ORIGINAL INSTRUCTIONS

Functional Safety

Switch Amplifier
KFD2-SH-Ex1(.T)(.OP),
KHA6-SH-Ex1

SIL
IEC 61508/61511

SIL 3 PL d

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"

2017-04

1 Introduction

1.1 Contents

This document contains safety-relevant information for usage of the device. 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!

For full information on the product, refer to the 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:

- EU-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

The devices are safety components according to the machinery directive 2006/42/EC.

This isolated barrier is used for intrinsic safety applications.

The device transfers digital signals (SN/S1N proximity sensors or approved dry contacts) from a hazardous area to a safe area.

Unlike an SN/S1N series proximity sensor, a mechanical contact requires a 10 kΩ resistor to be placed across the contact in addition to a 1.5 kΩ resistor in series.

Lead breakage (LB) and short circuit (SC) conditions of the control circuit are continuously monitored.

During an fault condition, the fault indication output energizes and outputs I and II de-energize.

For safety applications up to SIL 3, output I must be used. For safety applications up to SIL 2, output I and output II can be used.

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

KFD2-SH-Ex1, KHA6-SH-Ex1

The input controls 1 relay contact output with 3 NO contacts (1 output is in series to the both output relays for the safety function), 1 relay contact output with 1 NO contact, and 1 passive transistor output (fault indication output).

KFD2-SH-Ex1.T

The input controls 1 active voltage output and 1 relay contact output with a NO contact.

KFD2-SH-Ex1.T.OP

The input controls 1 active voltage output and 1 relay contact output with a NO contact.

The device can only be supplied by Power Rail.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input, output I, output II
- Non-safety relevant interfaces: fault indication output, power supply

Note!

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs GmbH Lilienthalstraße 200, 68307 Mannheim, Germany
Internet: www.pepperl-fuchs.com

KFD2-SH-Ex1, KFD2-SH-Ex1.T, KFD2-SH-Ex1.T.OP, KHA6-SH-Ex1	Up to SIL 3 Up to PL d

2.4 Standards and Directives for Functional Safety

Device-specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 2, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

Machinery Directive 2006/42/EC	• EN/ISO 13849, part 1, edition 2015: Safety-related parts of control systems (manufacturer) • IEC/EN 62061, edition 2005 + A1:2012/2013 + A2:2015: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1, 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:

- The fault indication output which signals if the field circuits are broken or shorted is not considered in the FMEDA and the calculations.
- For output I of the KFD2-SH-Ex1 and KHA6-SH-Ex1 devices, use the 3 redundant relay contacts to establish the necessary redundancy.
- 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 safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- Observe for the high demand mode the useful lifetime limitations of the output relays.
- 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.

SIL 3 application

If you use output I of the device, you can reach SIL 3 according to IEC 61508.

- The device shall claim less than 10 % of the total failure rate for a SIL 3 safety loop.
- For a SIL 3 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^{-3}, hence the maximum allowable PFD_{avg} value would then be 10^{-4}.
- For a SIL 3 application operating in high demand mode the total PFH value of the SIF should be smaller than 10^{-7} per hour, hence the maximum allowable PFH value would then be 10^{-8} per hour.
- Since the safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 90 % according to table 2 of IEC/EN 61508-2 for a SIL 3 (sub) system.

SIL 2 application

If you use output I or output II of the device, you can reach SIL 2 according to IEC 61508.

- 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.
- 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.

PL d application

- If you use output I of the device, you can use the device in safety control loops up to performance level PL d.
- The devices were qualified for use in applications acc. to EN/ISO 13849-1. They fulfill PL d and are designed as Category 3 equipment. Consider the rules for use given in this standard.

3.3 Safety Function and Safe State

Safe State

The safe state of the outputs is the de-energized state. This state is reached when the input is in low state.

Safety Function

K*-SH-Ex1**

The devices have two outputs that can be used for the safety function. Output I is a relay output with triplicated output relay, intended for use in applications up to SIL 3 or PL d. Output II is an additional relay output that may by itself be used in applications up to SIL 2.

KFD2-SH-Ex1.T(.OP)

The devices have two outputs that can be used for the safety function. Output I is an electronic output that may be used in applications up to SIL 3 or PL d. Output II may be used in applications up to SIL 2.

Line Fault Detection

The input circuit of all versions is supervised. The related safety function is defined as the outputs are low/de-energized (safe state), if a line fault or a short circuit of the sensor is detected.

Reaction Time

The reaction time for all safety functions is < 30 ms.

Note!

The fault indication output is not safety relevant.

3.4 Characteristic Safety Values

KHA6-SH-Ex1

Parameters acc. to IEC 61508	Characteristic values	
Assessment type and documentation	FMEDA, proven-in-use assessment, certificate	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0 [1]	0
SIL	3 (proven-in-use)	2 (proven-in-use)
Safety function	Output I is de-energized when input in low state	Output II is de-energized when input in low state
λ_s	266 FIT	179 FIT
λ_{du}	0.6 FIT	51.9 FIT
λ_{dd}	76.8 FIT	50.4 FIT
$\lambda_{no\ effect}$ [2]	190 FIT	143 FIT
$\lambda_{total\ (safety\ function)}$	289 FIT	280 FIT
SFF	99.8 %	81 %
MTBF [3]	214 years	269 years
$MTTF_d$	1477 years	–
DC_d	99.2 % (high)	–
$B10_d$	250000	–
Category (ISO 13849-1)	3	–
PL	d	–
PFH	6.47×10^{-10} 1/h	5.19×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	2.83×10^{-6}	2.27×10^{-4}
PFD_{avg} for T_1 = 2 years	5.67×10^{-6}	4.55×10^{-4}
PFD_{avg} for T_1 = 5 years	1.42×10^{-5}	1.14×10^{-3}
Reaction time [4]	< 30 ms	< 30 ms

Table 3.1

1 The redundant relays can be considered as elements with hardware fault tolerance. For this calculation the redundant relays were considered as "diagnostics" for the relay with a DC value of 99 % to take care of a possible common cause failure.

2 "Annunciation failures" are not directly influencing the safety functions and are therefore added to the $\lambda_{no\ effect}$ value.

3 acc. to SN29500. This value is calculated with the failure rates of the device components which are part of the safety function of the device.

4 Time between fault detection and fault reaction.

KFD2-SH-Ex1

Parameters acc. to IEC 61508	Characteristic values	
Assessment type and documentation	FMEDA, proven-in-use assessment, certificate	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0 [1]	0
SIL	3 (proven-in-use)	2 (proven-in-use)
Safety function	Output I is de-energized when input in low state	Output II is de-energized when input in low state
λ_s	237 FIT	203 FIT
λ_{du}	0.6 FIT	51.9 FIT
λ_{dd}	50.5 FIT	36.6 FIT
$\lambda_{no\ effect}$ [2]	215 FIT	156 FIT
$\lambda_{total\ (safety\ function)}$	288 FIT	291 FIT
SFF	99.8 %	82 %
MTBF [3]	204 years	254 years
$MTTF_d$	2240 years	–
DC_d	98.7 % (medium)	–
$B10_d$	250000	–
Category (ISO 13849-1)	3	–
PL	d	–
PFH	6.47×10^{-10} 1/h	5.19×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	2.83×10^{-6}	2.27×10^{-4}
PFD_{avg} for T_1 = 2 years	5.67×10^{-6}	4.55×10^{-4}
PFD_{avg} for T_1 = 5 years	1.42×10^{-5}	1.14×10^{-3}
Reaction time [4]	< 30 ms	< 30 ms

Table 3.2

1 The redundant relays can be considered as elements with hardware fault tolerance. For this calculation the redundant relays were considered as "diagnostics" for the relay with a DC value of 99 % to take care of a possible common cause failure.

2 "Annunciation failures" are not directly influencing the safety functions and are therefore added to the $\lambda_{no\ effect}$ value.

3 acc. to SN29500. This value is calculated with the failure rates of the device components which are part of the safety function of the device.

4 Time between fault detection and fault reaction.

KFD2-SH-Ex1.T(.OP)

Parameters acc. to IEC 61508	Characteristic values	
Assessment type and documentation	FMEDA, proven-in-use assessment, certificate	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0	
SIL	3 (proven-in-use)	2 (proven-in-use)
Safety function	Output I is de-energized when input in low state	Output II is de-energized when input in low state
λ_s	181 FIT	194 FIT
λ_{du}	1.4 FIT	51.6 FIT
λ_{dd}	38.4 FIT	38.4 FIT
$\lambda_{no\ effect}$ [1]	195 FIT	130 FIT
$\lambda_{total\ (safety\ function)}$	218 FIT	282 FIT
SFF	99.4 %	81 %
MTBF [2]	275 years	276 years
$MTTF_d$	2860 years	–
DC_d	96.5 % (medium)	–
$B10_d$	–	–
Category (ISO 13849-1)	3	–
PL	d	–
PFH	1.38×10^{-9} 1/h	5.16×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	6.04×10^{-6}	2.26×10^{-4}
PFD_{avg} for T_1 = 2 years	1.21×10^{-6}	4.52×10^{-4}
PFD_{avg} for T_1 = 5 years	3.02×10^{-5}	1.13×10^{-3}
Reaction time [3]	< 30 ms	< 30 ms

Table 3.3

1 "Annunciation failures" are not directly influencing the safety functions and are therefore added to the $\lambda_{no\ effect}$ value.

2 acc. to SN29500. This value is calculated with the failure rates of the device components which are part of the safety function of the device.

3 Time between fault detection and fault reaction.

The characteristic safety values like PFD, PFH, SFF, HFT and T_1 are taken from the FMEDA report and the assessment documentation created by the issuer. Please note, 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).

The safety values $MTTF_d$, DC_d, Category and PL for the machinery directive are taken from the assessment report and certificate.

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 to 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 the ambient conditions support a long life time, for example 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.

Maximum Switching Power of Output Contacts KFD2-SH-Ex1

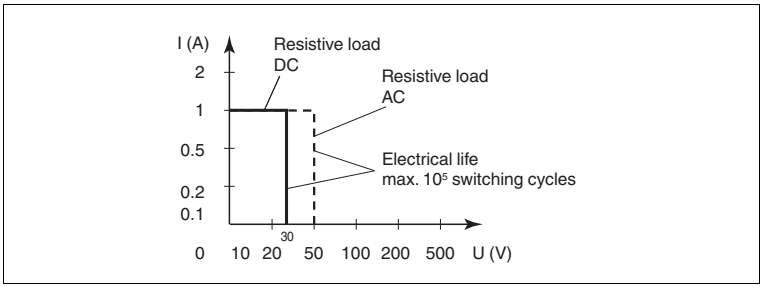

Figure 3.1

Maximum Switching Power of Output Contacts KHA6-SH-Ex1

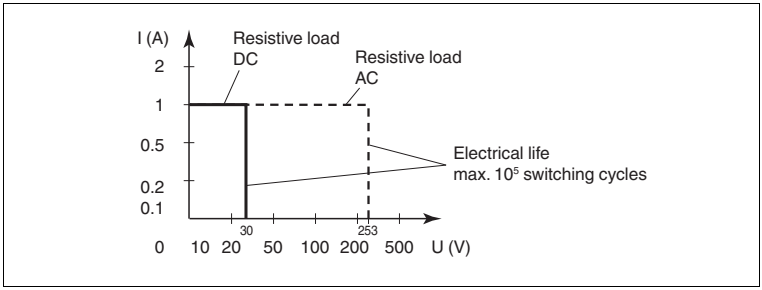

Figure 3.2

Maximum Switching Power of Output Contacts KFD2-SH-Ex1.T(.OP)

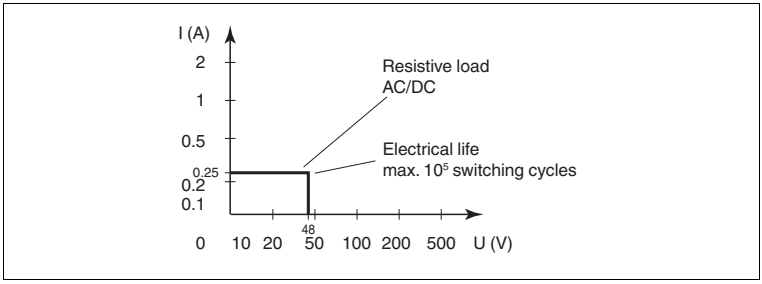

Figure 3.3

The maximum number of switching cycles is depending on the electrical load and may be higher if reduced currents and voltages are applied.

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

A configuration of the device is not necessary and not possible.

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 instructions 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 8 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test Procedure

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 with an accuracy better than 0.1 %
  For the proof test of the intrinsic safety side of the devices, a special digital multimeter for intrinsically safe circuits must be used.

  Intrinsically safe circuits that were operated with non-intrinsically safe circuits may not be used as intrinsically safe circuits afterwards.
- Power supply set at nominal voltage of 24 V DC.
- Potentiometer 4.7 kΩ.
- Resistor 220 Ω/150 kΩ.
- Resistor 1.3 kΩ/0.5 W (.T(.OP) version only).
- Resistor 1 kΩ/1 W.

Proof Test Procedure

1. Prepare a test set-up, see figure below.
2. Simulate the state of the sensor
   - 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)
3. Connect a load of 1.3 kΩ to the voltage output of the .T(.OP) device.
4. Supply the relay contact output by 24 V DC externally. Connect an 1 kΩ resistor as load to the relay contact output. Test this configuration with a multimeter for the state (on).
5. For versions with triplicated relays, test each single relay with a multimeter if the off state is reached.

   ↳ The input threshold must be between 2.1 mA and 2.8 mA. The hysteresis must be between 170 µA and 250 µA (measured with input multimeter and potentiometer).
   If the input current is above the threshold,
   - the voltage output must be activated, voltage level higher than 20 V DC (.T(.OP) version only),
   - the relay contact output must conduct (approx. 24 mA over 1 kΩ),
   - the yellow LED must be on.
6. For the functional safety it is important that the voltage output is **definitely off** (less than 1 V DC) and each single relay contact output is **definitely open (high impedance)**, if the input is below the lower threshold (typ. 2.5 mA) or above the higher threshold (typ. 6 mA).
7. Connect the resistor R_{SC} (220 Ω) or the resistor R_{LB} (150 kΩ) to the input.

   ↳ The red LED must indicate the fault, the voltage output is off, the relay contact outputs are high impedant (> 100 kΩ).

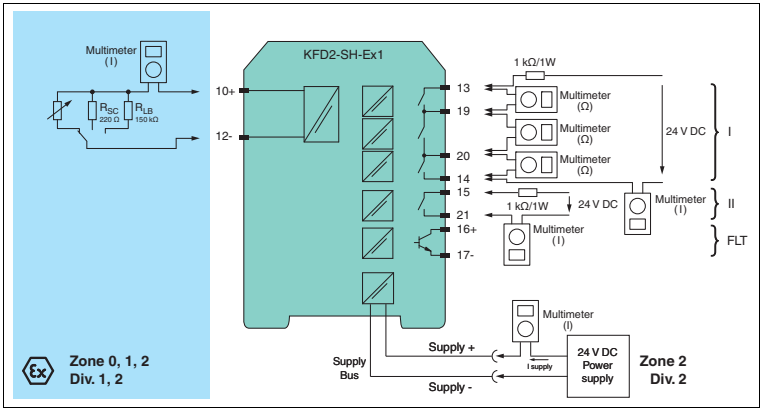

Figure 5.1 Proof test set-up for KFD2-SH-Ex1, KHA6-SH-Ex1

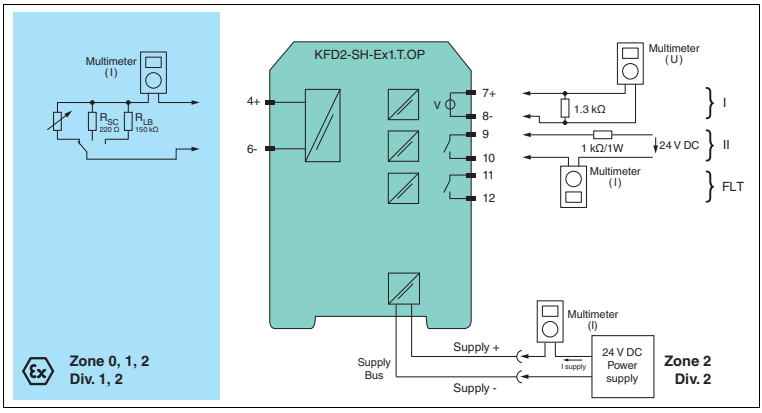

Figure 5.2 Proof test set-up for KFD2-SH-Ex1.T(.OP)

6 List of evaluated Sensors

The following sensors were evaluated for use in conjunction with PL d and SIL 3:

NJ2-11-SN
NJ2-11-SN-G
NJ2-11-SN-G-..M [1]
NJ2-12GK-SN
NJ2-12GK-SN-..M [1]
NJ4-12GK-SN
NJ4-12GK-SN-..M [1]
NJ3-18GK-S1N
NJ3-18GK-S1N-..M [1]
NJ5-18GK-SN
NJ5-18GK-SN-..M [1]
NJ8-18GK-SN
NJ8-18GK-SN-..M [1]
NJ6-22-SN
NJ6-22-SN-G
NJ6-22-SN-G-..M [1]
NJ5-30GK-S1N
NJ5-30GK-S1N-..M [1]
NJ10-30GK-SN
NJ10-30GK-SN-..M [1]
NJ15-30GK-SN
NJ15-30GK-SN-..M [1]
NJ6S1+U1+N1
NJ15S+U1+N
NJ20S+U1+N
NJ40-FP-SN-P1
SJ2-SN
SJ2-S1N
SJ3,5-SN
SJ3,5-SN-Y89604
SJ3,5-S1N
NCN3-F25-SN4-V1
PL2-F25-SN4-K
PL3-F25-SN4-K

Table 6.1

[1] -..M means different cable lengths in meter (m).

Additionally, mechanical switches may be used. See chapter 2.1.

2017-04

7 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.

8 List of Abbreviations

B_{10d}	Number of switching cycles of relays until 10 % of these components have failed
Category	Category acc. to EN/ISO 13849-1
DC_d	**D**iagnostic **C**overage of dangerous faults
DCS	**D**istributed **C**ontrol **S**ystem
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 path that have no effect on the safety function
$\lambda_{-not\ part}$	Probability of failures of components that are not in the safety path
$\lambda_{-total\ (safety\ function)}$	Safety function
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
$MTTF_d$	**M**ean **T**ime **T**o dangerous **F**ailures
MTTR	**M**ean **T**ime **T**o **R**epair
PFD_{avg}	Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
PL	**P**erformance **L**evel acc. to EN/ISO 13849-1
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
T_1	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

2017-04

2017-04

2017-04

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-2992B
04/2017