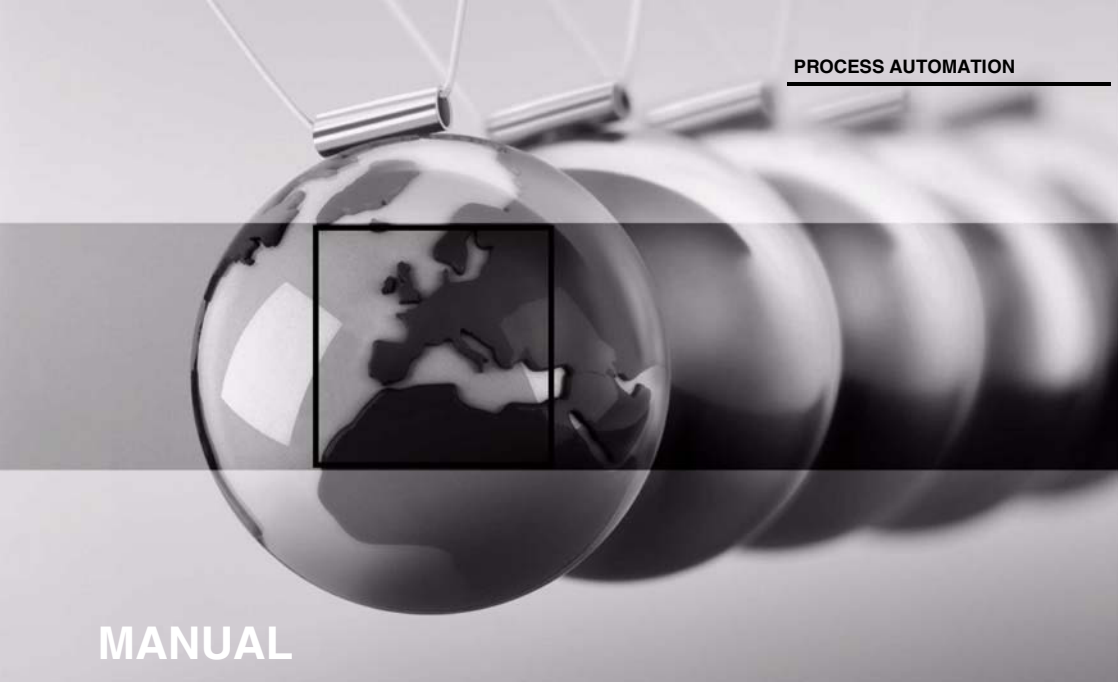

MANUAL

Functional Safety

Switch Amplifier

KFD2-SOT3-Ex*(.LB)(.IO)(-Y1), KFD2-ST3-Ex*(.LB)

SIL

IEC 61508/61511

ISO9001

CE

SIL 2

PEPPERL+FUCHS

PROTECTING YOUR PROCESS

With regard to the supply of products, the current issue of the following document is applicable: The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship"

2016-03

1 Introduction

1.1 Contents

This document contains information for usage of the device in functional safety-related applications. You need this information to use your product throughout the applicable stages of the product life cycle. These can include the following:

- Product identification
- Delivery, transport, and storage
- Mounting and installation
- Commissioning and operation
- Maintenance and repair
- Troubleshooting
- Dismounting
- Disposal

Note!

This document does not substitute the instruction manual.

Note!

For full information on the product, refer to the instruction manual and further documentation on the Internet at www.pepperl-fuchs.com.

The documentation consists of the following parts:

- Present document
- Instruction manual
- Manual
- Datasheet

Additionally, the following parts may belong to the documentation, if applicable:

- EC-type of examination
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- FMEDA report
- Assessment report
- Additional documents

For more information about functional safety products from Pepperl+Fuchs see www.pepperl-fuchs.com/sil.

1.2 Safety Information

Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismounting lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismounting of the product. The personnel must have read and understood the instruction manual and the further documentation.

Intended Use

The device is only approved for appropriate and intended use. Ignoring these instructions will void any warranty and absolve the manufacturer from any liability.

The device is developed, manufactured and tested according to the relevant safety standards.

Use the device only

- for the application described
- with specified environmental conditions
- with devices that are suitable for this safety application

Improper Use

Protection of the personnel and the plant is not ensured if the device is not used according to its intended use.

1.3 Symbols Used

This document contains symbols for the identification of warning messages and of informative messages.

Warning Messages

You will find warning messages, whenever dangers may arise from your actions. It is mandatory that you observe these warning messages for your personal safety and in order to avoid property damage.

Depending on the risk level, the warning messages are displayed in descending order as follows:

Danger!
This symbol indicates an imminent danger.

Non-observance will result in personal injury or death.

Warning!
This symbol indicates a possible fault or danger.

Non-observance may cause personal injury or serious property damage.

Caution!
This symbol indicates a possible fault.

Non-observance could interrupt the device and any connected systems and plants, or result in their complete failure.

Informative Symbols

Note!
This symbol brings important information to your attention.

Action

This symbol indicates a paragraph with instructions. You are prompted to perform an action or a sequence of actions.

2 Product Description

2.1 Function

General

This isolated barrier is used for intrinsic safety applications.

The device transfers digital signals (NAMUR sensors or dry contacts) from a hazardous area to a safe area.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

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

If the device is operated via Power Rail, additionally a collective error message is available.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

IO Versions

The outputs are galvanically isolated from each other.

KFD2-SOT3-Ex1.LB(.IO)

The input controls two passive transistor outputs.

During an error condition, the transistors revert to its de-energized state.

Via switch the function of the second output can be defined as a signal output or a fault indication output.

KFD2-SOT3-Ex2(.IO)(-Y1)

Each input controls a passive transistor output.

During an error condition, the transistors revert to its de-energized state.

KFD2-ST3-Ex1.LB

The input controls two active transistor outputs.

During an error condition, the transistors revert to its de-energized state.

Via switch the function of the second output can be defined as a signal output or a fault indication output.

KFD2-ST3-Ex2

Each input controls an active transistor output.

During an error condition, the transistors revert to its de-energized state.

2.2 Interfaces

The device has the following interfaces:

- Safety relevant interfaces:
  - KFD2-SOT3-Ex1.LB(.IO), KFD2-ST3-Ex1.LB: input I, output I, output II
  - KFD2-SOT3-Ex2(.IO)(-Y1), KFD2-ST3-Ex2: input I, input II, output I, output II
- Non-safety relevant interfaces: fault indication output and collective error message output

Note!

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs GmbH Lilienthalstraße 200, 68307 Mannheim, Germany

KFD2-SOT3-Ex1.LB, KFD2-SOT3-Ex1.LB.IO, KFD2-SOT3-Ex2, KFD2-SOT3-Ex2.IO, KFD2-SOT3-Ex2.IO-Y1	Up to SIL 2
KFD2-ST3-Ex1.LB, KFD2-ST3-Ex2	

2.4 Standards and Directives for Functional Safety

Device specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 7, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1 – 3, edition 2003: Functional safety – Safety instrumented systems for the process industry sector (user)

3 Planning

3.1 System Structure

3.1.1 Low Demand Mode of Operation

If there are two control 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 dangerous **F**ailure on **D**emand) and the T_1 value (proof test interval that has a direct impact on the PFD_{avg} value)
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.2 High Demand or Continuous Mode of Operation

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

The relevant safety parameters to be verified are:

- the PFH value (**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)

3.1.3 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 IEC/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.

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rate based on the Siemens standard SN29500.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- The device will be used under average industrial ambient conditions, which are comparable with the classification "stationary mounted" in MIL-HDBK-217F. Alternatively, the following ambient conditions are assumed:
  - IEC/EN 60654-1 Class C (sheltered location) with temperature limits in the range of the manufacturer's specifications and an average temperature of 40 °C over a long period. The humidity level is within manufacturer's rating. For a higher average temperature of 60 °C, the failure rates must be multiplied by a factor of 2.5 based on experience. A similar factor must be used if frequent temperature fluctuations are expected.
- The indication of a dangerous failure (via fault bus) is detected within 1 hour by the programmable logic controller (PLC).
- The fault indication output which signals if the field circuits are broken or shorted is not considered in the FMEDA and the calculations.

SIL 2 application

- The device shall claim less than 10 % of the total failure budget for a SIL 2 safety loop.
- For a SIL 2 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 SIL 2 application operating in high demand mode 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.
- The safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- Since the safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 60 % according to table 2 of IEC/EN 61508-2 for a SIL 2 (sub) system.

2016-03

3.3 Safety Function and Safe State

Safe State

The safe state of output I and output II is the high impedant state.

The high impedant state shows an open circuit on the output.

Safety Function

The safety function has two modes of operation:

- normal operation (output follows input)
- inverted operation (output inverts input)

The 1-channel devices have two outputs where output II may be used in safety relevant applications if it is configured to follow output I.

Do not use the outputs of the device in the same safety function, since the outputs use common components.

Observe that only one input and one output are part of the same safety function in the 2-channel version.

Therefore the DIP switch settings for all channels used in safety relevant applications are:

DIP Switch Settings 1-channel Devices

Function	Mode	KFD2-SOT3-Ex1.LB(.IO), KFD2-ST3-Ex1.LB
Mode output I	normal mode	S1 position I
	inverted mode	S1 position II
Assignment output II	follow output I	S2 position I
	LB/SC detection [1]	S2 position II
Line fault detection	ON	S3 position I
	OFF [2]	S3 position II

Table 3.1

[1] This mode may not be used if output II is used for safety relevant applications.
[2] This switch setting may not be used if the device is used for safety relevant applications.

DIP Switch Settings 2-channel Devices

Function	Mode	KFD2-SOT3-Ex2(.IO)(-Y1), KFD2-ST3-Ex2
Mode channel I	normal mode	S1 position I
	inverted mode	S1 position II
Mode channel II	normal mode	S2 position I
	inverted mode	S2 position II
Line fault detection	ON	S3 position I
	OFF [1]	S3 position II

Table 3.2

[1] This switch setting may not be used if the channel is used for safety relevant applications.

Line Fault Detection

For use in a safety function enable the line fault detection.

The input loop of all versions is supervised. The related safety function is that the outputs go to fault state (safe state) if a line fault is detected.

Reaction Time

The time for a step function from input to output is < 20 ms.

Note!

The collective error message output is not safety relevant.

3.4 Characteristic Safety Values

KFD2-SOT3-Ex*(.LB)(.IO)(-Y1)

Parameters acc. to IEC 61508	Characteristic values
Assessment type and documentation	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL (SC)	2
Safety function	Normal/inverted operation
λ_s [1]	113 FIT
λ_{dd}	3.3 FIT
λ_{du}	30.4 FIT
$\lambda_{total\ (safety\ function)}$	147 FIT
$\lambda_{not\ part}$	75 FIT
SFF [1]	79 %
MTBF [2]	317 years
PFH	3.04×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	1.33×10^{-4}
PFD_{avg} for T_1 = 2 years	2.67×10^{-4}
PFD_{avg} for T_1 = 5 years	6.66×10^{-4}
PTC	100 %

Table 3.3

[1] For transfer from the FMEDA report the following rules apply: "Annunciation failures" have no direct influence on the safety function and are therefore counted as "No effect failures". "No effect failures" are not influencing the safety function and are therefore not included in SFF and in the failure rates of the safety function.

[2] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h. The value is calculated for one safety function of the device.

For splitter devices (1 input and 2 outputs) the first output should be used for implementing the safety function. When the second output is used, 6.7 FIT must be added to the λ_{du}.

KFD2-ST3-Ex*(.LB)

Parameters acc. to IEC 61508	Characteristic values
Assessment type and documentation	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL (SC)	2
Safety function	Normal/inverted operation
λ_s	97 FIT
λ_{dd}	3.3 FIT
λ_{du}	25.2 FIT
$\lambda_{total\ (safety\ function)}$	126 FIT
$\lambda_{not\ part}$	75 FIT
SFF [1]	80 %
MTBF [2]	345 years
PFH	2.52×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	1.10×10^{-4}
PFD_{avg} for T_1 = 2 years	2.21×10^{-4}
PFD_{avg} for T_1 = 5 years	5.51×10^{-4}
PTC	100 %

Table 3.4

[1] For transfer from the FMEDA report the following rules apply: "Annunciation failures" have no direct influence on the safety function and are therefore counted as "No effect failures". "No effect failures" are not influencing the safety function and are therefore not included in SFF and in the failure rates of the safety function.

[2] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h. The value is calculated for one safety function of the device.

For splitter devices (1 input and 2 outputs) the first output should be used for implementing the safety function. When the second output is used, 6.7 FIT must be added to the λ_{du}.

The characteristic safety values like PFD, PFH, SFF, HFT and T_1 are taken from the FMEDA report. Observe that PFD and T_1 are related to each other.

The function of the devices has to be checked within the proof test interval (T_1).

3.5 Useful Life Time

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful lifetime of components is not exceeded. Beyond this useful lifetime, the result of the probabilistic estimation is meaningless as the probability of failure significantly increases with time. The useful lifetime 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 operating 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 lifetime of each component.

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

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

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

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

- if there are no components with reduced life time in the safety loop (for example electrolytic capacitors, relays, flash memories, optocoupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

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

4 Mounting and Installation

Installing the device

1. Observe the safety instructions in the instruction manual.
2. Observe the information in the manual.
3. Observe the requirements for the safety loop.
4. Connect the device only to devices that are suitable for this safety application.
5. Check the safety function to ensure the expected output behavior.

4.1 Configuration

Configuring the Device

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the front of the device.

1. De-energize the device before configuring the device.
2. Open the cover.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Close the cover.
5. Secure the DIP switches to prevent unintentional adjustments.
6. Connect the device again.

Note!

For more information see the corresponding datasheets.

5 Operation

Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.

Operating the device

1. Observe the safety instruction in the instruction manual.
2. Observe the information in the manual.
3. Use the device only with devices that are suitable for this safety application.
4. Correct any occurring safe failures within 24 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test

According to IEC/EN 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous failures that are not detected otherwise.

Check the function of the subsystem at periodic intervals depending on the applied PFD_{avg} in accordance with the characteristic safety values.
See chapter 3.4.

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

Equipment required:

- Digital multimeter without special accuracy

  Use for the proof test of the intrinsic safety side of the device a special digital multimeter for intrinsically safe circuits.

  If intrinsically safe circuits are operated with non-intrinsically safe circuits, they must no longer be used as intrinsically safe circuits.
- Power supply set to nominal voltage of 24 V DC
- Load resistor approx. 250 Ω
- Simulate the sensor state 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).

Check the settings after the configuration by suitable tests.

Proof Test Procedure

1. Test each input channel individually. The threshold must be between 1.4 mA and 1.9 mA. The hysteresis must be between 150 µA and 250 µA.

   ↳ For normal mode of operation the outputs must have a low impedance, if the input current is above the threshold. This state is indicated by yellow LED, > 80 mA when R approx. 250 Ω.

   For inverse mode of operation the outputs must have a low impedance, if the input current is below the threshold. This state is indicated by yellow LED, > 80 mA when R approx. 250 Ω.
2. Connect a resistor R_{SC} (220 Ω) or a resistor R_{LB} (150 kΩ) to the input.

   ↳ The device must detect an external fault. This state is indicated by red LED and the output of the corresponding channel must be in fault state.
3. Test the outputs with a certain current, i. e. > 80 mA and a voltage set to 24 V DC. Test that the outputs are definitely not conducting, if the yellow LED is off.
4. Set back the device to the original settings for the current application after the test.
5. Secure the DIP switches to prevent unintentional adjustments.

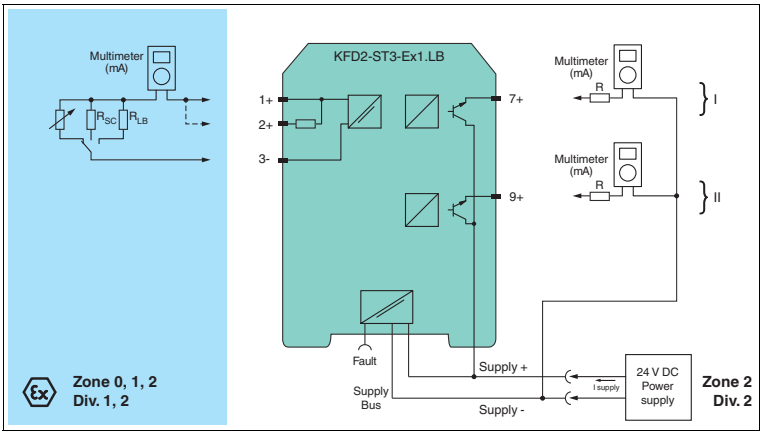

Figure 5.1 Proof test set-up for KFD2-ST3-Ex1.LB

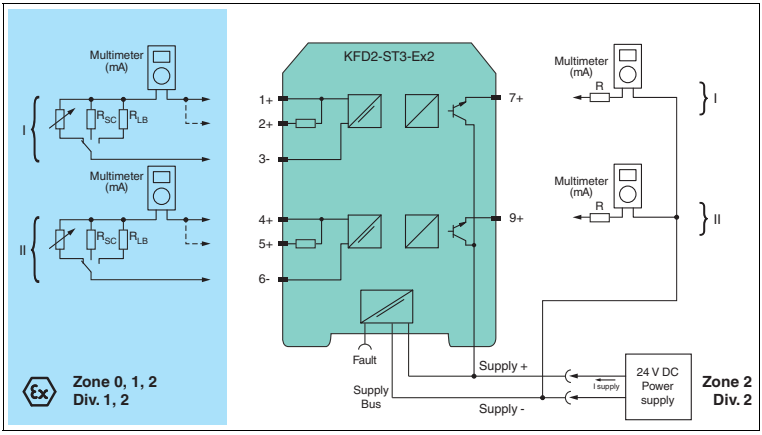

Figure 5.2 Proof test set-up for KFD2-ST3-Ex2

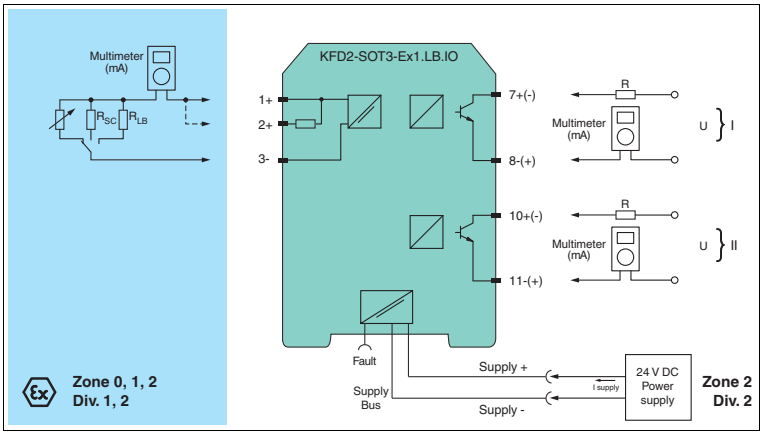

Figure 5.3 Proof test set-up for KFD2-SOT3-Ex1.LB(.IO)

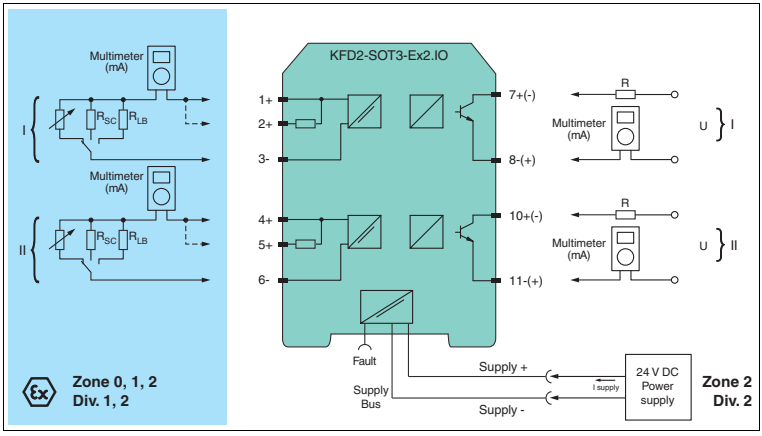

Figure 5.4 Proof test set-up for KFD2-SOT3-Ex2(.IO)(-Y1)

6 Maintenance and Repair

Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.

Maintaining, Repairing or Replacing the Device

In case of maintenance, repair or replacement of the device, proceed as follows:

1. Implement appropriate maintenance procedures for regular maintenance of the safety loop.
2. Ensure the proper function of the safety loop, while the device is maintained, repaired or replaced.
   If the safety loop does not work without the device, shut down the application.
   Do not restart the application without taking proper precautions.
   Secure the application against accidental restart.
3. Do not repair a defective device. A defective device must only be repaired by the manufacturer.
4. Replace a defective device only by a device of the same type.

7 List of Abbreviations

ESD	**E**mergency **S**hut**d**own
FIT	**F**ailure **I**n **T**ime in 10^{-9} 1/h
FMEDA	**F**ailure **M**ode, **E**ffects, and **D**iagnostics **A**nalysis
λ_{s}	Probability of safe failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{no\ effect}$	Probability of failures of components in the safety loop that have no effect on the safety function. The no effect failure is not used for calculation of SFF.
$\lambda_{not\ part}$	Probability of failure of components that are not in the safety loop
$\lambda_{total\ (safety\ function)}$	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**estoration
PCS	**P**rocess **C**ontrol **S**ystem
PFD_{avg}	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
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
SIL (SC)	**S**afety **I**ntegrity **L**evel (**S**ystematic **C**apability)
SIS	**S**afety **I**nstrumented **S**ystem
T_1	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

2016-03

2016-03

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/contact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

DOCT-5021
03/2016