developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL

CE

RoHS III
COMPLIANT

EAC

Safety manual

NK10

Fill Level Limiter

09015141 • SHB_EN_NK10 • Rev. ST4-B • 01/21

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 the German inspection authority TÜV Süd under EN 61508 for SIL1 and SIL2 (SIL3 for redundant circuitry).

1.1 Standards

Directives

Pressure Equipment Directive 2014/68/EU
Item 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

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: Fill level sensors

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 *(eng: Mean Time Between Failures)*

Mean operating duration between two failures.

MTTR *(eng: Mean Time To Repair)*

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

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

Probability of dangerous failures of a safety function on demand.

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

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

λ_S *(eng: Lambda Safe)*

Overall rate of all safe failures.

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

Overall rate for dangerous, detected failures.

λ_{DU} *(eng: 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)*

Proportion of failures that do not have the potential to place the safety system in a dangerous or impermissible functional status.

FIT *(en: 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))*

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

X 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.

1.3 Other applicable documents

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.

In a single-channel architecture (1oo1), devices up to SIL 2 can be used. In a multi-channel redundant architecture, use up to SIL 3 is possible. The switching contacts of the fill level limiter must be monitored by a suitable higher-order safety system as a 1oo2 system as per DIN EN 61508.

2.2 Function diagram

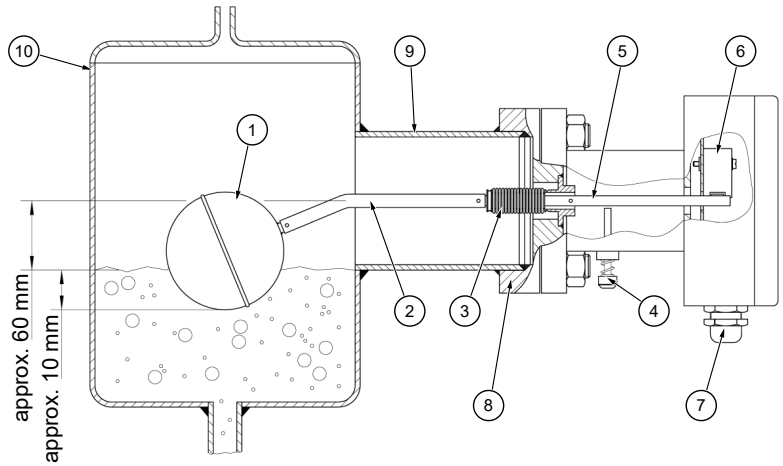

Fig. 1: Function diagram

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

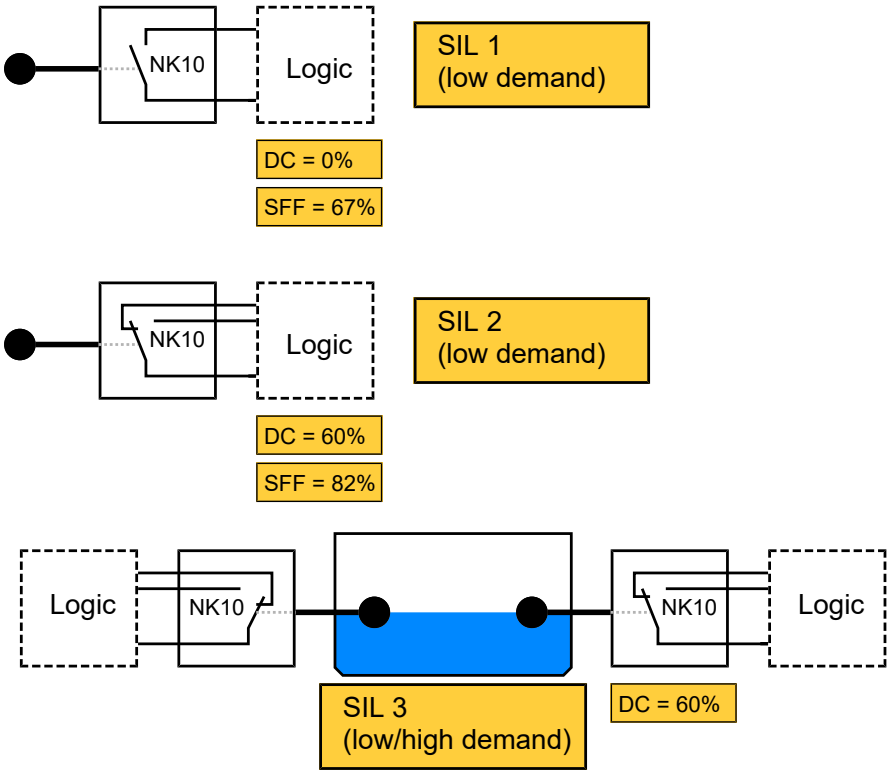

Fig. 2: Connection diagram SIL

3.2 Maintenance and Repeat Tests

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. We recommend the following regular inspection to guarantee reliable operation and a long service life:

- 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 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.

3.3 Safety coefficients

NOTICE! SIL 2 and/or SIL 3 are achieved with the fill level limiter as a sensor in combination with an external logic or PLC.

	SIL 1	SIL 2	SIL 3
Equipment type	A	A	A
Operating mode	LOW	LOW	LOW/HIGH
Inspection intervals	1 year	1 year	1 year
Service life	100000 switching cycles, 15 years	100000 switching cycles, 15 years	100000 switching cycles, 15 years
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 years	241 years	241 years

*) single-channel use

4 SIL Certificate

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

Product Service

CERTIFICATE

No. Z10 027632 0002 Rev. 01

Holder of Certificate: **FISCHER**
Mess- und Regeltechnik GmbH
Bielefelder Straße 37a
32107 Bad Salzuflen
GERMANY

Factory(ies): 027632

Certification Mark:

Product: **Level indicator**
Level Limiter

Model(s): **NK10**

Parameters: 1oo1 configuration: SIL 1/2
1oo2 configuration: SIL 3

Degree of protection: IP55
Rated output current
at 250Vac: 6A
at 250Vdc: 250mA

Tested according to: IEC 61508-1:2010
IEC 61508-2:2010

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: 717503460

Valid until: 2025-10-25

Date, 2020-10-26 (Claudio Gregorio)

A4 / 07.17

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

Fig. 3: SIL_IEC61508_DE_EN(1)Part1

5 Attachments

5.1 Glossary

Fig. (A Z)	Definition
β	**Common Cause Factor** Proportionality factor between the CCF rate (failure due to a common cause) and the dangerous failure rate of the individual channel.
DC	**Diagnostic Coverage Factor** The DC parameter shows the ratio of the number of detected dangerous failures (λ_{DD}) to the total number of dangerous failures (λ_D) an. $DC = \frac{\sum \text{dangerous detected failure}}{\sum \text{dangerous failure}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
FIT	**Failure in Time** Failure rate with respect to the time interval 10^9 hours. $1\ FIT = 1 \times 10^{-9} \frac{1}{h}$
FMEDA	**Failure Mode Effect and Diagnostic Analysis** Procedure to determine causes of failures and their impact on the system
HDM	**High Demand Mode** Operating mode with high or continuous demand on the safety function. The demand rate to the safety system is greater than once annually.
HFT	**Hardware Fault Tolerance** The hardware fault tolerance states how many dangerous failures are possible due to the architecture without endangering the execution of the safety function. • HFT = 0 The occurrence of a dangerous failure will lead to a failure of the safety function. • HFT = 1 Only the occurrence of two dangerous failures will lead to a failure of the safety function.
LDM	**Low Demand Mode** 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	**Architecture with M out of N channels** System architecture MooN with the variables M and N: Classification and description of safety-related systems with regard to redundancy and applied selection procedures. • N - is the total number of redundant channels of a safety-related architecture and/or safety circuit. • M - determines the number of channels that must operate correctly to carry out the safety function.
MTBF	**Mean Time Between Failures** Mean operating duration between two failures.
$MTTF_d$	**Mean Time To Dangerous Failures** Operating duration up to a dangerous fault.
MRT	**Mean Repair Time** Mean time for the repair.
MTTR	**Mean Time To Repair** Average time between the occurrence of a failure and restoration of the system.
PFD	**Probability of Failure on Demand** Probability of a dangerous failure on demand of the safety function for an operating mode with a low demand rate.
PFH	**Probability of a dangerous Failure per Hour** Frequency of a dangerous failure of the safety function for an operating mode with a high or continuous demand rate (high demand).
PFS	**Probability of Failure Spurious** 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.
SFF	**Safe Failure Fraction** This is determined by the rate of non-dangerous errors plus the diagnosed and/or recognised errors in ration to the overall failure rate of the system.
SIF	**Safety Instrumented Function** 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	**Safety Integrity Level** 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	**Safety Instrumented 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	**Proof Test Interval** 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.

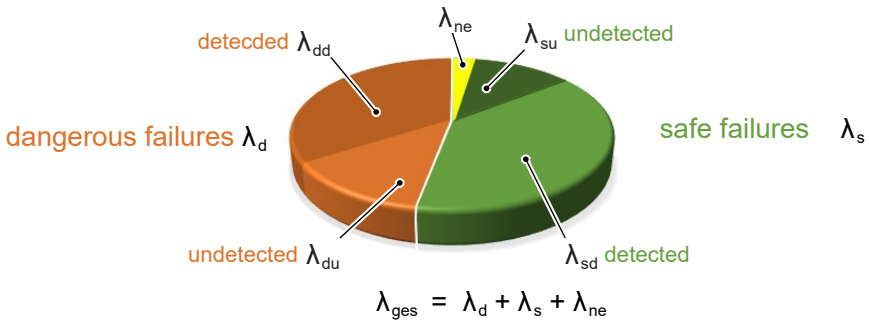

Fig. 4: Failure rates

λ_d	**Dangerous failure rate**
λ_{dd}	**Dangerous detected failure rate**
λ_{du}	**Dangerous undetected failure rate**
λ_s	**Safe failure rate**
λ_{sd}	**Safe detected failure rate**
λ_{su}	**Safe undetected failure rate**
λ_{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

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