SAFETY MANUAL SIL

SWITCH AMPLIFIER

KF**-SR2-(Ex)*(.LB),
KFD2-SR2-(Ex)2.2S

SIL
IEC 61508/61511

ISO9001

SIL2

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

1 Introduction

1.1 General Information

This manual contains information for application of the device in functional safety related loops.

The corresponding data sheets, the operating instructions, the system description, the Declaration of Conformity, the EC-Type-Examination Certificate and applicable Certificates (see data sheet) are integral parts of this document.

The documents mentioned are available from **www.pepperl-fuchs.com** or by contacting your local Pepperl+Fuchs representative.

Mounting, commissioning, operation, maintenance and dismounting of any devices may only be carried out by trained, qualified personnel. The instruction manual must be read and understood.

When it is not possible to correct faults, the devices must be taken out of service and action taken to protect against accidental use. Devices should only be repaired directly by the manufacturer. De-activating or bypassing safety functions or failure to follow the advice given in this manual (causing disturbances or impairment of safety functions) may cause damage to property, environment or persons for which Pepperl+Fuchs GmbH will not be liable.

The devices are developed, manufactured and tested according to the relevant safety standards. They must only be used for the applications described in the instructions and with specified environmental conditions, and only in connection with approved external devices.

1.2 Intended Use

KF-SR2-*.W**

These signal conditioners provide the isolation for non-intrinsically safe applications.

They transfer digital signals (NAMUR sensors/mechanical contacts) from the field to the control system.

The proximity sensor or switch controls a form C change-over contact for the load. The normal output state can be reversed using switch S1 for channel I and switch S2 for channel II in 2-channel versions.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

KF-SR2-Ex*.W**

These isolated barriers are used for intrinsic safety applications.

They transfer digital signals (NAMUR sensors/mechanical contacts) from a hazardous area to a safe area.

The proximity sensor or switch controls a form C change-over contact for the safe area load. The normal output state can be reversed using switch S1 for channel I and switch S2 for channel II in 2-channel versions.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

KF-SR2-1.W.LB**

These signal conditioners provide the isolation for non-intrinsically safe applications.

They transfer digital signals (NAMUR sensors/mechanical contacts) from the field to the control system.

The proximity sensor or switch controls a form C change-over contact for the load. The normal output state can be reversed using switch S1. Switch S2 allows output channel II to be switched between signal output and error message output. Switch S3 enables or disables line fault detection of the field circuit.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

KF-SR2-Ex1.W.LB**

These isolated barriers are used for intrinsic safety applications.

They transfer digital signals (NAMUR sensors/mechanical contacts) from a hazardous area to a safe area.

The proximity sensor or switch controls a form C change-over contact for the safe area load. The normal output state can be reversed using switch S1. Switch S2 allows output channel II to be switched between signal output and error message output. Switch S3 enables or disables line fault detection of the field circuit.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

KFD2-SR2-2.2S

This signal conditioner provides the isolation for non-intrinsically safe applications.

It transfers digital signals (NAMUR sensors/mechanical contacts) from the field to the control system.

The proximity sensor or switch controls two form A NO contacts for the load. The mode of operation can be reversed with switches S1 and S2. Line fault detection (LFD) can be selected or disabled via switch S3.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

KFD2-SR2-Ex2.2S

This isolated barrier is used for intrinsic safety applications.

It transfers digital signals (NAMUR sensors/mechanical contacts) from a hazardous area to a safe area.

The proximity sensor or switch controls two form A NO contacts for the safe area load. The mode of operation can be reversed with switches S1 and S2. Line fault detection (LFD) can be selected or disabled via switch S3.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

The devices are single device for DIN rail mounting.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

KF**-SR2-(Ex)*(.LB)
KFD2-SR2-(Ex)2.2S

Up to SIL2

The stars replace a combination of characters, depending on the product.

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 2, edition 2000:
  Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)
- Electromagnetic compatibility:
  - EN 61326-1:2006
  - NE 21:2006

System specific standards and directives

- Functional safety IEC 61511 part 1, edition 2003:
  Standard of functional safety: safety instrumented systems for the process industry sector (user)

2 Planning

2.1 System Structure

2.1.1 Low Demand Mode

If there are two loops, one for the standard operation and another one for the functional safety, then usually the demand rate for the safety loop is assumed to be less than once per year.

The relevant safety parameters to be verified are:

- the PFD_{avg} value (average **P**robability of **F**ailure on **D**emand) and T_{proof} (proof test interval that has a direct impact on the PFD_{avg})
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance architecture)

2.1.2 High Demand Mode

If there is only one loop, which combines the standard operation and safety related operation, then usually the demand rate for this loop is assumed to be higher than once per year.

The relevant safety parameters to be verified are:

- PFH (**P**robability of dangerous **F**ailure per **H**our)
- Fault reaction time of the safety system
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance architecture)

2.1.3 Safe Failure Fraction

The safe failure fraction describes the ratio of all safe failures and dangerous detected failures to the total failure rate.

$SFF = (\lambda_s + \lambda_{dd}) / (\lambda_s + \lambda_{dd} + \lambda_{du})$

A safe failure fraction as defined in EN 61508 is only relevant for elements or (sub)systems in a complete safety loop. The device under consideration is always part of a safety loop but is not regarded as a complete element or subsystem.

For calculating the SIL of a safety loop it is necessary to evaluate the safe failure fraction of elements, subsystems and the complete system, but not of a single device.

Nevertheless the SFF of the device is given in this document for reference.

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Only one input and one output are part of the considered safety function (only 2-channel version).
- Short circuit (SC) detection and lead breakage (LB) detection are activated.
- The collective error output which signals if the field wiring is broken or shorted is not considered in the FMEDA and the calculations.
- The device shall claim less than 10 % of the total failure budget for a SIL2 safety loop.
- For a SIL2 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (**S**afety **I**nstrumented **F**unction) should be smaller than 10^{-2}, hence the maximum allowable PFD_{avg} value would then be 10^{-3}.
- For a SIL2 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-6} per hour, hence the maximum allowable PFH value would then be 10^{-7} per hour.
- Failure rate based on the Siemens SN29500 data base.
- Failure rates are constant, wear out mechanisms are not included.
- External power supply failure rates are not included.
- The safety-related device is considered to be of type **B** components with a Hardware Fault Tolerance of **0**.
- The IEC 61511-1 section 11.4.4 allows devices to be used in applications one SIL higher than given by table 3 of IEC 61508-2, if the device is proven in use. The assessment and proven-in-use demonstration lead to the result that the device may be used in applications up to SIL2. However, it is the responsibility of the end-user to decide on applying proven-in-use devices.
- The application program in the safety logic solver is configured to detect underrange and overrange failures. Therefore these failures have been classified as **dangerous detected** failures.
- For the High Demand Mode of operation, a fault reaction time of 5 minutes must be tolerated by the process. In this case also regard the lifetime limitations of the output relays available in the data sheet of the device.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
  - IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 ºC. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 ºC, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours (e. g. remove sensor burnout).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (for example: substitution by an equivalent device).
- For the calculation it was also assumed that the indication of a dangerous error (via fault bus) would be detected within 1 hour by the logic solver (SPS).

2.3 Safety Function and Safe State

The safe state is defined as the outputs being low (de-energized).

Safety Function 1-channel Devices

KF-SR2-(Ex)1.W**	
S1 position I (normal operation)	In normal operation, the safe state is reached with NAMUR sensor input in off state.
S1 position II (inverse operation)	In inverse operation, the safe state is reached with NAMUR sensor input in on state.

KF-SR2-(Ex)1.W.LB**	
S1 position I (normal operation)	In normal operation, the safe state is reached with NAMUR sensor input in off state.
S1 position II (inverse operation)	In inverse operation, the safe state is reached with NAMUR sensor input in on state.
S2 position I (output II as signal output)	Output II has the same switching state like output I.
S2 position II (output II as error message output)	LB/SC output – de-energized in case of fault. Not for safety relevant application of output II.

Safety Function 2-channel Devices

KF-SR2-(Ex)2.****	
S1 position I (normal operation input channel I)	In normal operation, output I reaches the safe state with the NAMUR sensor input I in off state.
S1 position II (inverse operation input channel I)	In inverse operation, output I reaches the safe state with the NAMUR sensor input I in on state.
S2 position I (normal operation input channel II)	In normal operation, output II reaches the safe state with the NAMUR sensor input II in off state.
S2 position II (inverse operation input channel II)	In inverse operation, output II reaches the safe state with the NAMUR sensor input II in on state.

LB/SC Diagnosis

The input loop of all versions is supervised, if the line fault detection is active (mandatory, see data sheet) The line fault detection is activated if switch S3 is in position I. The related safety function is defined as the outputs are low/de-energized (safe state), if there is a line fault detected.

Note!

The failure outputs are not safety relevant.

Reaction Time

The reaction time for all safety functions is < 20 ms.

2.4 Characteristic Safety Values

KFD2-SR2-(Ex)*.W(.LB)

Parameters acc. to IEC 61508	Values
Assessment type and documentation	Full assessment
Device type	B
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL	2 (proven-in-use acc. to IEC 61511)
Safety function	One relay output of one channel
λ_s [1]	138.6 FIT
λ_d [1]	72.3 FIT
$\lambda_{\text{no effect}}$ [2]	76.6 FIT
$\lambda_{\text{total (safety function)}}$	288 FIT
$\lambda_{\text{no part}}$	62.7 FIT
SFF	74.86 %
MTBF [3]	325 years
PFH	2.85×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	3.17×10^{-4}
PFD_{avg} for T_{proof} = 2 years	6.33×10^{-4}
PFD_{avg} for T_{proof} = 5 years	1.58×10^{-3}
Reaction time [4]	< 20 ms

[1] "Not considered" failures are counted 50 % as safe failures and 50 % as dangerous failures as in the FMEDA report issued by exida.com.

[2] "No effect" failures are not influencing the safety functions and are therefore added to the λ_S.

[3] acc. to SN29500. This value includes failures which are not part of the safety function.

[4] Time between fault detection and fault reaction.

Table 2.1

KFA*-SR2-(Ex)*.W(.LB)

Parameters acc. to IEC 61508	Values
Assessment type and documentation	Full assessment
Device type	B
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL	2 (proven-in-use acc. to IEC 61511)
Safety function	One relay output of one channel
λ_s[1]	112.1 FIT
λ_d[1]	65.1 FIT
$\lambda_{\text{no effect}}$[2]	51.9 FIT
$\lambda_{\text{total (safety function)}}$	229 FIT
$\lambda_{\text{no part}}$	20.0 FIT
SFF	71.58 %
MTBF [3]	458 years
PFH	6.51×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	2.85×10^{-4}
PFD_{avg} for T_{proof} = 2 years	5.70×10^{-4}
PFD_{avg} for T_{proof} = 5 years	1.42×10^{-3}
Reaction time [4]	< 20 ms

[1] "Not considered" failures are counted 50 % as safe failures and 50 % as dangerous failures as in the FMEDA report issued by exida.com.

[2] "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[3] acc. to SN29500. This value includes failures which are not part of the safety function.

[4] Time between fault detection and fault reaction.

Table 2.2

KFD2-SR2-(Ex)2.2S

Parameters acc. to IEC 61508	Values
Assessment type and documentation	Full assessment
Device type	B
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL	2 (proven-in-use acc. to IEC 61511)
Safety function	One relay output of one channel
λ_s [1]	156 FIT
λ_d [1]	84.3 FIT
$\lambda_{\text{no effect}}$ [2]	86.3 FIT
$\lambda_{\text{total (safety function)}}$	327 FIT
$\lambda_{\text{no part}}$	66.4 FIT
SFF	74.18 %
MTBF [3]	290 years
PFH	8.43×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	3.70×10^{-4}
PFD_{avg} for T_{proof} = 2 years	7.39×10^{-4}
PFD_{avg} for T_{proof} = 5 years	1.85×10^{-3}
Reaction time [4]	< 20 ms

[1] "Not considered" failures are counted 50 % as safe failures and 50 % as dangerous failures as in the FMEDA report issued by exida.com.

[2] "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[3] acc. to SN29500. This value includes failures which are not part of the safety function.

[4] Time between fault detection and fault reaction.

Table 2.3

The characteristic safety values like PFD, SFF, HFT and T_{proof} are taken from the SIL report/FMEDA report. Please note, PFD and T_{proof} are related to each other.

The function of the devices has to be checked within the proof test interval (T_{proof}).

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces. For corresponding terminals see data sheet.

- Safety relevant interfaces:

KF**-SR2-(Ex)*(.LB)
KFD2-SR2-(Ex)2.2S

- Non-safety relevant interfaces: output ERR

3.2 Configuration

The device must be configured through the user accessible DIP switches for the required output function before the start-up. During the functionality any change of the operating function (DIP switch modification) can invalidate the safety function behavior and must be avoided.

The KF devices provide a suitable cover to protect against accidental changes.

3.3 Useful Life Time

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful life time of components is not exceeded. Beyond this useful life time, the result of the probabilistic calculation is meaningless as the probability of failure significantly increases with time. The useful life time is highly dependent on the component itself and its operating conditions – temperature in particular (for example, the electrolytic capacitors can be very sensitive to the working temperature).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful life time of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful life time is valid.

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 years.

Our experience has shown that the useful life time of a Pepperl+Fuchs product can be higher

- if there are no components with reduced life time in the safety path (like electrolytic capacitors, relays, flash memory, opto coupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful life time refers to the (constant) failure rate of the device. The effective life time can be higher.

3.4 Installation and Commissioning

Installation has to consider all aspects regarding the SIL level of the loop. During installation or replacement of the device the loop has to shut down. Devices have to be replaced by the same type of devices.

4 Proof Test

4.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous fails that are otherwise not detected by diagnostic test.

The functionality of the subsystem must be verified at periodic intervals depending on the applied PFD_{avg} in accordance with the data provided in this manual. See chapter 2.4.

It is under the responsibility of the operator to define the type of proof test and the interval time period.

The ancillary equipment required:

- Digital multimeter with an accuracy better than 0.1 %
  For the proof test of the intrinsic safety side of the devices, a special digital multimeter for intrinsic safety circuits must be used. Intrinsic safety circuits that were operated with circuits of other types of protection may not be used as intrinsically safe circuits afterwards.
- Power supply set at nominal voltage of 24 V DC

The settings have to be verified after the configuration by means of suitable tests.

Procedure:

Sensor state must be simulated by a potentiometer of 4.7 kΩ (threshold for normal operation), by a resistor of 220 Ω (short circuit detection) and by a resistor of 150 kΩ (lead breakage detection).

The input test needs to be done for each input channel individually. The threshold must be between 1.4 mA and 1.9 mA, the hysteresis must be between 170 µA and 250 µA. The input test must be done on the connector that is used in the application.

- For normal mode of operation the relay must be activated (yellow LED on), if the input current is above the threshold.
- For inverse mode of operation the relay must be activated (yellow LED on), if the input current is below the threshold.

If the resistor R_{SC} (220 Ω) or the resistor R_{LB} (150 kΩ) is connected to the input, the unit must detect an external error. The red LED shall be flashing and the relay of the corresponding channel shall de-activate.

All relay outputs of a device need to be tested with a certain current, i. e. 100 mA. To avoid any electrical shock problems, we recommend to use 24 V DC for this test. For the philosophy of Functional Safety it is important to test, that the relay contacts are **definitely open**, if the relay is de-activated.

After the test the unit needs to be set back to the original settings for the current application. Furthermore the switches for the settings need to be saved against undeliberate changes. This can be achieved by fixing the label flap.

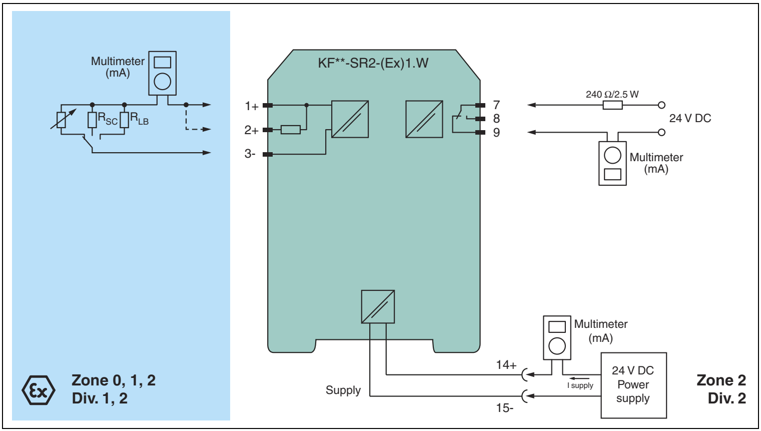

Figure 4.1 Proof test set-up for KF**-SR2-(Ex)1.W

Usage in Zone 0, 1, 2/Div. 1, 2 only for KF**-SR2-Ex1.W.

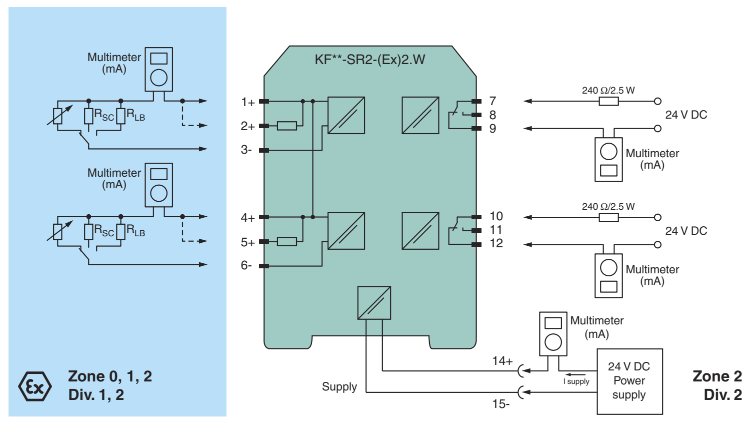

Figure 4.2 Proof test set-up for KF**-SR2-(Ex)2.W

Usage in Zone 0, 1, 2/Div. 1, 2 only for KF**-SR2-Ex2.W.

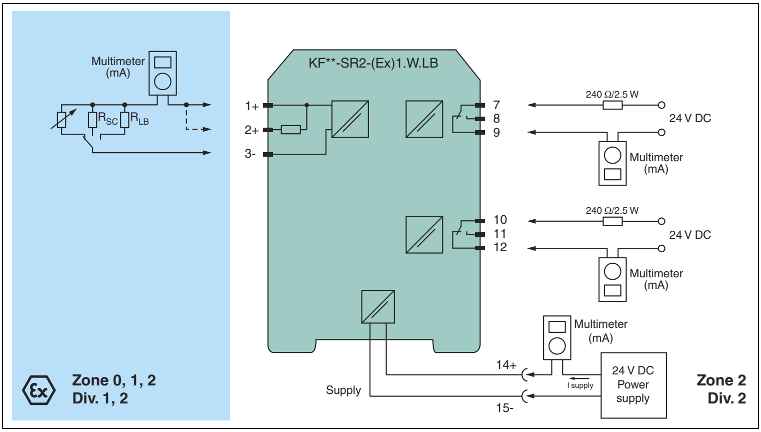

Figure 4.3 Proof test set-up for KF**-SR2-(Ex)1.W.LB

Usage in Zone 0, 1, 2/Div. 1, 2 only for KF**-SR2-Ex1.W.LB.

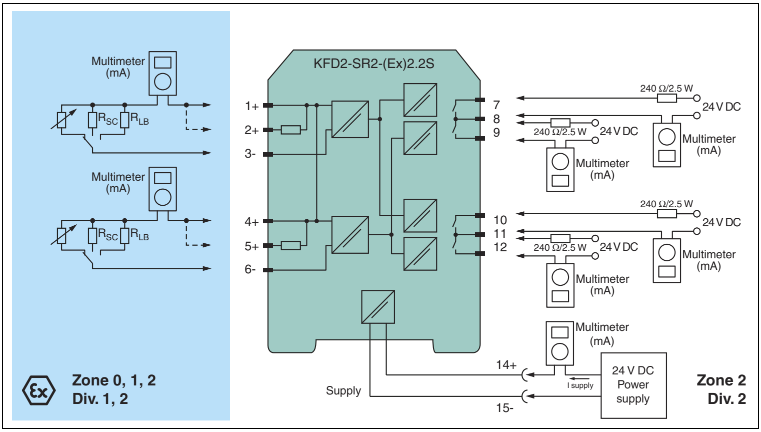

Figure 4.4 Proof test set-up for KFD2-SR2-(Ex)2.2S

Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD2-SR2-Ex2.2S.

5 Abbreviations

FIT	**F**ailure **I**n **T**ime
FMEDA	**F**ailure **M**ode, **E**ffects and **D**iagnostics **A**nalysis
λ_s	Probability of safe failure
λ_d	Probability of dangerous failure
$\lambda_{\text{no effect}}$	Probability of failures of components in the safety path that have no effect on the safety function
$\lambda_{\text{not part}}$	Probability of failure of components that are not in the safety path
$\lambda_{\text{total (safety function)}}$	Safety function
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
MTTR	**M**ean **T**ime **T**o **R**epair
$\mathbf{PFD_{avg}}$	Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
PTC	**P**roof **T**est **C**overage
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIS	**S**afety **I**nstrumented **S**ystem
$\mathbf{T_{proof}}$	Proof Test Interval
ERR	Error
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

For the Pepperl+Fuchs representative
closest to you check www.pepperl-fuchs.com/pfcontact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

Subject to modifications