



IEC 61508  
**SIL2**  
ISO 13849  
**PLd**



Ex II 1/2G Ex ia IIC T4 Ga/Gb  
Ex II 2D Ex ia IIIC T80°C Db



**RoHS II**  
COMPLIANT

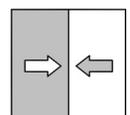


## Sicherheitshandbuch

**DE49 ## 0**

Digitaler Differenzdrucktransmitter

für explosionsgefährdete Bereiche  
Staub Explosionsschutz Zone 21 und 22, trockene Stäube  
Gas Explosionsschutz Zone 1 und 2, Gase und Dämpfe



## Impressum

**Hersteller:****FISCHER Mess- und Regeltechnik GmbH**Bielefelderstr. 37a  
D-32107 Bad Salzuflen

Telefon: +49 5222 974 0

Telefax: +49 5222 7170

eMail: [info@fischermesstechnik.de](mailto:info@fischermesstechnik.de)web: [www.fischermesstechnik.de](http://www.fischermesstechnik.de)**Technische Redaktion:**

Dokumentationsbeauftragter: T. Malischewski

Technischer Redakteur: R. Kleemann

Alle Rechte, auch die der Übersetzung, vorbehalten. Kein Teil dieses Dokuments darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung der Fa. FISCHER Mess- und Regeltechnik GmbH, Bad Salzuflen, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Eine Reproduktion zu innerbetrieblichen Zwecken ist ausdrücklich gestattet.

Markennamen und Verfahren werden nur zu Informationszwecken ohne Rücksicht auf die jeweilige Patentlage verwendet. Bei der Zusammenstellung der Texte und Abbildungen wurde mit größter Sorgfalt verfahren. Trotzdem können fehlerhafte Angaben nicht ausgeschlossen werden. Die Fa. FISCHER Mess- und Regeltechnik GmbH kann dafür weder die juristische Verantwortung noch irgendeine Haftung übernehmen.

Technische Änderungen sind vorbehalten.

© FISCHER Mess- und Regeltechnik 2020

### Versionsgeschichte

Rev. ST4-A 03/19	Version 1 (Erstausgabe)
Rev. ST4-B 03/20	Version 2 (Erweiterung SIL, neue FMEAs) ab Firmware 2.01d

# Inhaltsverzeichnis

<b>1 Geltungsbereich und Standards .....</b>	<b>4</b>
<b>2 Gerätebeschreibung und Einsatzbereich .....</b>	<b>5</b>
2.1 Sicherheitsfunktion .....	5
2.2 Definition des sicheren Zustandes .....	5
2.3 Parametrierung.....	5
<b>3 Hinweise zur Projektierung.....</b>	<b>6</b>
3.1 Bestimmungsgemäßer Gebrauch.....	6
3.2 Funktionale Sicherheit (IEC 61508).....	6
3.2.1 Betriebsart.....	6
3.2.2 Prüfintervall .....	6
3.2.3 Gebrauchsdauer .....	6
3.2.4 Montage und Installation.....	6
3.3 Performance Level (EN ISO 13849-1).....	7
3.3.1 Betriebsart.....	7
3.3.2 Prüfintervall.....	7
3.3.3 Gebrauchsdauer .....	7
3.3.4 Montage und Installation.....	8
<b>4 Wiederkehrende Prüfungen.....</b>	<b>9</b>
4.1 Wartung .....	9
4.2 Funktionsprüfung.....	9
<b>5 Sicherheitstechnische Kenngrößen .....</b>	<b>11</b>
5.1 Sensortyp A.....	11
5.2 Sensortyp B .....	13
<b>6 Anhang .....</b>	<b>15</b>
6.1 Glossar .....	15
6.2 Fehlerraten .....	17
6.3 Gerätetypen.....	18
6.4 Symbolerklärung.....	19

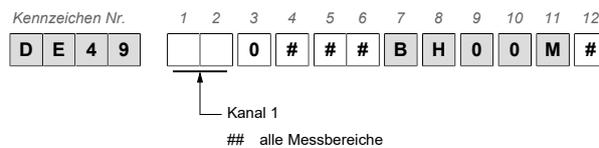
# 1 Geltungsbereich und Standards

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

Diese Dokumentation enthält Informationen und Sicherheitshinweise, die für den Einsatz des Differenzdrucktransmitters DE49 in sicherheitsbezogenen Systemen benötigt werden.

Sie richtet sich an Personen, die das Gerät montieren, parametrieren und in Betrieb nehmen, als auch an Projektentwickler und Betreiber.

Dieses Sicherheitshandbuch gilt für alle Ausführungen des Differenzdrucktransmitters DE49. Die Sicherheitskennzahlen sind abhängig vom verwendeten Sensorelement und werden für zwei Messbereichsgruppen (Sensor A [▶ 11] und Sensor B [▶ 13]) angegeben.



Die Sicherheitskennzahlen wurden anhand von FMEAs ermittelt. Diese gelten unter der Bedingung, dass das Ausgangssignal von einer nachgeschalteten Steuerung überwacht und ausgewertet wird.



Abb. 1: Verarbeitungskette

Der Differenzdrucktransmitter verfügt über einen 4 ... 20 mA Analogausgang, der für die Sicherheitsfunktion verwendet werden kann.

Für die Berechnungen wurden die nachfolgenden Normen herangezogen.

Funktionale Sicherheit	<b>IEC 61508: 2010</b> Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer/programmierbarer elektronischer Systeme
Sicherheit von Maschinen	<b>EN ISO 13849-1:2015</b> Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze
Bauteil-Ausfallraten	<b>SN 29000: 2013</b> Ausfallraten (Siemens)

## 2 Gerätebeschreibung und Einsatzbereich

### 2.1 Sicherheitsfunktion

Der Differenzdrucktransmitter überträgt das Eingangssignal (Druck) in ein normiertes analoges 4...20 mA Ausgangssignal.

### 2.2 Definition des sicheren Zustandes

$\Delta I$ : Maximal mögliche Messunsicherheit des Gerätes in mA

Ausgangssignal $I_{out}$	Sichererer Zustand	Bemerkung
4...20 mA	$4 \text{ mA} - \Delta I \leq I_{out} \leq 20 \text{ mA} + \Delta I$	Stromsignal stimmt mit dem anliegenden Druck überein.

Die Messunsicherheit ergibt sich aus der Summe der maximalen Kennlinienabweichung und dem nach der Kompensation sich ergebenden Rest-Temperaturfehler. Beide Angaben findet man im Datenblatt. Die Werte werden in % bezogen auf den Messbereich (FS) angegeben.

Anmerkung: Für die Berechnung wird der jeweils größere TK von Nullpunkt oder Spanne verwendet.

$$\Delta I = F_{60^\circ\text{C}} \cdot \text{FS}$$

Beispiel: Messbereich 0... 10 mbar

$$F_{60^\circ\text{C}} [\%] = K_{\max} + (\text{TK}_N + \text{TK}_S) \cdot \frac{60^\circ\text{C} - 25^\circ\text{C}}{10}$$

$$= 1\% + (0,4\% + 0,3\%) \cdot 3,5$$

$$= 1\% + 0,7\% \cdot 3,5$$

$$= 3,45\%$$

$$\Delta I = F_{60^\circ\text{C}} \cdot \text{FS}$$

$$= 3,45\% \cdot 16 \text{ mA} = \frac{3,45 \cdot 16 \text{ mA}}{100} = 0,552 \text{ mA}$$

Signalspanne

$$\text{FS} = 20 \text{ mA} - 4 \text{ mA}$$

Datenblattwerte ( $T=25^\circ\text{C}$ )

Max. Kennlinienabweichung

$$K_{\max} = 1\%$$

Max. Temperaturkoeffizient

$$\text{TK}_N = 0,4\%/10\text{K} \quad (\text{Nullpunkt})$$

$$\text{TK}_S = 0,3\%/10\text{K} \quad (\text{Spanne})$$

Abb. 2: Berechnung der Messunsicherheit

### 2.3 Parametrierung



#### **! WARNUNG**

#### Parameteränderung

Das Gerät wird werkseitig parametrierung ausgeliefert. Diese Parametrierung darf nur vom Betreiber der Anlage oder von dafür beauftragtem und unterwiesenenem Fachpersonal geändert werden.

Die werkseitig festgelegten Grenzen für das Ausgangssignal dürfen nicht verändert werden.

Die Parametrierung kann auf zwei Arten geändert werden.<sup>(1)</sup>

- Durch Tastatureingabe am Gerät
- Durch Fernparametrierung mittels Transmitter-PC-Interface

Bei der Fernparametrierung können Übertragungsfehler auftreten. Deshalb ist es zwingend erforderlich alle Parameter und die Sicherheitsfunktion nach der Übertragung am Gerät zu verifizieren.

<sup>(1)</sup> Beachten Sie hierzu die Angaben in der Betriebsanleitung.

## 3 Hinweise zur Projektierung

### 3.1 Bestimmungsgemäßer Gebrauch

Das Gerät kann als Teil einer Sicherheitsfunktion zur Überwachung von Differenzdruck bei trockenen neutralen gasförmigen Medien eingesetzt werden.

Das Gerät kann in explosionsgefährdeten Bereichen Zone 21 und 22 (trockene Stäube) bzw. Zone 1 und 2 (Gase und Dämpfe) eingesetzt werden.

### 3.2 Funktionale Sicherheit (IEC 61508)

#### 3.2.1 Betriebsart

Das Gerät wird in der Betriebsart mit niedriger Anforderungsrate (Low Demand Mode) eingesetzt. Die Anforderungsrate ist geringer als einmal pro Jahr und nicht mehr als die doppelte Frequenz der Wiederholungsprüfung. Die Zugehörige Kenngröße ist der PFD Wert.

#### 3.2.2 Prüfintervall

Ein Proof-Test ist nach Inbetriebnahme und danach spätestens nach Ablauf des festgelegten Prüfintervalls durchzuführen.

Die Tabellen im Abschnitt Sicherheitstechnische Kennzahlen geben die durchschnittliche Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall in Abhängigkeit vom Prüfintervall und der Systemarchitektur an.

#### 3.2.3 Gebrauchsdauer

Die Gebrauchsdauer (Lifetime) beträgt ab Produktionsdatum 10 Jahre.

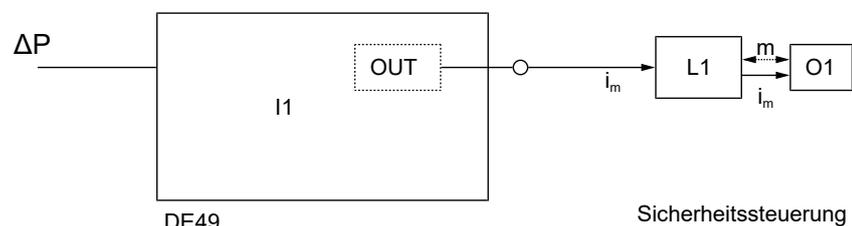
Wird die Gebrauchsdauer überschritten, können die Fehlerraten durch Verschleiß und Alterung allmählich ansteigen und die berechneten PFD-Werte können nicht mehr angewandt werden. Im ungünstigsten Fall führt dies zum Verlust der SIL Einstufung.

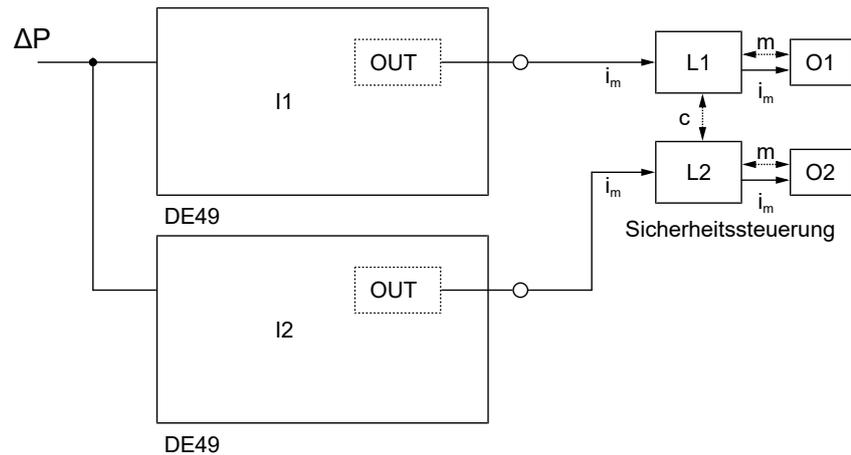
#### 3.2.4 Montage und Installation

Beachten Sie hierzu auch die Montageanleitung der Betriebsanleitung.

**HINWEIS! Beachten Sie, dass die Auswertung und Überwachung der Signale durch die nachgeschaltete Sicherheitssteuerung (SRP/CS) erfolgen muss. Bei einer Abweichung muss der sichere Zustand eingenommen werden.**

#### Architektur 1oo1 (SIL1)



**Architektur 1oo2 (SIL2)****Legende**

$i_m$	Verbindungsmittel
$c$	Kreuzvergleich
I1, I2	Differenzdrucktransmitter (DE49)
L1, L2	Logik
$m$	Überwachung
O1, O2	Ausgabeeinheiten
OUT	Ausgang (DE49)

**3.3 Performance Level (EN ISO 13849-1)****3.3.1 Betriebsart**

Das Gerät wird in der Betriebsart mit hoher Anforderungsrate eingesetzt. Die Anforderungsrate ist einmal pro Jahr.

**3.3.2 Prüfintervall**

Ein Proof-Test ist nach Inbetriebnahme und danach in regelmäßigen Intervallen durchzuführen. Die Prüfintervalle können anhand der Sicherheitskennzahlen [► 11] durch den Betreiber festgelegt werden.

**3.3.3 Gebrauchsdauer**

Die Gebrauchsdauer (Lifetime) beträgt ab Produktionsdatum 20 Jahre.

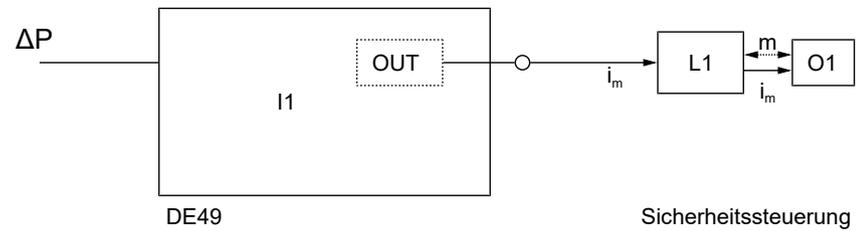
Wird die Gebrauchsdauer überschritten, können die Fehlerraten durch Verschleiß und Alterung allmählich ansteigen.

### 3.3.4 Montage und Installation

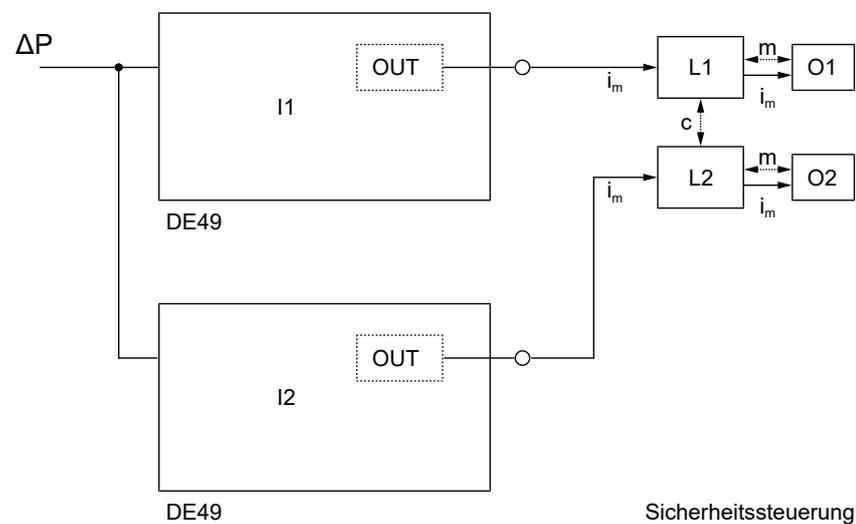
Beachten Sie hierzu auch die Montageanleitung der Betriebsanleitung.

**HINWEIS! Beachten Sie, dass die Auswertung und Überwachung der Signale durch die nachgeschaltete Sicherheitssteuerung (SRP/CS) erfolgen muss. Bei einer Abweichung muss der sichere Zustand eingenommen werden.**

#### Kategorie 1 (PL c)



#### Kategorie 3 (PL d)



#### Legende

$i_m$	Verbindungsmedium
$c$	Kreuzvergleich
I1, I2	Differenzdrucktransmitter (DE49)
L1, L2	Logik
$m$	Überwachung
O1, O2	Ausgabeeinheiten
OUT	Ausgang (DE49)

## 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! Die EMV- und Umweltbedingungen müssen den getesteten Niveaus der EMV-Richtlinie 2014/30/EU entsprechen.**

Die Festlegung der Proof-Test Prozedur für das gesamte Sicherheitstechnische-System ist Aufgabe des Betreibers.

Folgender Funktionstest ist für die sicherheitstechnische Komponente DE49 durchzuführen.

1. Überprüfung der Funktionalität bei Eingangswerten innerhalb des Messbereichs.
2. Überprüfung der Funktionalität bei Eingangswerten außerhalb des Messbereichs.

Der Prüfdruck sollte möglichst mit dem Sicherheitstechnischen System (SIS) selbst erzeugt werden, sofern dies möglich ist. In diesem Falle könnte gleichzeitig überprüft werden, ob die Signale von der übergeordneten Sicherheitssteuerung korrekt verarbeitet und über den Aktor weitergeleitet werden.

Andernfalls muss der DE49 ausgebaut und wie folgt verschaltet werden:

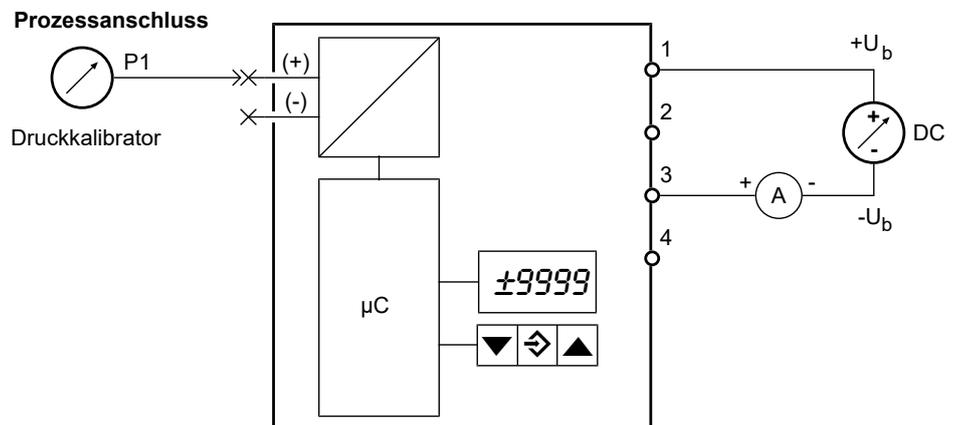


Abb. 3: Funktionstest

#### Prüfmittelliste

Prüfmittel	Verwendung	Auflösung
Druckkalibrator	Eingangssignal	0,1% vom Endwert
Multimeter	Ausgangssignal	1 µA (10 mV)
Stromversorgung	12 ... 32 V DC einstellbar	0,1 V

$\Delta I$ : Messunsicherheit  
des Gerätes in mA

### **Eingangswerte innerhalb des Messbereichs**

1. Stellen Sie eine Betriebsspannung von 24 V ein.
2. Stellen Sie mit dem Druckkalibrator ein Eingangssignal ein, dass dem Messbereichsanfang entspricht.
3. Prüfen Sie das Ausgangssignal.  
Der Ausgang muss ein Signal von 4 mA -  $\Delta I$  liefern.
4. Stellen Sie mit dem Druckkalibrator ein Eingangssignal ein, dass dem Messbereichsende entspricht.
5. Prüfen Sie das Ausgangssignal.  
Der Ausgang muss ein Signal von 20 mA +  $\Delta I$  liefern

### **Eingangswerte außerhalb des Messbereichs**

1. Stellen Sie mit dem Druckkalibrator ein Eingangssignal ein, dass deutlich unterhalb des Messbereichsanfang liegt.
2. Prüfen Sie das Ausgangssignal.  
Der Ausgang muss ein Signal  $< 4 \text{ mA} - \Delta I$  liefern.
3. Stellen Sie mit dem Druckkalibrator ein Eingangssignal ein, dass deutlich oberhalb des Messbereichsanfang liegt.
4. Prüfen Sie das Ausgangssignal.  
Der Ausgang muss ein Signal  $> 20 \text{ mA} + \Delta I$  liefern.

## 5 Sicherheitstechnische Kenngrößen

Die sicherheitstechnischen Kennzahlen sind abhängig vom verwendeten Sensorelement und werden für zwei Messbereichsgruppen (Sensor Typ A und Sensor Typ B) angegeben.

### 5.1 Sensortyp A

Die nachfolgenden Sicherheitskennzahlen gelten für folgende Geräteausführungen:



Messbereich	
<b>52</b>	0 ... 4 mbar
<b>53</b>	0 ... 6 mbar
<b>54</b>	0 ... 10 mbar
<b>55</b>	0 ... 16 mbar
<b>56</b>	0 ... 25 mbar
<b>57</b>	0 ... 40 mbar
<b>58</b>	0 ... 60 mbar
<b>59</b>	0 ... 100 mbar
<b>A6</b>	-2,5 ... +2,5 mbar
<b>A7</b>	-4 ... +4 mbar
<b>A8</b>	-6 ... +6 mbar
<b>A9</b>	-10 ... +10 mbar
<b>B1</b>	-16 ... +16 mbar
<b>B2</b>	-25 ... +25 mbar
<b>C5</b>	-40 ... +40 mbar
<b>B3</b>	-60 ... +60 mbar
<b>B4</b>	-100 ... +100 mbar
<b>D7</b>	0 ... 400 Pa
<b>D8</b>	0 ... 600 Pa
<b>D9</b>	0 ... 1000 Pa
<b>E1</b>	0 ... 1600 Pa
<b>L6</b>	-250 ... +250 Pa
<b>N1</b>	0 ... 1 kPa
<b>N2</b>	0 ... 1,6 kPa
<b>N3</b>	0 ... 2,5 kPa
<b>N4</b>	0 ... 4 kPa
<b>N5</b>	0 ... 6 kPa
<b>E5</b>	0 ... 10 kPa
<b>L8</b>	-1 ... +1 kPa
<b>L9</b>	-1,6 ... +1,6 kPa
<b>M6</b>	-2,5 ... +2,5 kPa
<b>M7</b>	-4 ... +4 kPa
<b>M8</b>	-6 ... +6 kPa

Gerätetyp	Typ B	Komplexes Gerät
Betriebsart	Low Demand	Anforderung max. 1/Jahr
<b>Ausfallraten</b>		
$\lambda_s$	114,1 Fit	Rate aller ungefährlichen Fehler
$\lambda_d$	136,0 Fit	Rate aller gefährlichen Fehler
$\lambda_{dd}$	84,0 Fit	Rate aller entdeckbaren gefährlichen Fehler
$\lambda_{du}$	52,0 Fit	Rate aller unentdeckbaren gefährlichen Fehler

**SIL (DIN EN 61508)****1oo1 Architektur**

HFT	0	Hardwarefehlertoleranz
SFF	79,2 %	Anteil der ungefährlichen Ausfälle

Die Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall (PFD) ist abhängig vom Prüfintervall.

Prüfintervall	1 Jahr	2 Jahre	5 Jahre	10 Jahre
PFD	$2,3 \cdot 10^{-4}$	$4,6 \cdot 10^{-4}$	$1,1 \cdot 10^{-3}$	$2,3 \cdot 10^{-3}$
SIL	SIL1	SIL1	SIL1	SIL1

**1oo2 Architektur**

$\beta$	10%	Wahrscheinlichkeit, dass der gleiche Fehler zur selben Zeit in beiden Kanälen auftritt.
$\beta_d$	5%	Wahrscheinlichkeit, dass der gleiche gefährliche Fehler zur selben Zeit in beiden Kanälen auftritt.
MRT	8 Std.	Mittlere Zeitdauer für eine Reparatur
MTTR	8 Std.	Mittlere Instandsetzungszeit
HFT	1	Hardwarefehlertoleranz
SFF	65,5 %	Anteil der ungefährlichen Ausfälle

Die Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall (PFD) ist abhängig vom Prüfintervall.

Prüfintervall	1 Jahr	2 Jahre	5 Jahre	10 Jahre
PFD	$2,3 \cdot 10^{-5}$	$4,6 \cdot 10^{-5}$	$1,6 \cdot 10^{-4}$	$2,3 \cdot 10^{-4}$
SIL	SIL2	SIL2	SIL2	SIL2

**PL (DIN EN ISO 13849)**

MTTF <sub>d</sub>	839,8 Jahre	hoch	Hardwarefehlertoleranz
DC	61,7 %	niedrig	Anteil der ungefährlichen Ausfälle

Erreichbarer Performancelevel	PL
Kategorie 1	c
Kategorie 3	d

### 5.2 Sensortyp B

Die nachfolgenden Sicherheitskennzahlen gelten für folgende Geräteausführungen:



Messbereich	
<b>D1</b>	0 ... 25 Pa
<b>D2</b>	0 ... 40 Pa
<b>D3</b>	0 ... 60 Pa
<b>D4</b>	0 ... 100 Pa
<b>L5</b>	-25 ... +25 Pa
<b>R6</b>	-40 ... +40 Pa
<b>2L</b>	-60 ... +60 Pa
<b>L7</b>	-100 ... +100 Pa
<b>L0</b>	-20 ... +80 Pa

Gerätetyp	Typ B	Komplexes Gerät
Betriebsart	Low Demand	Anforderung max. 1/Jahr

Ausfallraten		
$\lambda_s$	101,1 Fit	Rate aller ungefährlichen Fehler
$\lambda_d$	1757,3 Fit	Rate aller gefährlichen Fehler
$\lambda_{dd}$	1119,1 Fit	Rate aller entdeckbaren gefährlichen Fehler
$\lambda_{du}$	638,2 Fit	Rate aller unentdeckbaren gefährlichen Fehler

#### SIL (DIN EN 61508)

##### 1oo1 Architektur

HFT	0	Hardwarefehlertoleranz
SFF	65,7 %	Anteil der ungefährlichen Ausfälle

Die Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall (PFD) ist abhängig vom Prüfintervall.

Prüfintervall	1 Jahr	2 Jahre	5 Jahre	10 Jahre
PFD	$2,8 \cdot 10^{-3}$	$5,6 \cdot 10^{-3}$	$1,4 \cdot 10^{-2}$	$2,8 \cdot 10^{-2}$
SIL	SIL1	SIL1	SIL1	SIL1

##### 1oo2 Architektur

$\beta$	10%	Wahrscheinlichkeit, dass der gleiche Fehler zur selben Zeit in beiden Kanälen auftritt.
$\beta_d$	5%	Wahrscheinlichkeit, dass der gleiche gefährliche Fehler zur selben Zeit in beiden Kanälen auftritt.
MRT	8 Std.	Mittlere Zeitdauer für eine Reparatur
MTTR	8 Std.	Mittlere Instandsetzungszeit
HFT	1	Hardwarefehlertoleranz
SFF	65,5 %	Anteil der ungefährlichen Ausfälle

Die Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall (PFD) ist abhängig vom Prüfintervall.

Prüfintervall	1 Jahr	2 Jahre	5 Jahre	10 Jahre
PFD	$2,9 \cdot 10^{-4}$	$6,0 \cdot 10^{-4}$	$1,6 \cdot 10^{-3}$	$3,7 \cdot 10^{-3}$
SIL	SIL2	SIL2	SIL2	SIL2

#### PL (DIN EN ISO 13849)

MTTF <sub>d</sub>	65 Jahre	hoch	Hardwarefehler toleranz
DC	63,7 %	niedrig	Anteil der ungefährlichen Ausfälle
Erreichbarer Performancelevel		PL	
Kategorie 1		c	
Kategorie 3		d	

## 6 Anhang

### 6.1 Glossar

Abk. (↓ <sup>A</sup> / <sub>Z</sub> )	Definition
<b>DC</b>	<p>(en) <b>Diagnostic Coverage Faktor</b> (de) Diagnosedeckungsgrad</p> <p>Der DC Parameter gibt das Verhältnis der Anzahl aller entdeckbaren gefährlichen Fehler (<math>\lambda_{DD}</math>) zur gesamten Anzahl der gefährlichen Fehler (<math>\lambda_D</math>) an.</p> $DC = \frac{\sum \text{erkannter gefährlicher Fehler}}{\sum \text{gesamter gefährlicher Fehler}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
<b>FIT</b>	<p>(en) <b>Failure in Time</b> (de) Ausfälle pro Zeit</p> <p>Ausfallrate bezogen auf das Zeitintervall <math>10^9</math> Stunden.</p> $1 \text{ FIT} = 1 \times 10^{-9} \frac{1}{\text{h}}$
<b>FMEDA</b>	<p>(en) <b>Failure Mode Effect and Diagnostic Analysis</b> (de) Gefährdung und Risikoanalyse</p> <p>Verfahren zur Ermittlung von Fehlerursachen und deren Auswirkung auf das System.</p>
<b>HDM</b>	<p>(en) <b>High Demand Mode</b> (de) Betriebsart mit hoher Anforderungsstufe</p> <p>Betriebsart mit hoher oder kontinuierlicher Anforderung der Sicherheitsfunktion. Die Anforderungsrate an das sicherheitsbezogene System beträgt mehr als einmal pro Jahr.</p>
<b>HFT</b>	<p>(en) <b>Hardware Fault Tolerance</b> (de) Hardware-Fehlertoleranz</p> <p>Die Hardware-Fehlertoleranz gibt an, wie viele gefährliche Fehler aufgrund der Architektur möglich sind, ohne dass die Ausführung der Sicherheitsfunktion gefährdet ist.</p> <ul style="list-style-type: none"> <li>• HFT = 0 Der Eintritt eines gefährlichen Fehlers führt bereits zum Ausfall der Sicherheitsfunktion.</li> <li>• HFT = 1 Erst der Eintritt von zwei gefährlichen Fehlern führt zum Ausfall der Sicherheitsfunktion.</li> </ul>
<b>LDM</b>	<p>(en) <b>Low Demand Mode</b> (de) Betriebsart mit niedriger Anforderungsstufe</p> <p>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.</p>

<b>MooN</b>	<p>(en) <b>Architecture with M out of N channels</b>          (de) Systemarchitektur mit M aus N Kanälen</p> <hr/> <p>Systemarchitektur MooN mit den Variablen M und N:          Klassifizierung und Beschreibung des sicherheitsbezogenen Systems hinsichtlich der Redundanz und den angewandten Auswahlverfahren.</p> <ul style="list-style-type: none"> <li>• N - gibt die gesamte Anzahl der redundanten Kanäle einer sicherheitsbezogenen Architektur bzw. eines Sicherheitskreises an.</li> <li>• M – bestimmt, wie viele Kanäle korrekt arbeiten müssen, um die Sicherheitsfunktion auszuführen.</li> </ul>
<b>MTBF</b>	<p>(en) <b>Mean Time Between Failures</b>          (de) Mittlere Brauchbarkeitsdauer</p> <hr/> <p>Mittlere Betriebsdauer zwischen zwei Ausfällen.</p>
<b>MTTF<sub>d</sub></b>	<p>(en) <b>Mean Time To Dangerous Failures</b>          (de) Mittlere Zeit bis zum gefahrbringenden Ausfall</p> <hr/> <p>Betriebsdauer bis zu einem gefahrbringenden Fehler.</p>
<b>MRT</b>	<p>(en) <b>Mean Repair Time</b>          (de) Mittlere Reparaturdauer</p> <hr/> <p>Mittlere Zeitdauer für die Reparatur.</p>
<b>MTTR</b>	<p>(en) <b>Mean Time To Repair</b>          (de) Mittlere Instandsetzungszeit</p> <hr/> <p>Mittlere Zeitdauer zwischen dem Auftreten eines Fehlers und der Wiederherstellung des Systems.</p>
<b>PFD</b>	<p>(en) <b>Probability of Failure on Demand</b>          (de) Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall</p> <hr/> <p>Wahrscheinlichkeit eines gefahrbringenden Ausfalls bei Anforderung der Sicherheitsfunktion für eine Betriebsart mit niedriger Anforderungsrate (Low Demand).</p>
<b>PFH</b>	<p>(en) <b>Probability of a dangerous Failure per Hour</b>          (de) Ausfallwahrscheinlichkeit pro Stunde für die Sicherheitsfunktion</p> <hr/> <p>Häufigkeit eines gefahrbringenden Ausfalls der Sicherheitsfunktion für eine Betriebsart mit hoher oder kontinuierlicher Anforderungsrate (High Demand).</p>
<b>PFS</b>	<p>(en) <b>Probability of Failure Spurious</b>          (de) Ausfallwahrscheinlichkeit aufgrund einer nicht beabsichtigten Prozessabschaltung</p> <hr/> <p>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.</p>

---

<b>SFF</b>	<b>(en) Safe Failure Fraction</b> <b>(de) Anteil der ungefährlichen Ausfälle</b>
	Ergibt sich aus der Rate der ungefährlichen Fehler plus der diagnostizierten bzw. erkannten Fehler im Verhältnis zur gesamten Ausfallrate des Systems.
<b>SIF</b>	<b>(en) Safety Instrumented Function</b> <b>(de) Sicherheitstechnische Funktion</b>
	Die Sicherheitsfunktion (SIF) ist eine Schutzmaßnahme, die nur im Störfall aktiviert wird und dann verhindert, dass Personen, Umwelt und Sachwerte Schaden nehmen.
<b>SIL</b>	<b>(en) Safety Integrity Level</b> <b>(de) Sicherheits-Integritätslevel</b>
	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.
<b>SIS</b>	<b>(en) Safety Instrumented System</b> <b>(de) Sicherheitstechnisches-System</b>
	Sicherheitstechnisches-System zur Ausführung einer oder mehrerer sicherheitstechnischer Funktionen. Ein solches System besteht mindestens aus einem Sensor, einer übergeordneten Sicherheitssteuerung und einem Aktor.
<b>T<sub>1</sub></b>	<b>(en) Proof Test Interval</b> <b>(de) Prüfintervall</b>
	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.

---

## 6.2 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.

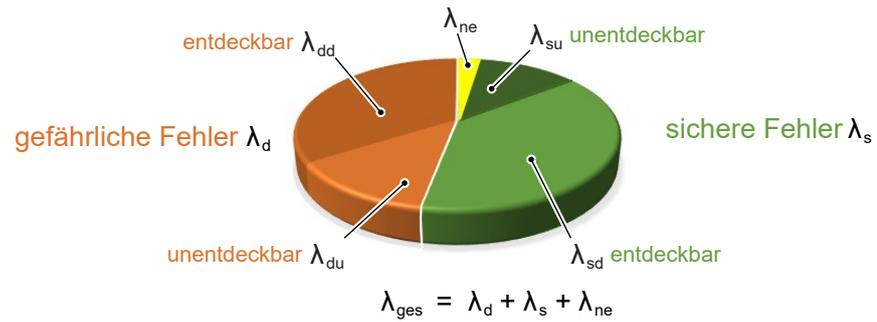


Abb. 4: Fehlerraten

$\lambda_d$	(en) <b>Dangerous failure rate</b> (de) Rate aller gefährlichen Fehler
$\lambda_{dd}$	(en) <b>Dangerous detected failure rate</b> (de) Rate aller entdeckbaren gefährlichen Fehler
$\lambda_{du}$	(en) <b>Dangerous undetected failure rate</b> (de) Rate aller unentdeckbaren gefährlichen Fehler
$\lambda_s$	(en) <b>Safe failure rate</b> (de) Rate aller ungefährlichen Fehler
$\lambda_{sd}$	(en) <b>Safe detected failure rate</b> (de) Rate aller entdeckbaren sicheren Fehler
$\lambda_{su}$	(en) <b>Safe undetected failure rate</b> (de) Rate aller unentdeckbaren sicheren Fehler
$\lambda_{ne}$	(en) <b>No effect failure rate</b> (de) Rate aller Fehler ohne Auswirkung

### 6.3 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.

## 6.4 Symbolerklärung



### **GEFAHR**

#### Art und Quelle der Gefahr

Diese Darstellung wird verwendet um auf eine **unmittelbar** gefährliche Situation hinzuweisen, die Tod oder schwerste Körperverletzungen zur Folge **haben wird** (höchste Gefährdungsstufe).

1. Vermeiden Sie die Gefahr, indem Sie die geltenden Sicherheitsbestimmungen beachten.



### **WARNUNG**

#### Art und Quelle der Gefahr

Diese Darstellung wird verwendet um auf eine **möglicherweise** gefährliche Situation hinzuweisen, die Tod oder schwere Körperverletzungen zur Folge **haben kann** (mittlere Gefährdungsstufe).

1. Vermeiden Sie die Gefahr, indem Sie die geltenden Sicherheitsbestimmungen beachten.



### **VORSICHT**

#### Art und Quelle der Gefahr

Diese Darstellung wird verwendet um auf eine **möglicherweise** gefährliche Situation hinzuweisen, die leichte bis mittlere Körperverletzungen, Sach- oder Umweltschäden zur Folge **haben kann** (niedrige Gefährdungsstufe).

1. Vermeiden Sie die Gefahr, indem Sie die geltenden Sicherheitsbestimmungen beachten.



### **HINWEIS**

#### Hinweis / Tipp

Diese Darstellung wird verwendet um nützliche Hinweise oder Tipps für einen effizienten und störungsfreien Betrieb zu geben.



**FISCHER Mess- und Regeltechnik GmbH**

Bielefelder Str. 37a  
D-32107 Bad Salzuflen

Tel. +49 5222 974-0

Fax +49 5222 7170

[www.fischermesstechnik.de](http://www.fischermesstechnik.de)

[info@fischermesstechnik.de](mailto:info@fischermesstechnik.de)