developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL

RoHS III COMPLIANT

Sicherheitshandbuch

NK10

Füllstandbegrenzer

09015130 • SHB_DE_NK10 • Rev. ST4-C • 08/22

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
web: www.fischermesstechnik.de

Technische Redaktion: Dokumentationsbeauftragter: T. Malischewski
Technischer Redakteur: R. Kleemann

Versionsgeschichte

Rev. ST4-A 11/18	Version 1 (Erstausgabe)
Rev. ST4-B 01/21	Version 2 (Korrektur Geltungsbereich: U-Nr. entfällt))
Rev. ST4-C 08/22	Version 3 (neue SIL Zertifizierung)

Inhaltsverzeichnis

1 Geltungsbereich und Standards

Dieses Dokument gilt für die Füllstandbegrenzer der Baureihe NK10.

Diese sicherheitsgerichteten Füllstandbegrenzer sind vom TÜV entsprechend IEC 61508 (Teil 1-2 und 4-7:2010) für SIL1 und SIL2 (SIL 3 bei redundanter Verschaltung) zertifiziert.

1.1 Standards

Richtlinien

Druckgeräterichtlinie 2014/68/EU
Ausrüstungsteil für die Verwendung in einer Sicherheitskette als gesamtes Ausrüstungsteil mit Sicherheitsfunktion der Kategorie IV

Mitgeltende EG-Richtlinie:
Niederspannungsrichtlinie 2014/35/EU

Angewandte Normen und Regelwerke:

IEC 61508
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - (Teil1-2 und 4-7)

EN 61511
Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie

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.

PFH *(en: Probability Failure per Hour)*

Durchschnittliche Wahrscheinlichkeit eines gefährlichen Ausfalls pro Stunde.

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

Prozentualer Anteil der ungefährlichen Ausfälle an der Gesamtzahl der möglichen Ausfälle , die das sicherheitsbezogene System in einen gefährlichen oder unzulässigen Funktionszustand 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.

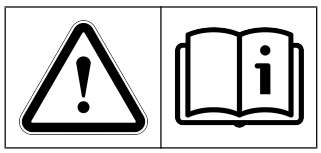
LDM *(en: Low Demand Mode)*

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.

HDM *(en: High Demand Mode)*

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

1.3 Mitgeltende Unterlagen



Betriebsanleitungen und Datenblätter enthalten wichtige Sicherheitshinweise und technische Daten, die für den sicheren Betrieb unerlässlich sind.

Die Dokumente gelten in der jeweils aktuellen Fassung, die auf der Webseite www.fischermesstechnik.de zur Verfügung stehen.

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.

Die Sicherheitsfunktion ist definiert als:

1. Sicheres Schalten bei Erreichen des eingestellten Grenzwertes (Schalter S1)
2. Sichere Vorwarnung bei Erreichen des eingestellten Grenzwertes (Schalter S2) - Option

Die Schaltkontakte des Füllstandbegrenzers sind dabei durch eine geeignete übergeordnete Einrichtung sicherheitsgerichtet im Sinne der EN 61508 zu überwachen.

In einer einkanaligen Architektur (1oo1) können die Geräte bis SIL 2 eingesetzt werden. In einer mehr-kanaligen, redundanten Architektur (1oo2) ist der Einsatz bis SIL 3 möglich.

2.2 Funktionsbild

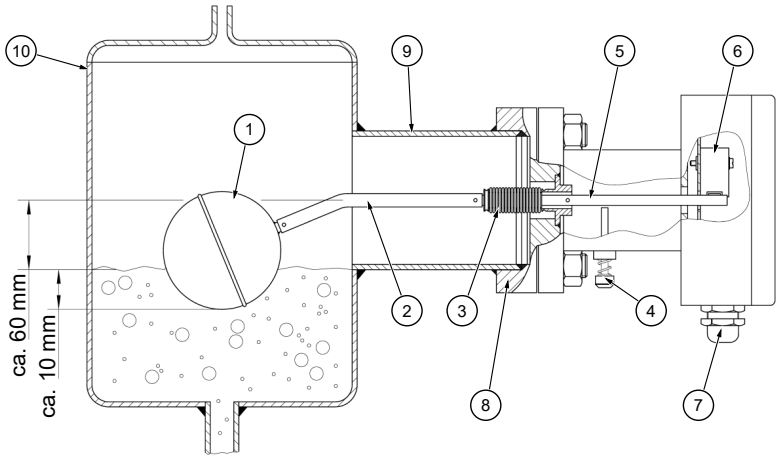


Abb. 1: Funktionsbild

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

Die Schaltkontakte des Füllstandbegrenzers sind durch eine geeignete übergeordnete Einrichtung sicherheitsgerichtet im Sinne der EN 61508 zu überwachen, um den erforderlichen Diagnosedeckungsgrad (DC) zu erreichen.

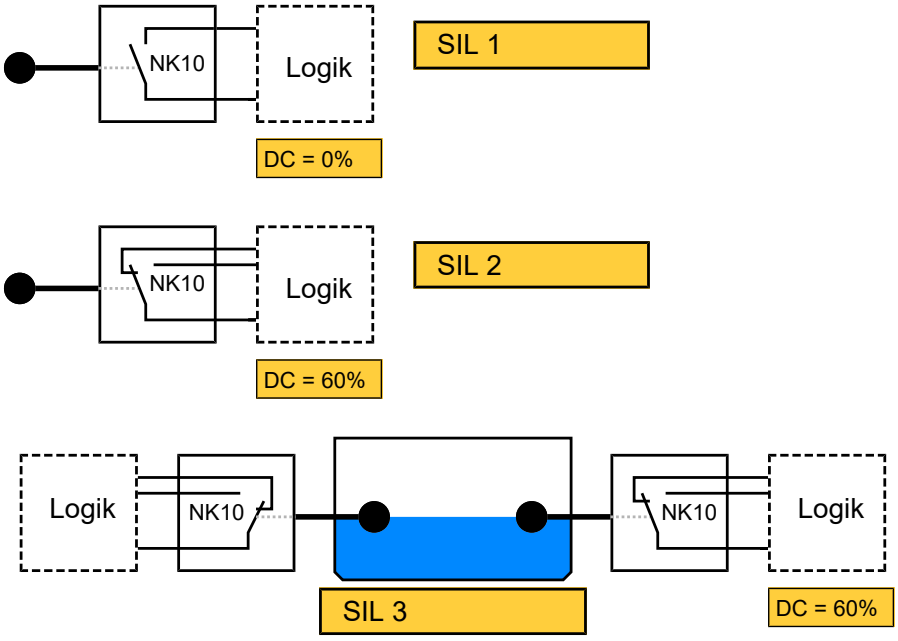


Abb. 2: Anschlussschema SIL

3.2 Wartung und wiederkehrende Prüfungen

Beachten Sie hierzu auch die Angaben in der Betriebsanleitung.

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 den nachfolgend genannten Punkten:

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

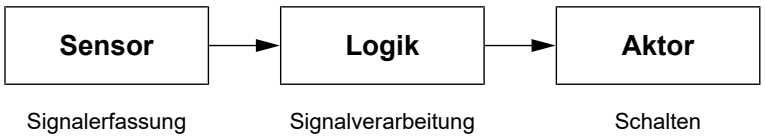
Die Prüfung hat einmal pro Jahr oder je nach Betriebsvorschrift auch öfter zu erfolgen und muss schriftlich dokumentiert werden.

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

Alle defekten oder mit Mängeln behafteten Geräte sind direkt an unsere Reparaturabteilung zu senden. Wir bitten darum alle Geräterücksendungen mit unserer Verkaufsabteilung abzustimmen. Zur Rücksendung des Gerätes ist die Originalverpackung oder eine geeignete Transportverpackung zu verwenden.

3.3 Sicherheitskennzahlen

SIL 1/2 bzw. SIL 3 werden mit dem Füllstandbegrenzer NK10 (als Sensor) nur in Verbindung mit einer sicherheitsgerichteten übergeordneten Einrichtung (Logik) im Sinne der EN 61508 erreicht.



- Der NK10 besitzt keine integrierte Diagnose. Ist eine Diagnose der Sicherheitsfunktion erforderlich, so muss diese als Teil des sicherheitsgerichteten Gesamtsystems durch externe Maßnahmen bereitgestellt werden. Die angegebenen Ausfallraten für DC=60% verstehen sich als Richtwerte in Verbindung mit der Auswertelogik und sind anlagespezifisch zu berechnen.
- Die Ausfallraten, die für den Low Demand Mode ermittelt wurden, können auch für High Demand Mode Anwendungen bis zu einer maximalen Anforderungsrate von 12-mal pro Jahr zur Berechnung des PFH verwendet werden. Bis zu dieser Anforderungsrate ist mit keinen Fehlern zu rechnen, die auf Verschleiß zurückzuführen sind.

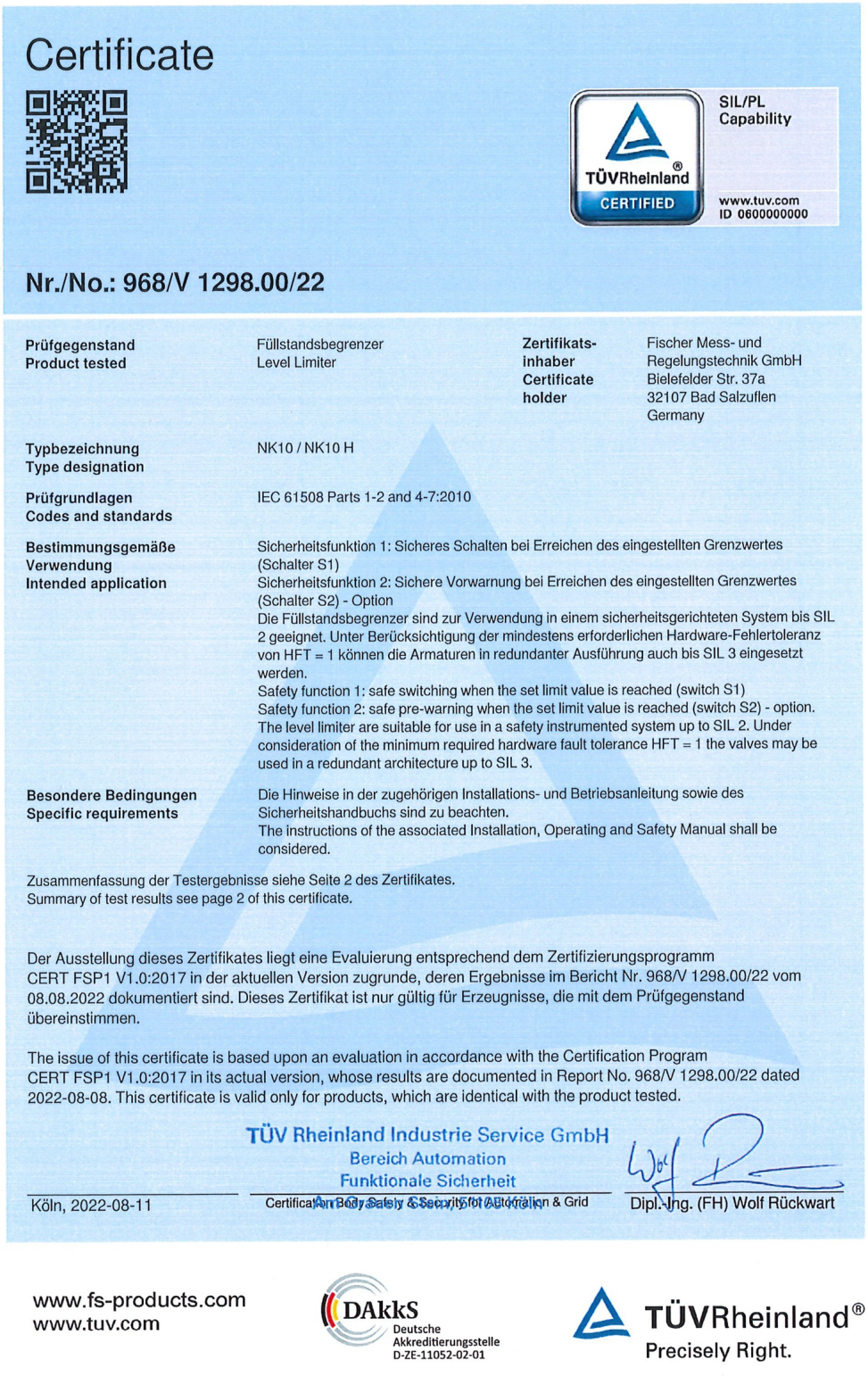
$$PFH = \lambda_d$$

Gerätetyp	A
Betriebsart	LDM (Low Demand Mode)
Hardware Fehlertoleranz	HFT 0
Systematische Fähigkeit	SC 3
Prüfintervall	T_1=1Jahr
Gebrauchsdauer	10000 Schaltspiele oder 15 Jahre

Architektur 1oo1			
Diagnosedeckungsgrad	DC	0	60
Fehlerrate	λ_{du}	$3{,}13 * 10^{-7}$ 1/h (313 FIT)	$1{,}25 * 10^{-7}$ 1/h (125 FIT)
Ausfallraten Low Demand Mode	PFD_{avg}	$1{,}39 * 10^{-3}$	$5{,}50 * 10^{-4}$
Ausfallraten High Demand Mode	PFH	$3{,}13 * 10^{-7}$ 1/h	$1{,}25 * 10^{-7}$ 1/h

Architektur 1oo2			
Diagnosedeckungsgrad	DC	0	60
Fehlerrate	λ_{du}	$3{,}13 * 10^{-7}$ 1/h (313 FIT)	$1{,}25 * 10^{-7}$ 1/h (125 FIT)
Ausfallraten Low Demand Mode	PFD_{avg}	$1{,}41 * 10^{-4}$	$5{,}55 * 10^{-5}$
Ausfallraten High Demand Mode	PFH	$3{,}20 * 10^{-8}$ 1/h	$1{,}26 * 10^{-8}$ 1/h

4 SIL Zertifikat



Certificate

SIL/PL Capability

TÜVRheinland CERTIFIED

www.tuv.com
ID 0600000000

Nr./No.: 968/V 1298.00/22

Prüfgegenstand **Product tested**	Füllstandsbegrenzer Level Limiter	**Zertifikats-inhaber** **Certificate holder**	Fischer Mess- und Regelungstechnik GmbH Bielefelder Str. 37a 32107 Bad Salzuflen Germany
Typbezeichnung **Type designation**	NK10 / NK10 H		
Prüfgrundlagen **Codes and standards**	IEC 61508 Parts 1-2 and 4-7:2010		
Bestimmungsgemäße Verwendung **Intended application**	Sicherheitsfunktion 1: Sicheres Schalten bei Erreichen des eingestellten Grenzwertes (Schalter S1) Sicherheitsfunktion 2: Sichere Vorwarnung bei Erreichen des eingestellten Grenzwertes (Schalter S2) - Option Die Füllstandsbegrenzer sind zur Verwendung in einem sicherheitsgerichteten System bis SIL 2 geeignet. Unter Berücksichtigung der mindestens erforderlichen Hardware-Fehlertoleranz von HFT = 1 können die Armaturen in redundanter Ausführung auch bis SIL 3 eingesetzt werden. Safety function 1: safe switching when the set limit value is reached (switch S1) Safety function 2: safe pre-warning when the set limit value is reached (switch S2) - option. The level limiter are suitable for use in a safety instrumented system up to SIL 2. Under consideration of the minimum required hardware fault tolerance HFT = 1 the valves may be used in a redundant architecture up to SIL 3.		
Besondere Bedingungen **Specific requirements**	Die Hinweise in der zugehörigen Installations- und Betriebsanleitung sowie des Sicherheitshandbuchs sind zu beachten. The instructions of the associated Installation, Operating and Safety Manual shall be considered.		

Zusammenfassung der Testergebnisse siehe Seite 2 des Zertifikates.
Summary of test results see page 2 of this certificate.

Der Ausstellung dieses Zertifikates liegt eine Evaluierung entsprechend dem Zertifizierungsprogramm CERT FSP1 V1.0:2017 in der aktuellen Version zugrunde, deren Ergebnisse im Bericht Nr. 968/V 1298.00/22 vom 08.08.2022 dokumentiert sind. Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.

The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT FSP1 V1.0:2017 in its actual version, whose results are documented in Report No. 968/V 1298.00/22 dated 2022-08-08. This certificate is valid only for products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit

Köln, 2022-08-11 — Certification Body Safety & Security for Automation & Grid — Dipl.-Ing. (FH) Wolf Rückwart

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-01

TÜVRheinland® Precisely Right.

10/222 12. 12 E A4 © TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

Abb. 3: 968_V_1298_00_22_de_en_el_Seite_1

968/V 1298.00/22 - page 2

TÜVRheinland®
Precisely Right.

Holder: Fischer Mess- und Regeltechnik GmbH
Bielefelder Straße 37a
D-32107 Bad Salzuflen
Germany

Product tested: **Level indicator / level limiter**
NK10 / NK10 H

Results of Assessment

Route of Assessment		2_H / 1_S
Type of Sub-system		Type A
Mode of Operation		Low Demand Mode
Hardware Fault Tolerance	HFT	0
Systematic Capability		**SC 3**

Safe switching when the set limit value is reached (switch S1)

Dangerous Failure Rate	λ_D	3.13 E-07 / h	**313 FIT**
Average Probability of Failure on Demand 1oo1	$PFD_{avg}(T_1)$	1.39 E-03	
Average Probability of Failure on Demand 1oo2	$PFD_{avg}(T_1)$	1.41 E-04	

Safe prewarning when the set limit value is reached (switch S2) - option

Dangerous Failure Rate	λ_D	3.13 E-07 / h	**313 FIT**
Average Probability of Failure on Demand 1oo1	$PFD_{avg}(T_1)$	1.39 E-03	
Average Probability of Failure on Demand 1oo2	$PFD_{avg}(T_1)$	1.41 E-04	

Assumptions for the calculations above: DC = 0 %, T_1 = 1 year, MRT = 72 h, β_{1oo2} = 10 %

High Demand Mode
In the opinion of the testing laboratory, the failure rates determined for the low demand mode can also be used for high demand mode applications up to a maximum demand rate of n_{op} = 12 / a. No failures due to wear are to be expected.

Origin of failure rates
The stated failure rates for low demand are the result of an FMEDA with tailored failure rates for the design and manufacturing process.
Furthermore the results have been verified by qualification tests and field-feedback data.
Failure rates include failures that occur at a random point in time and are due to degradation mechanisms such as ageing.
The stated failure rates do not release the end-user from collecting and evaluating application-specific reliability data.

Periodic Tests and Maintenance
The given values require periodic tests and maintenance as described in the Safety Manual.
The operator is responsible for the consideration of specific external conditions (e.g. ensuring of required quality of media, max. temperature, time of impact), and adequate test cycles.

Abb. 4: 968_V_1298_00_22_de_en_el_Seite_2

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.
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.

[(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.

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.

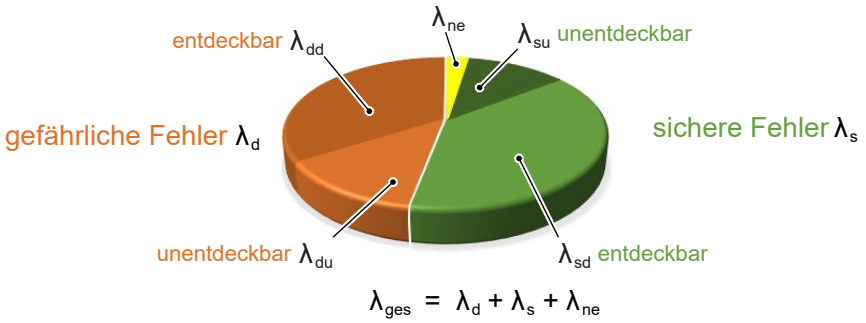


Abb. 5: Fehlerraten

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