developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL

CE
RoHS III
COMPLIANT
EAC

Sicherheitshandbuch

NK10

Füllstandbegrenzer

09015130 • SHB_DE_NK10 • Rev. ST4-B • 01/21

Inhaltsverzeichnis

1 Geltungsbereich und Standards

Dieses Dokument gilt für die Füllstandbegrenzer der Baureihe NK10.

Diese sicherheitsgerichteten Füllstandbegrenzer sind vom TÜV Süd entsprechend EN 61508 für SIL1 und SIL2 (SIL 3 bei redundanter Verschaltung) zertifiziert.

1.1 Standards

Richtlinien

Druckgeräterichtlinie 2014/68/EU
Ausrüstungsteil mit Sicherheitsfunktion Kategorie IV

Mitgeltende EG-Richtlinie:
Niederspannungsrichtlinie 2014/35/EU

Angewandte Normen und Regelwerke:

EN 61508
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

EN 61511
Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozess

EN 61010-1
Sicherheitsbestimmungen für elektrische Mess-, Steuer-, Regel- und Laborgeräte - Allgemeine Anforderungen

DIN 4754-3
Wärmeübertragungsanlagen mit organischen Wärmeträgern - Teil 3: Füllstandsicherungen

EN 13445-1
Unbefeuerte Druckbehälter

1.2 Abkürzungen

SIL *(en: Safety Integrity Level)*
Sicherheitsanforderungsstufe

Die internationale Norm IEC 61508 definiert vier diskrete Sicherheitsanforderungsstufen (SIL 1 bis SIL 4). Jede Stufe entspricht einem Wahrscheinlichkeitsbereich für das Versagen einer Sicherheitsfunktion. Je höher die Stufe des sicherheitsbezogenen Systems ist, umso geringer ist die Wahrscheinlichkeit, dass die geforderten Sicherheitsfunktionen nicht ausführt werden.

HFT *(en: Hardware Failure Tolerance)*
Hardwarefehlertoleranz

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

MTBF *(en: Mean Time Between Failures)*

Mittlere Betriebsdauer zwischen zwei Ausfällen.

MTTR *(en: Mean Time To Repair)*

Mittlere Zeitdauer zwischen dem Auftreten eines Fehlers und der Reparatur.

PFD *(en: Probability of Failure on Demand)*

Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall.

PFD_{AVG} *(en: Average Probability of Failure on Demand)*

Mittlere Wahrscheinlichkeit gefahrbringender Ausfälle einer Sicherheitsfunktion im Anforderungsfall.

λ_S *(en: Lambda Safe)*

Gesamtrate aller sicheren Ausfälle.

λ_{DD} *(en: Lambda Dangerous Detected failures)*

Gesamtrate für gefährliche, erkannte Ausfälle.

λ_{DU} *(en: Lambda Dangerous Undetected failures)*

Gesamtrate für gefährliche, nicht erkannte Ausfälle.

DC *(en: Diagnostic Coverage)*

Der Diagnosedeckungsgrad ist ein Maß für die Erkennung möglicher Fehler durch Tests.

SFF *(en: Safe Failure Fraction)*
Anteil ungefährlicher Ausfälle

Anteil von Ausfällen ohne Potenzial, das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand zu versetzen.

FIT *(en: Failure In Time)*
Ausfallhäufigkeit

Anzahl der Fehler innerhalb 10^9 Stunden.

T1 *(en: Test Intervall)*

Prüfintervall der Schutzfunktion.

XooY *(en: X out of Y))*
Auswahlschaltung:

Klassifizierung und Beschreibung des sicherheitsbezogenen Systems hinsichtlich Redundanz und angewandtem Auswahlverfahren.

- X Gibt an, wie oft die Sicherheitsfunktion ausgeführt wird (Redundanz).
- Y Bestimmt, wie viele Kanäle korrekt arbeiten müssen.

LDM *(en: Low Demand Mode)*

Betriebsart, bei der die Anforderungsrate an das sicherheitsbezogene System nicht mehr als einmal pro Jahr beträgt und nicht größer als die doppelte Frequenz der Wiederholungsprüfung ist.

1.3 Mitgeltende Unterlagen

Datenblatt Standard	09005238	DB_DE_NK10
Datenblatt ATEX	09005535	DB_DE_NK10_H
Betriebsanleitung Standard	09005016	BA_DE_NK10
Betriebsanleitung ATEX	09005110	BA_DE_NK10_H

2 Gerätebeschreibung und Einsatzbereich

2.1 Aufbau und Sicherheitsfunktion

Das Schwimmersystem des Füllstandbegrenzers befindet sich im flüssigkeitsgefüllten Behälter (Ausdehnungsgefäß). Die bei Füllstandänderung entstehende Schwimmerbewegung wird über die mit einem Edelstahlbalg abgedichtete Schwimmerstange direkt auf einen Schalter übertragen. Der Drehpunkt der Schwimmerstange liegt außerhalb des Druckraumes.

Außerhalb des Druckraumes befindet sich eine Prüftaste, die eine Funktionsprüfung nach DIN 4754-3 ohne Absenkung des Füllstandes ermöglicht. Bei Betätigung der Prüftaste wird der Schwimmerkörper gegen seinen Auftrieb bewegt.

Der Schaltpunkt des Schalters S1 (Klemme 1, 2, 3) wird werksseitig so justiert, dass die Umschaltung bei waagerechter Schwimmerstange erfolgt. Der optionale Vorwarnschalter S2 schaltet ca. 2,5 mm vor S1.

In einer einkanaligen Architektur (1oo1) können die Geräte bis SIL 2 eingesetzt werden. In einer mehr-kanaligen, redundanten Architektur ist der Einsatz bis SIL 3 möglich. Die Schaltkontakte des Füllstandbegrenzers sind dabei durch eine geeignete übergeordnete Einrichtung sicherheitsgerichtet als 1oo2-System im Sinne der DIN EN 61508 zu überwachen.

2.2 Funktionsbild

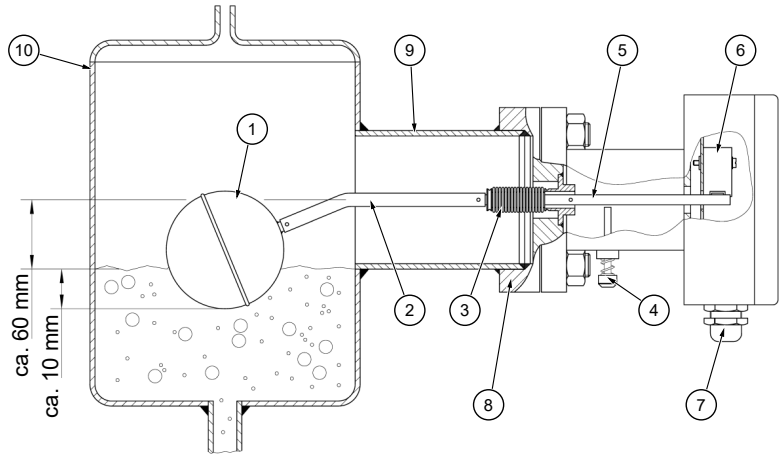

Abb. 1: Funktionsbild

1	Schwimmer	2	Schwimmerstange
3	Metallbalg	4	Prüftaste
5	Schalthebel	6	Microschalter S1
7	Kabelverschraubung	8	Flansch und Gegenflansch
9	Einschweissstutzen	10	Behälter

3 Hinweise zur Projektierung

Die Füllstandbegrenzer sind für eine Betriebsart mit niedriger Anforderungsrate (low demand mode) bis SIL2 vorgesehen.

In einer mehrkanaligen, redundanten Architektur ist der Einsatz als sicherheitsrelevantes Teilsystem in der Betriebsart mit niedriger oder hoher Anforderungsrate bis SIL3 möglich.

3.1 Anschlussschemata für SIL Anwendungen

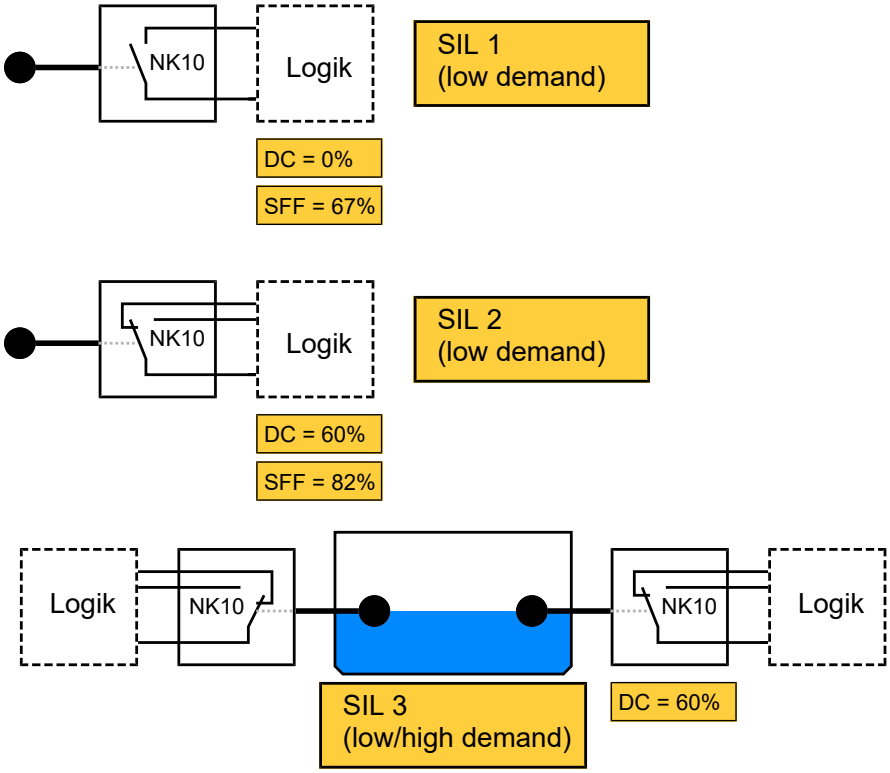

Abb. 2: Anschlussschema SIL

3.2 Wartung und wiederkehrende Prüfungen

Die in der SIL Herstellererklärung dokumentierten PFD Werte gelten für das Prüfintervall T1 = 1Jahr. Die Funktionsprüfung des Füllstandbegrenzers ist somit in der Anwendung jährlich durchzuführen.

VORSICHT! Beachten Sie Anlagensicherheit und Betriebsvorschriften.

Das Gerät ist wartungsfrei. Um einen zuverlässigen Betrieb und eine lange Lebensdauer des Gerätes sicherzustellen, empfehlen wir dennoch eine regelmäßige Prüfung des Gerätes in folgenden Punkten:

- Überprüfung der Schaltfunktion (mit Hilfe der Prüftaste) in Verbindung mit den Folgekomponenten.
- Dichtheits-Kontrolle der Flanschverbindung.
- Kontrolle der elektrischen Anschlüsse (Klemmverbindung der Kabel).

Die genauen Prüfzyklen sind den Betriebs- und Umgebungsbedingungen anzupassen. Beim Zusammenwirken verschiedener Gerätekomponenten sind auch die Betriebsanleitungen aller anderen Geräte zu beachten.

3.3 Sicherheitskennzahlen

HINWEIS! SIL 2 bzw. SIL 3 werden mit dem Füllstandbegrenzer als Sensor in Verbindung mit einer externen Logik oder SPS erreicht.

	SIL 1	SIL 2	SIL 3
Gerätetyp	A	A	A
Betriebsart	LOW	LOW	LOW/HIGH
Prüfintervall	1 Jahr	1 Jahr	1 Jahr
Gebrauchsdauer	100000 Schalt-spiele 15 Jahre	100000 Schalt-spiele 15 Jahre	100000 Schalt-spiele 15 Jahre
HFT *)	0	0	0
SFF	67 %	82 %	83 %
PFD_{avg}	$5{,}34*10^{-4}$	$2{,}94*10^{-4}$	---
PFD_G	---	---	$1{,}44*10^{-5}$
PFH_G	---	---	$7{,}95*10^{-9}$
λ_S	315,70 FIT	315,7 FIT	315,70 FIT
λ_{DD}	0,00 FIT	72,00 FIT	94,38 FIT
λ_{DU}	157,30 FIT	85,30 FIT	62,92 FIT
MTTR	72 h	72 h	72 h
MTBF	241 Jahre	241 Jahre	241 Jahre

*) einkanalige Verwendung

4 SIL Zertifikat

TÜV SÜD ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

ZERTIFIKAT

Nr. Z10 027632 0002 Rev. 01

Zertifikatsinhaber: **FISCHER**
Mess- und Regeltechnik GmbH
Bielefelder Straße 37a
32107 Bad Salzuflen
DEUTSCHLAND

Fertigungsstätte(n): 027632

Prüfzeichen:

Produkt: **Füllstandsgeräte**
Level Limiter

Modell(e): **NK10**

Parameter: 1oo1 Konfiguration: SIL 1/2
1oo2 Konfiguration: SIL 3

Schutzart: IP55
Nennausgangsstrom
bei 250Vac: 6A
bei 250Vdc: 250mA

Geprüft nach: IEC 61508-1:2010
IEC 61508-2:2010

Das Produkt wurde auf freiwilliger Basis auf die Einhaltung der grundlegenden Anforderungen geprüft und kann mit dem oben abgebildeten Prüfzeichen gekennzeichnet werden. Eine Veränderung der Darstellung des Prüfzeichens ist nicht erlaubt. Die Übertragung eines Zertifikates durch den Zertifikatsinhaber an Dritte ist unzulässig. Umseitige Hinweise sind zu beachten.

Prüfbericht Nr.: 717503460

Gültig bis: 2025-10-25

Datum, 2020-10-26 (Claudio Gregorio)

A4 / 07.17

Seite 1 von 1
TÜV SÜD Product Service GmbH • Zertifizierstelle • Ridlerstraße 65 • 80339 München • Deutschland

TÜV®

Abb. 3: SIL_IEC61508_DE_EN(1)Teil1

5 Anhang

5.1 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.
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.
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.

5.2 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.

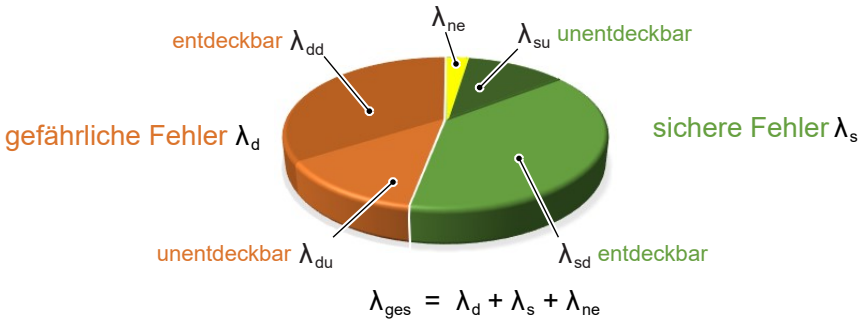

Abb. 4: Fehlerraten

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

5.3 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.

5.4 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.

Notizen

FISCHER Mess- und Regeltechnik GmbH
Bielefelder Str. 37a
D-32107 Bad Salzuflen

Tel. +49 5222 974-0
Fax +49 5222 7170
www.fischermesstechnik.de
info@fischermesstechnik.de