PROCESS AUTOMATION

SAFETY MANUAL SIL

RELAY MODULE
KFD0-RSH-1.4S.PS2

SIL

IEC 61508/61511

ISO9001

CE

SIL3

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, the Functional Safety Assessment 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

This signal conditioner is a loop powered safety relay module with a logic input and two different relay outputs:

It can be used as an interface in output loops for fire and gas systems classified as SIL3. The safe state in this application is **e**nergized **t**o **s**afe (ETS). Output I with two relays in parallel must be used, no fuse available.

It can also be used as an interface in output loops for ESD (**E**mergency **S**hut **D**own) systems classified as SIL3. The safe state in this application is **d**e-energized **t**o **s**afe (DTS). Output II with two relays in series must be used. An additional fuse in series to the relay contacts is available (see chapter 3).

With both outputs in combination a non safety application for dual pole switching (DPS) is possible.

Additionally a test input for proof tests is available. The proof test checks if each single relay is working correctly.

The device is usually mounted on a DIN rail in cabinets with access for qualified personnel only.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200
68307 Mannheim/Germany

KFD0-RSH-1.4S.PS2

Up to SIL3 (for DTS), up to SIL3 (for ETS)

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 – 7, 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 – 3, 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)

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Failure rates are constant, wear out mechanisms are not included.
- 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.
- Failure rate based on the Siemens SN29500 data base.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours.
- 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 high currents and high ambient temperature the de-rating given in the data sheet needs to be considered.
- The input of the device must be connected to a safety PLC which has minimum the SIL needed in the loop.
- The device shall claim less than 10 % of the total failure budget for a SIL3 safety loop.
- For a SIL3 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 SIL3 application operating in High Demand Mode of operation 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 circuit has a Hardware Fault Tolerance of **0** and it is a type **A** component, the SFF must be > 90 % according to table 2 of IEC 61508-2 for SIL3 (sub)system.

2.3 Safety Function and Safe State

DTS

Safety Function

The safety function of the device is defined: Whenever the input of the device is de-energized, the DTS output is not conducting.

Safe State

For the DTS safety function the safe state is defined as the DTS output being open (not conducting).

Reaction Time

The reaction time is < 20 ms.

ETS

Safety Function

The safety function of the device is defined: Whenever the input of the device is energized, the ETS output is conducting.

Safe State

For the ETS safety function the safe state is defined as the ETS output being closed (conducting).

Reaction Time

The reaction time is < 20 ms.

DPS

The dual pole switching application is no safety application.

General

For all applications the maximum switching frequency is limited to 10 Hz.

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables	
Assessment type and documentation	Full assessment	
Pepperl+Fuchs FMEDA report [1]	FS-0042EA-20A	
Device type	A	
Demand mode	Low Demand Mode or High Demand Mode	
Safety function [2]	ETS [4]	DTS
HFT	0	0
SIL	3	3
$\lambda_{sd} + \lambda_{su}$	139.7 FIT	144.77 FIT
λ_{dd}	0 FIT	0 FIT
λ_{du}	7.1 FIT	1.83 FIT
$\lambda_{\text{total (safety function)}}$	146.6 FIT	146.6 FIT
SFF	95.2 %	98.7 %
MTBF [3]	639 years	560 years
PFH	7.1×10^{-9} 1/h	1.83×10^{-9} 1/h
PFD_{avg} for T_1 = 1 year	3.1×10^{-5}	8.01×10^{-6}
T_{proof} max.	3 years	12 years
Reaction time	< 20 ms	

[1] Pepperl+Fuchs documentation number

[2] The device can be used in two safety functions, ETS (energized to safe) and DTS (de-energized to safe).

[3] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.

[4] For ETS in SIL2 applications no proof test has to be carried out, the calculated proof time is higher than the useful time (T_{proof} max. for ETS SIL2 is 32 years).

The characteristic safety values like PFD/PFH, 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: input, output I (ETS), output II (DTS)
- To avoid contact welding in DTS application we recommend to use a serial fuse in the load circuit. This can be the internal fuse F1 or any external fuse of max. 5 A nominal value.
- Test input interface may not be used during normal operation (only for proof test)

3.2 Configuration

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

ETS, DTS and DPS can be selected by using the referring terminals. See data sheet. The fuse in delivery status (2.5 A) can be changed to max 5 A. Please note the temperature derating according to the data sheet.

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.

Maximum Switching Power of Output Contacts

The useful life time is limited by the maximum switching cycles under load conditions. You can see the relationship between the maximum switching power and the load conditions in the diagram below.

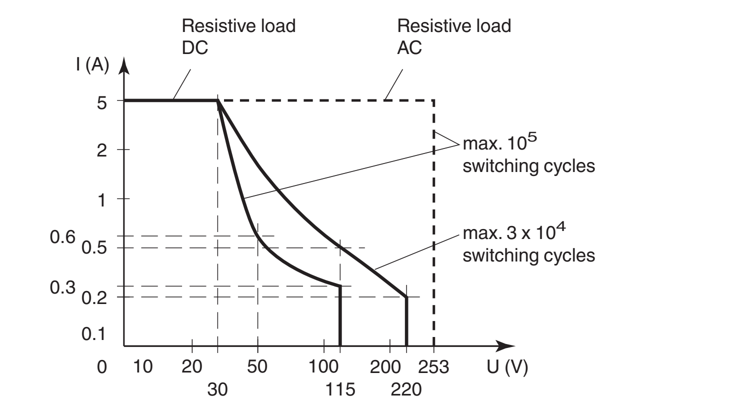

Figure 3.1

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 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:

- A digital multimeter (without special accuracy) will be used as ohmmeter (mid range recommended) to check the relay outputs. Closed contacts are shown with 0 Ω (low impedance), open contacts are shown with OL (overload/high impedance).
- Power supply set at nominal voltage of 24 V DC

Procedure:

For the proof test five tests have to be done as shown in the following table and pictures:

Test No.	Input or Test Input	Output (mA)
1	$V_{test\ input}$ = 24 V DC between terminals 10+, 11-	DTS output (terminals 5, 6): OL (overload) ETS output (terminals 2, 3): shows 0 Ω Red LED TST1 is flashing.
2	$V_{test\ input}$ = 24 V DC between terminals 11-, 12+	DTS output (terminals 5, 6): OL (overload) ETS output (terminals 2, 3): shows 0 Ω Red LED TST2 is flashing.
3	$V_{test\ input}$ = 24 V DC between terminals 10+, 11- and between terminals 11-, 12+	DTS output (terminals 5, 6): shows 0 Ω ETS output (terminals 2, 3): shows 0 Ω Both red LEDs are flashing.
4	$V_{test\ input}$ = 0 V DC between terminals 10+, 11- and between terminals 11-, 12+	DTS output (terminals 5, 6): OL (overload) ETS output (terminals 2, 3): OL (overload) Both red LEDs are off.
5	V_{input} = 24 V DC between terminals 7+ and 8- and with changed input polarity between terminals 7-, 8+	DTS output (terminals 5, 6): shows 0 Ω ETS output (terminals 2, 3): shows 0 Ω Yellow LED is on.

Table 4.1 Expected test results for a successful proof test

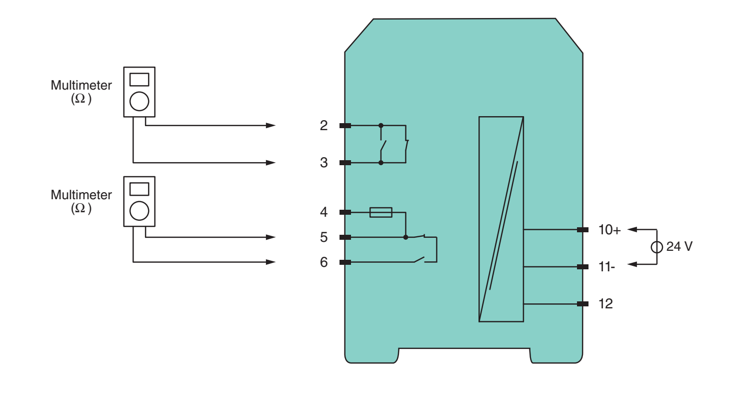

Figure 4.1 Proof test set-up for KFD0-RSH-1.4S.PS2, test 1

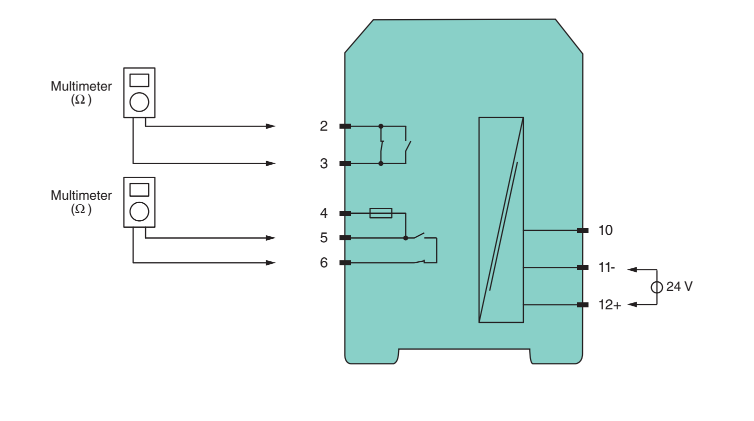

Figure 4.2 Proof test set-up for KFD0-RSH-1.4S.PS2, test 2

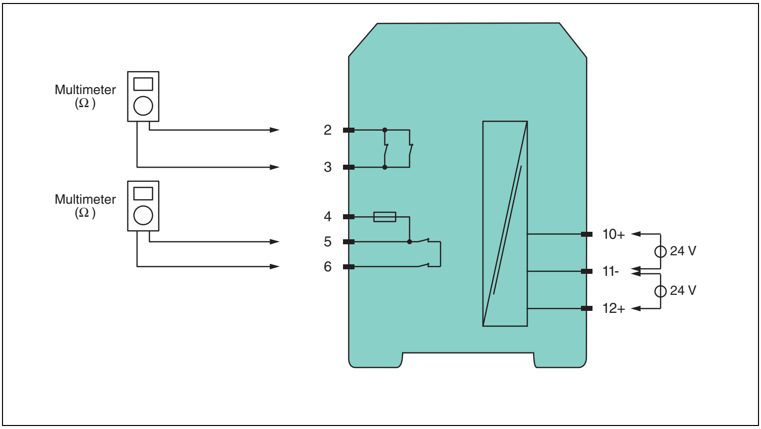

Figure 4.3 Proof test set-up for KFD0-RSH-1.4S.PS2, test 3

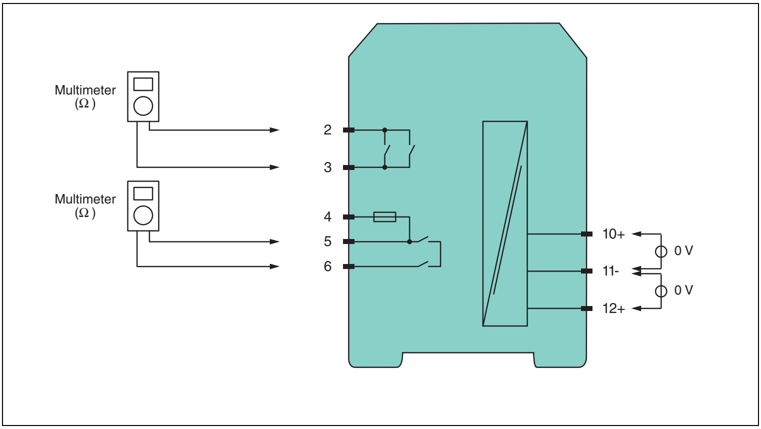

Figure 4.4 Proof test set-up for KFD0-RSH-1.4S.PS2, test 4

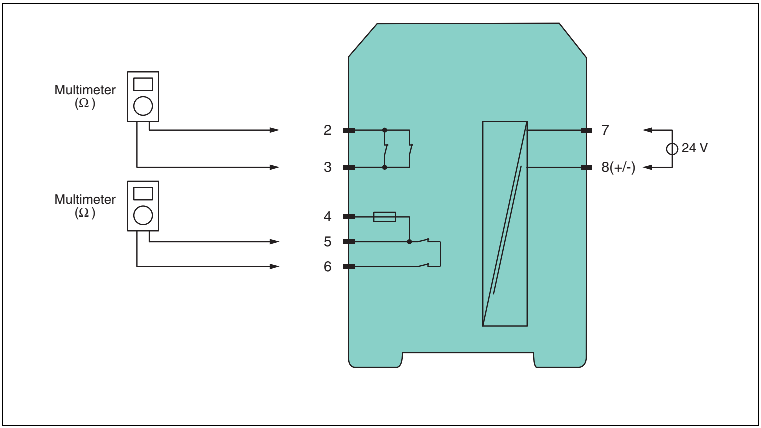

Figure 4.5 Proof test set-up for KFD0-RSH-1.4S.PS2, test 5

Only if all tests are successfully done, the proof test is successfull.

5 Abbreviations

FMEDA	**F**ailure **M**ode, **E**ffects and **D**iagnostics **A**nalysis
HFT	**H**ardware **F**ault **T**olerance
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
T$_{proof}$	Proof Test Interval
DPS	**D**ual **P**ole **S**witching
DTS	**D**e-energized **T**o **S**afe State
ESD	**E**mergency **S**hut **D**own
ETS	**E**nergized **T**o **S**afe State

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

225538 TDOCT-2052CENG
04/2011