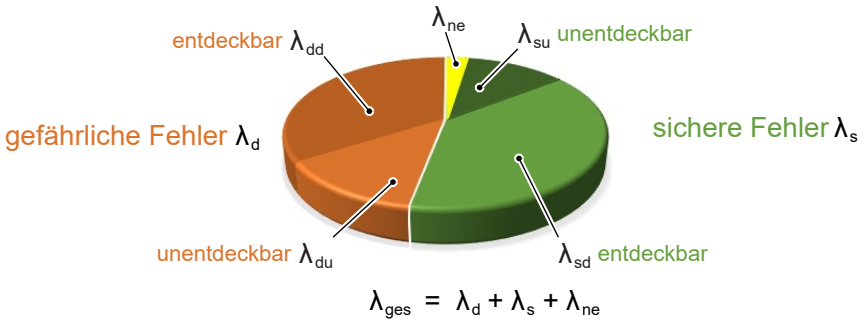


Abb. 8: Fehlerraten

λ_d *(en)* **Dangerous failure rate**
(de) Rate aller gefährlichen Fehler

λ_{dd} *(en)* **Dangerous detected failure rate**
(de) Rate aller entdeckbaren gefährlichen Fehler

λ_{du} *(en)* **Dangerous undetected failure rate**
(de) Rate aller unentdeckbaren gefährlichen Fehler

λ_s *(en)* **Safe failure rate**
(de) Rate aller ungefährlichen Fehler

λ_{sd} *(en)* **Safe detected failure rate**
(de) Rate aller entdeckbaren sicheren Fehler

λ_{su} *(en)* **Safe undetected failure rate**
(de) Rate aller unentdeckbaren sicheren Fehler

λ_{ne} *(en)* **No effect failure rate**
(de) Rate aller Fehler ohne Auswirkung

6.4 Gerätetypen

Typ-A **Einfaches Betriebsmittel**

Typ A Geräte sind „einfache“ Geräte bei denen das Ausfallverhalten aller eingesetzten Bauteile und das Verhalten unter Fehlerbedingungen vollständig bekannt ist.

Sie enthalten z.B. Relais, Widerstände und Transistoren, jedoch keine komplexen elektronischen Bauelemente wie z.B. Mikrocontroller.

Typ-B **Komplexes Betriebsmittel**

Typ B Geräte sind „komplexe“ Geräte bei denen das Ausfallverhalten der eingesetzten Bauteile und das Verhalten unter Fehlbedingungen nicht vollständig bekannt ist.

Diese Geräte enthalten elektronische Bauelemente wie Mikrocontroller, Mikroprozessoren oder ASICs. Bei diesen Bauelementen und insbesondere bei softwaregesteuerten Funktionen ist es schwierig, alle Fehler vollständig zu bestimmen.

Notizen

Notizen

FISCHER Mess- und Regeltechnik GmbH
Bielefelder Str. 37a
D-32107 Bad Salzuflen
Tel. +49 5222 974-0
www.fischermesstechnik.de
info@fischermesstechnik.de

Technische Änderungen vorbehalten. Subject to technical changes. Sous réserve de modifications techniques.