developing solutions

FISCHER
MESS- UND REGELTECHNIK

TÜVRheinland CERTIFIED
www.tuv.com
ID 0600000000
IEC 61508
SIL

CE
RoHS III COMPLIANT
EAC

# Safety manual

## NK10

Fill Level Limiter

09015141 • SHB_EN_NK10 • Rev. ST4-C • 08/22

# Masthead

**Manufacturer:** **FISCHER Mess- und Regeltechnik GmbH**

Bielefelderstr. 37a
D-32107 Bad Salzuflen

Telephone: +49 5222 974 0
Telefax: +49 5222 7170

eMail: info@fischermesstechnik.de
web: www.fischermesstechnik.de

**Technical editorial team:** Documentation representative: T. Malischewski
Technical editor: R. Kleemann





## Version history

| | |
|---|---|
| Rev. ST4-A 11/18 | Version 1 (first edition) |
| Rev. ST4-B 01/21 | Version 2<br>(Correction scope of application: U no. omitted) |
| Rev. ST4-C 08/22 | Version 3 (new SIL certification) |

# Table of contents

# 1 Scope and standards

This document applies to the fill level limiter series NK10.

These safety fill level limiters have been certified by TÜV as per IEC 61508 (Parts 1-2 and 4-7:2010) for SIL1 and SIL2 (SIL 3 for redundant circuitry).

## 1.1 Standards

**Directives**

**Pressure Equipment Directive 2014/68/EC**
Item of equipment for use in a safety chain as a whole piece of equipment with category IV safety function

Applicable EC Directive:
**Low-Voltage Directive 2014/35/EU**

**Standards and rules applied:**

**EN 61508**
Functional safety of safety-related electrical/electronic/programmable electronic systems - (Parts 1-2 and 4-7)

**EN 61511**
Functional safety - safety systems for the process industry

**EN 61010-1**
Safety regulations for electrical measuring, control, regulating and laboratory devices - general requirements

**DIN 4754-3**
Heat transfer installations with organic heat transfer fluids - Part 3: Filling level safeguards

**EN 13445-1**
Unfuelled pressure container

## 1.2 Abbreviations

**SIL** *(en: Safety Integrity Level)*
Safety Integrity Level

The international standard IEC 61508 defines four discreet safety requirement levels (SIL 1 to SIL 4). Each level corresponds to a probability range for the failure of a safety function. The higher the level of the safety system is, the lower is the probability that it will fail to perform the required safety function.

**HFT** *(en: Hardware Failure Tolerance)*
Hardware Failure Tolerance

Ability of a function unit to continue performing a particular function if faults or irregularities arise.

**MTBF** *(en: Mean Time Between Failures)*

Mean operating duration between two failures.

**MTTR** *(en: Mean Time To Repair)*

Average time between the occurrence of a failure in a device or system and its repair.

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

Probability of dangerous failures of a safety function on demand.

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

Average probability of dangerous failures of a safety function on demand.

**PFH** *(en: Probability Failure per Hour)*

Average probability of a dangerous failure per hour.

**$\lambda_S$** *(en: Lambda Safe)*

Overall rate of all safe failures.

**$\lambda_{DD}$** *(en: Lambda Dangerous Detected failures)*

Overall rate for dangerous, detected failures.

**$\lambda_{DU}$** *(en: Lambda Dangerous Undetected failures)*

Overall rate for dangerous, undetected failures.

**DC** *(en: Diagnostic Coverage)*

The diagnosis coverage level is a unit for the detection of potential errors by means of tests.

**SFF** *(en: Safe Failure Fraction)*
Safe Failure Fraction

Proportion of safe failures in the total number of possible failures that put the safety-related system in a dangerous or impermissible functional status.

**FIT** *(en: Failure In Time)*
Failure In Time

Number of failures within $10^9$ hours.

**T1** *(en: Test Interval)*

Inspection intervals for the protective function.

**XooY** *(en: X out of Y))*
Selection Circuit:

Classification and description of safety-related systems with regard to redundancy and applied selection procedures.

X Indicates the frequency with which the safety function was engaged (redundancy).

Y Determines the number of channels that must operate correctly.

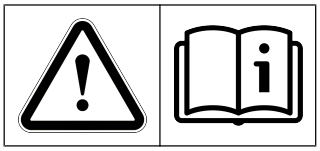
**LDM** *(en: Low Demand Mode)*

Mode of operation in which the demand rate to the safety system is not greater than once annually and not greater than twice the frequency of the repeat test.

**HDM** *(en: High Demand Mode)*

Mode of operation in which the demand rate to the safety system is greater than once annually or greater than twice the frequency of the repeat test.

## 1.3 Other applicable documents



Operating instructions and data sheets contain important safety instructions and technical data essential for safe operation.

The documents apply in the current version, which is available on the website www.fischermesstechnik.de.

| | | |
|---|---|---|
| Data sheet standard | 09005238 | DB_DE_NK10 |
| Data sheet ATEX | 09005535 | DB_DE_NK10_H |
| Operating manual standard | 09005016 | BA_DE_NK10 |
| Operating manual ATEX | 09005110 | BA_DE_NK10_H |

# 2 Description of the Device and Field of Application

## 2.1 Design and safety function

The swim system of the fill level limiter is contained in the fluid-filled reservoir (expansion tank). The swimming motions generated by changes in the fill level are transmitted directly to a switch by a swimmer rod sealed in a stainless-steel bellows. The fulcrum of the swimmer rod is located outside of the pressure chamber.

There is a test button outside the pressure chamber with which a function check as per DIN 4754-3 can be made without lowering the fill level. When pressed, the body of the swimmer is moved against its buoyancy.

The factory default switching point of switch S1 (clamps 1, 2, 3) is set so that it switches when the swimmer rod is horizontal. The optional warning switch S2 switches ca. 2.5 mm before S1.

The safety function is defined as:

1. Safe switching when the set limit value is reached (switch S1)
2. Safe pre-warning when the set limit value is reached (switch S2) - option

The switching contacts of the fill level limiter must be monitored by a suitable higher-order safety system as per IN EN 61508.

In a single-channel architecture (1oo1), devices up to SIL 2 can be used. In a multi-channel redundant architecture (1oo2), use up to SIL 3 is possible.

## 2.2 Function diagram

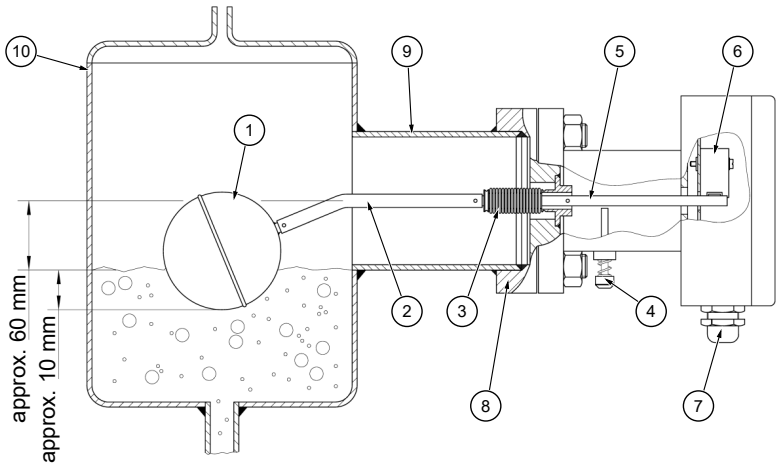



*Fig. 1:* Function diagram

| | | | |
|---|---|---|---|
| 1 | Swimmer | 2 | Swimmer rod |
| 3 | Metal bellows | 4 | Test button |
| 5 | Switch lever | 6 | Micro-switch S1 |
| 7 | Cable screw connection | 8 | Flange and counter-flange |
| 9 | Welding socket | 10 | Tank |

# 3 Notes on Planning

The fill level limiters are intended for a mode of operation with a low demand rate up to SIL 2.

Use as a safety-relevant subsystem in a mode of operation with low or high demand rate is possible up to SIL 3 in a multi-channel, redundant architecture.

## 3.1 Wiring diagram for SIL applications

The switching contacts of the level limiter must be monitored by a suitable higher-order device as per EN 61508 in order to achieve the required diagnostic coverage (DC).

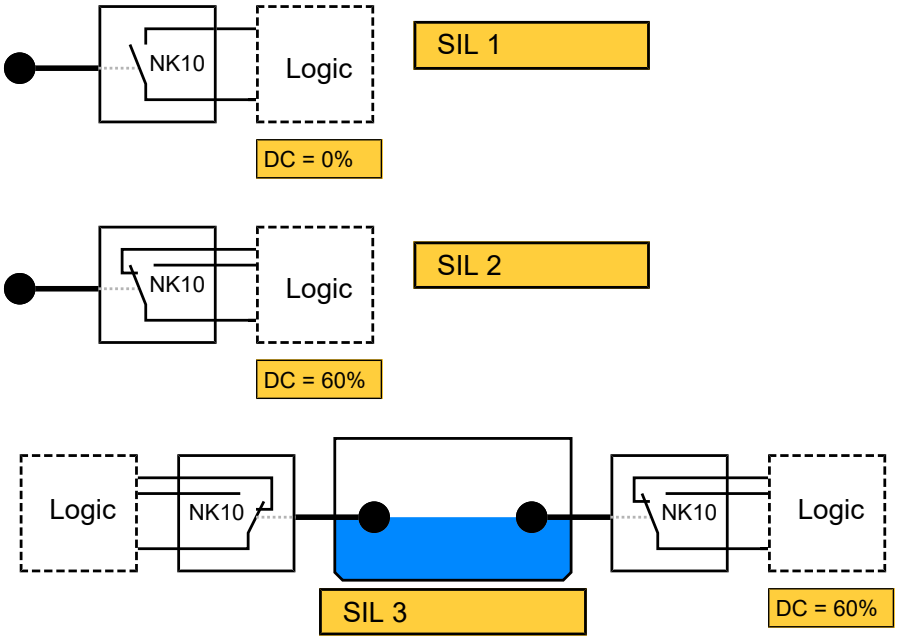



*Fig. 2:* Connection diagram SIL

## 3.2 Maintenance and Repeat Tests

Please also note the data in the attached operating instructions.

The PFD values given in the SIL manufacturer's declaration apply to inspection intervals of T1 = 1 year. The function test of the fill level limiter therefore needs to be carried out in the application every year.

**CAUTION! Observe the system safety and operating regulations.**

The instrument is maintenance-free. However, to ensure the device's reliable operation and long service life, we recommend regularly inspecting the device for the following points:

- Check the switching function (with the aid of the test button) in combination with the following components.
- Check the seal tightness of the flange connection.
- Check the electrical connections (cable clamp connection).

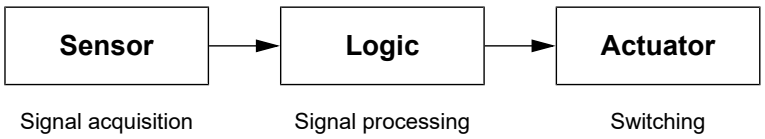
The test must be carried out once a year or more frequently depending on the operating regulations and must be documented in writing.

The exact test cycles need to be adapted to the operating and environmental conditions. If several components of the unit interact, all operating instructions of the other units also need to be observed.

All defective or faulty devices should be sent directly to our repair department. Please coordinate all shipments with our sales department. Return the device in the original packaging or a suitable transport container.

## 3.3 Safety coefficients

SIL 1/2 or SIL 3 can only be achieved with the level limiter NK10 (as sensor) in combination with a safety-related higher-order device (logic) as defined by EN 61508.




- The NK10 has no integrated diagnostics. If a diagnosis of the safety function is required, this must be provided by external measures as part of the overall safety-related system. The specified failure rates for DC=60% are guide values in connection with the evaluation logic and must be calculated for the specific system.
- 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 12 times per year to calculate the PFH. Up to this requirement rate, no errors that can be traced back to wear and tear are expected.

$$PFH = \lambda_d$$

| | |
|---|---|
| Dev. type | A |
| Operation mode | LDM (Low Demand Mode) |
| Hardware fault tolerance | HFT 0 |
| Systematic capability | SC 3 |
| Inspection intervals | $T_1$=1 year |
| Lifetime | 10000 switching cycles or 15 years |

| **Architecture 1oo1** | | | |
|---|---|---|---|
| Diagnostic coverage | DC | 0 | 60 |
| Error rate | $\lambda_{du}$ | 3.13 * $10^{-7}$ 1/h (313 FIT) | 1.25 * $10^{-7}$ 1/h (125 FIT) |
| Failure rate Low Demand Mode | $PFD_{avg}$ | 1.39 * $10^{-3}$ | 5.50 * $10^{-4}$ |
| Failure rates High Demand Mode | PFH | 3.13 * $10^{-7}$ 1/h | 1.25 * $10^{-7}$ 1/h |

| **Architecture 1oo2** | | | |
|---|---|---|---|
| Diagnostic coverage | DC | 0 | 60 |
| Error rate | $\lambda_{du}$ | 3.13 * $10^{-7}$ 1/h (313 FIT) | 1.25 * $10^{-7}$ 1/h (125 FIT) |
| Failure rate Low Demand Mode | $PFD_{avg}$ | 1.41 * $10^{-4}$ | 5.55 * $10^{-5}$ |
| Failure rates High Demand Mode | PFH | 3.20 * $10^{-8}$ 1/h | 1.26 * $10^{-8}$ 1/h |

# 4 SIL Certificate

## Certificate

SIL/PL Capability

TÜVRheinland® CERTIFIED

www.tuv.com
ID 0600000000

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

| | | | |
|---|---|---|---|
| **Prüfgegenstand**<br>**Product tested** | Füllstandsbegrenzer<br>Level Limiter | **Zertifikats-inhaber**<br>**Certificate holder** | Fischer Mess- und Regelungstechnik GmbH<br>Bielefelder Str. 37a<br>32107 Bad Salzuflen<br>Germany |
| **Typbezeichnung**<br>**Type designation** | NK10 / NK10 H | | |
| **Prüfgrundlagen**<br>**Codes and standards** | IEC 61508 Parts 1-2 and 4-7:2010 | | |
| **Bestimmungsgemäße Verwendung**<br>**Intended application** | Sicherheitsfunktion 1: Sicheres Schalten bei Erreichen des eingestellten Grenzwertes (Schalter S1)<br>Sicherheitsfunktion 2: Sichere Vorwarnung bei Erreichen des eingestellten Grenzwertes (Schalter S2) - Option<br>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.<br>Safety function 1: safe switching when the set limit value is reached (switch S1)<br>Safety function 2: safe pre-warning when the set limit value is reached (switch S2) - option.<br>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**<br>**Specific requirements** | Die Hinweise in der zugehörigen Installations- und Betriebsanleitung sowie des Sicherheitshandbuchs sind zu beachten.<br>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.



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

*Fig. 3:* 968_V_1298_00_22_de_en_el_page_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 | $\lambda_D$ | 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 | $\lambda_D$ | 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, $\beta_{1oo2}$ = 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.

TP-4800; Rev. 5.0 TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany

*Fig. 4:* 968_V_1298_00_22_de_en_el_page_2

# 5 Attachments

## 5.1 Glossary

| Fig. (↓A Z) | Definition |
|---|---|
| **β** | *(en)* **Common Cause Factor**<br>*(de)* Beta-Faktor<br>Proportionality factor between the CCF rate (failure due to a common cause) and the dangerous failure rate of the individual channel. |
| **DC** | *(en)* **Diagnostic Coverage Factor**<br>*(de)* Diagnosedeckungsgrad<br>The DC parameter shows the ratio of the number of detected dangerous failures ($\lambda_{DD}$) to the total number of dangerous failures ($\lambda_D$) an.<br>$DC = \frac{\sum \text{Known dangerous error}}{\sum \text{Total dangerous error}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$ |
| **FIT** | *(en)* **Failure in Time**<br>*(de)* Ausfälle pro Zeit<br>Failure rate with respect to the time interval $10^9$ hours.<br>$1\ FIT = 1 \times 10^{-9} \frac{1}{h}$ |
| **FMEDA** | *(en)* **Failure Mode Effect and Diagnostic Analysis**<br>*(de)* Gefährdung und Risikoanalyse<br>Procedure to determine causes of failures and their impact on the system. |
| **HDM** | *(en)* **High Demand Mode**<br>*(de)* Betriebsart mit hoher Anforderungsstufe<br>Operating mode with high or continuous demand on the safety function. The demand rate to the safety system is greater than once annually. |
| **HFT** | *(en)* **Hardware Fault Tolerance**<br>*(de)* Hardware-Fehlertoleranz<br>The hardware fault tolerance states how many dangerous failures are possible due to the architecture without endangering the execution of the safety function.<br>• HFT = 0<br>The occurrence of a dangerous failure will lead to a failure of the safety function.<br>• HFT = 1<br>Only the occurrence of two dangerous failures will lead to a failure of the safety function. |
| **LDM** | *(en)* **Low Demand Mode**<br>*(de)* Betriebsart mit niedriger Anforderungsstufe |

| | |
|---|---|
| | The safety function will only be carried out on demand to bring the system into a defined safe state. The frequency of requirements does not exceed one a year. |
| **MooN** | *(en)* **Architecture with M out of N channels**<br>*(de)* Systemarchitektur mit M aus N Kanälen |
| | System architecture MooN with the variables M and N:<br>Classification and description of safety-related systems with regard to redundancy and applied selection procedures.<br>• N - is the total number of redundant channels of a safety-related architecture and/or safety circuit.<br>• M - determines the number of channels that must operate correctly to carry out the safety function. |
| **MTBF** | *(en)* **Mean Time Between Failures**<br>*(de)* Mittlere Brauchbarkeitsdauer |
| | Mean operating duration between two failures. |
| **$MTTF_d$** | *(en)* **Mean Time To Dangerous Failures**<br>*(de)* Mittlere Zeit bis zum gefahrbringenden Ausfall |
| | Operating duration up to a dangerous fault. |
| **MRT** | *(en)* **Mean Repair Time**<br>*(de)* Mittlere Reparaturdauer |
| | Mean time for the repair. |
| **MTTR** | *(en)* **Mean Time To Repair**<br>*(de)* Mittlere Instandsetzungszeit |
| | Average time between the occurrence of a failure and restoration of the system. |
| **PFD** | *(en)* **Probability of Failure on Demand**<br>*(de)* Wahrscheinlichkeit einer Fehlfunktion im Anforderungsfall |
| | Probability of a dangerous failure on demand of the safety function for an operating mode with a low demand rate. |
| **PFH** | *(en)* **Probability of a dangerous Failure per Hour**<br>*(de)* Ausfallwahrscheinlichkeit pro Stunde für die Sicherheitsfunktion |
| | Frequency of a dangerous failure of the safety function for an operating mode with a high or continuous demand rate (high demand). |
| **PFS** | *(en)* **Probability of Failure Spurious**<br>*(de)* Ausfallwahrscheinlichkeit aufgrund einer nicht beabsichtigten Prozessabschaltung |
| | Frequency of failure due to a false alarm that leads to an unintentional process shutdown by the safety system. The smaller the value, the higher the system availability. |
| **SC** | *(en)* **systematic capability**<br>*(de)* systematische Eignung |

| | |
|---|---|
| | Measure of confidence (expressed on a scale of SC 1 to SC 4) that an item's systematic safety integrity meets the requirements of the stated SIL for the designated item safety function when the item is specified in accordance with the compliant item safety manual for the item instructions is applied. |
| **SFF** | *(en)* **Safe Failure Fraction**<br>*(de)* Anteil der ungefährlichen Ausfälle |
| | Resulting from the rate of safe errors plus the diagnosed or detected errors in relation to the system's total failure rate.[(1)] |
| **SIF** | *(en)* **Safety Instrumented Function**<br>*(de)* Sicherheitstechnische Funktion |
| | The safety function (SIF) is a protective measure that is only activated in the event of an incident to prevent injuries, damage and pollution. |
| **SIL** | *(en)* **Safety Integrity Level**<br>*(de)* Sicherheits-Integritätslevel |
| | One of four discrete levels to assess the requirements relating to the reliability of the safety functions in safety systems. SIL 4 is the highest and SIL 1 the lowest safety integrity level. Each level corresponds to a probability range for the failure of a safety function. |
| **SIS** | *(en)* **Safety Instrumented System**<br>*(de)* Sicherheitstechnisches-System |
| | Safety system for performance of one or several safety functions. A system of this kind comprises at least a sensor, an overriding safety control system and an actuator. |
| **$T_1$** | *(en)* **Proof Test Interval**<br>*(de)* Prüfintervall |
| | The safety system must always be in a state that guarantees the defined safety integrity. The proof test is carried out to confirm this. The test interval states the intervals in which a proof test needs to be carried out to guarantee the safety function. |

## 5.2 Failure rates

The error rates differ in principle as follows:

1. Safe failures
2. Dangerous failures
3. No effect failure

The first two types of errors are further divided into detectable and undetectable errors.

The failure without effect and the safe failures, whether detected or undetected, have no influence on the safety function. On the other hand, dangerous errors lead to a dangerous state of the system. The following diagram provides an overview.

[(1)] Due to the lack of diagnosis and negligible number of errors in mechanical components, the method can only be used to a limited extent for valves, drives and other mechanical components. It is therefore the responsibility of the end user to ensure an appropriate SFF through suitable diagnostic measures and intrinsically safe construction.

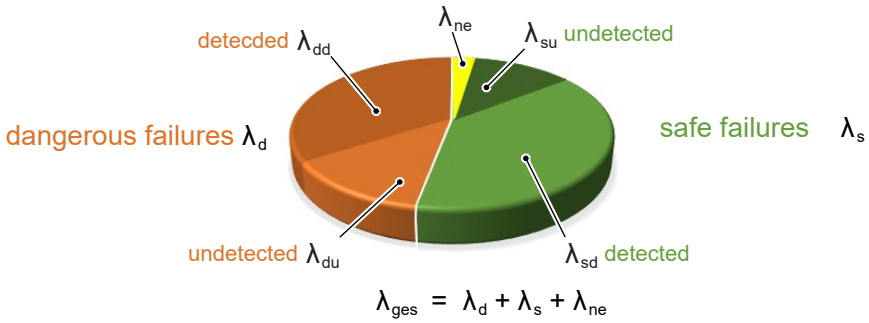



*Fig. 5:* Failure rates

| | |
|---|---|
| $\lambda_d$ | **Dangerous failure rate** |
| $\lambda_{dd}$ | **Dangerous detected failure rate** |
| $\lambda_{du}$ | **Dangerous undetected failure rate** |
| $\lambda_s$ | **Safe failure rate** |
| $\lambda_{sd}$ | **Safe detected failure rate** |
| $\lambda_{su}$ | **Safe undetected failure rate** |
| $\lambda_{ne}$ | **No effect failure rate** |

## 5.3 Unit types

**Type A** — **Simple operating equipment**

Type A units are 'simple' units for which the failure behaviour of all parts used and the behaviour under failure conditions is completely known.

This includes e.g. relays, resistors and transistors, however no complex electronic parts, e.g. microcontrollers.

**Type B** — **Complex operating equipment**

Type B units are 'complex' units for which the failure behaviour of all parts used and the behaviour under failure conditions is not completely known.

These units contain electronic parts such as microcontrollers, microprocessors or ASICs. In these parts and, in particular for software-controlled functions, it is difficult to fully determine all failures.

## 5.4 Pictogram explanation

**⚠ DANGER**

**Type and source of danger**

This indicates a **direct** dangerous situation that could lead to death or **serious injury** (highest danger level).

1. Avoid danger by observing the valid safety regulations.

**⚠ WARNING**

**Type and source of danger**

This indicates a **potentially** dangerous situation that could lead to death or **serious injury** (medium danger level).

1. Avoid danger by observing the valid safety regulations.

**⚠ CAUTION**

**Type and source of danger**

This indicates a **potentially** dangerous situation that could lead to slight or serious injury, damage or **environmental pollution** (low danger level).

1. Avoid danger by observing the valid safety regulations.

**NOTICE**

**Note / advice**

This indicates useful information of advice for efficient and smooth operation.

## Notes

## Notes

## Notes

**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