PROCESS AUTOMATION

SAFETY MANUAL SIL

Relay Module
KFD0-RO-(Ex)*

SIL
IEC 61508/61511

ISO9001

SIL2 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 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, installation, commissioning, operation, maintenance and disassembly 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

KFD0-RO-*

The KFD0-RO-* provides the galvanic isolation between field circuits and control circuits. The device switches circuits on the field side.

KFD0-RO-Ex*

The KFD0-RO-Ex* is used for intrinsic safety applications. The device switches intrinsically safe circuits on the field side.

General

Typical applications for the use of the device are remote reset, fire alarm testing or remote calibration of strain gauges.

The outputs are galvanically isolated to the inputs. The inputs are not polarized and share a common reference potential.

Each input of the device is protected by a fuse and an electronic current limiting.

The KFD0-RO-(Ex)* is a single device for DIN rail mounting.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

KFD0-RO-*
KFD0-RO-Ex*

Up to SIL3

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).
- 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.
- 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.
- 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 **A** components with a Hardware Fault Tolerance of **0**.
- Since the circuit has a Hardware Fault Tolerance of **0** and it is a type **A** component, the SFF must be > 60 % according to table 2 of IEC 61508-2 for SIL2 (sub)system.
- Since the circuit has a Hardware Fault Tolerance of **0 (or 1)** and it is a type **A** component, the SFF must be > 90 % (or > 60 %) according to table 2 of IEC 61508-2 for SIL3 (sub)system.
- 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 safety function is that a de-energized input leads to the output being open (not conducting). The output at pins 2 and 3 (pins 5 and 6 for channel 2) in open circuit is the safe state.

Reaction Time

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

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Values	
Assessment type and documentation	FMEDA report	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0	1 [3]
SIL	2	3
Safety function	DTS [4] One relay output of one channel	DTS [4] Two relay outputs controlled by the same input
λ_s	85.2 FIT	170.4 FIT
λ_{dd}	0 FIT	0 FIT
λ_{du}	40 FIT	4.4 FIT
$\lambda_{total\ (safety\ function)}$	160 FIT	320.8 FIT
SFF	75.0 %	98.6 %
MTBF [1]	351 years	351 years
PFH	4.0×10^{-8} 1/h	4.42×10^{-9} 1/h
PFD_{avg} for T_{proof} = 1 year	1.75×10^{-4}	1.94×10^{-5}
PFD_{avg} for T_{proof} = 2 years	3.54×10^{-4}	3.87×10^{-5}
PFD_{avg} for T_{proof} = 5 years	8.76×10^{-4}	9.68×10^{-5}
Reaction time [2]	< 20 ms	

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

[2] Time between fault detection and fault reaction.

[3] The redundance of the circuit parts has already been regarded in the probabilistic calculations. The given failure probabilities, SFF, PFD and PFH need to be used as complete values for one single SIL3 safety path with HFT = 0.

[4] DTS = **D**e-energized **T**o **S**afe State

Table 2.1

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: input I, input II, output I, output II

3.2 Configuration

A configuration is done by correctly attaching the input potentials and output relays.

For two separate signal paths that can be used in applications up to SIL2, the input of each channel supplies the respective output without combining the two separate safety paths. The only common part of the safety functions is the potential at pin 8. The user must ensure that the combination of the potentials of the two safety paths is not leading to unwanted behavior of the input signals.

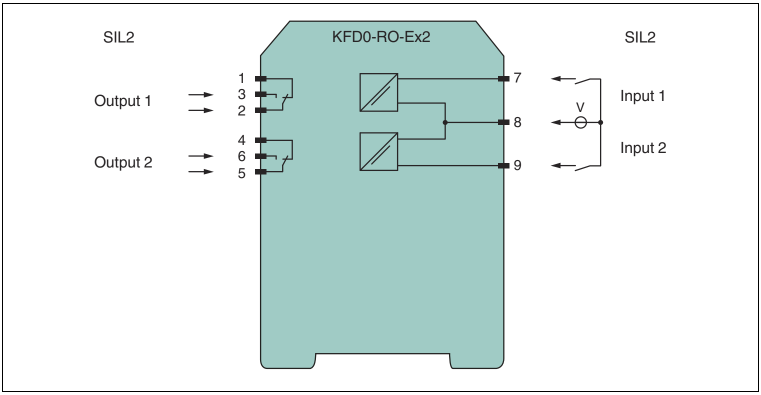

Figure 3.1 SIL2 application

For one combined output that can be used in applications up to SIL3, the relay outputs need to be connected in series. Input signals can either be coming from one SIL3 signal source or from two SIL2 signal sources. For the two signal sources, the potentials must be connectable without influence on the signal source at pin 8.

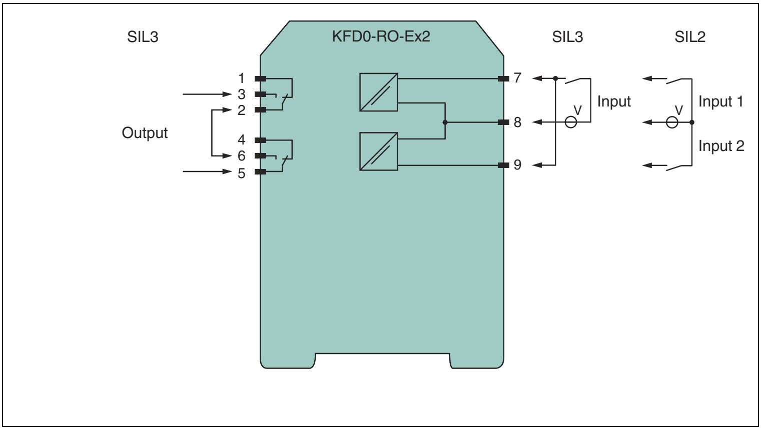

Figure 3.2 SIL3 apllication

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 electrical load conditions. You can see the relationship between the maximum switching power and the load conditions in the diagram below.

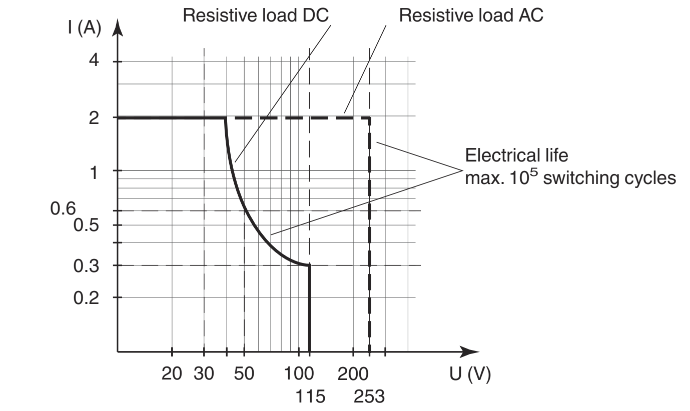

Figure 3.3 Characteristic of Ex versions KFD0-RO-Ex*

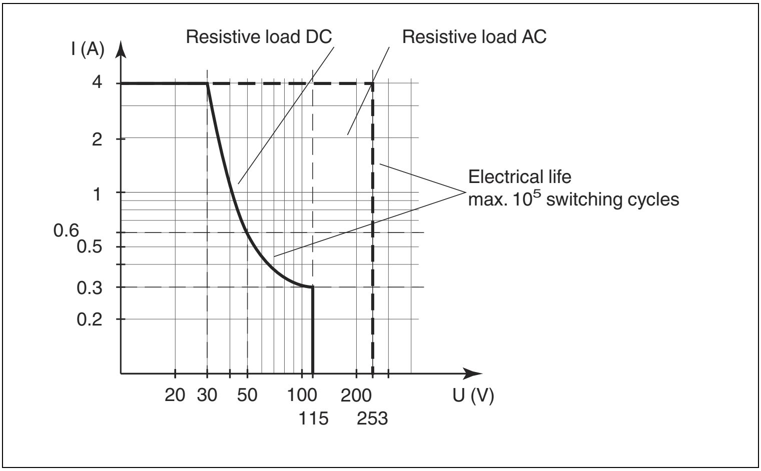

Figure 3.4 Characteristic of non-Ex versions KFD0-RO-*

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

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 measures must be taken to ensure the safety of the loop, in case of no redundancy the loop has to be 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 failures 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:

The voltage input must be simulated by applying a 24 V supply in the orientation that is used for this safety application. Where both polarities are used the test must be done in both orientations.

The input test needs to be done for each input channel individually.

- Without voltage applied between terminals 7 and 8(second channel terminals 8 and 9), terminals 1 and 2 (second channel terminals 4 and 5) must be conducting while terminals 2 and 3 (second channel terminals 5 and 6) must be non-conducting. The corresponding LED must be off.
- When voltage is applied between terminals 7 and 8 (second channel terminals 8 and 9), the state of the outputs is exactly the opposite to the situation without voltage applied.

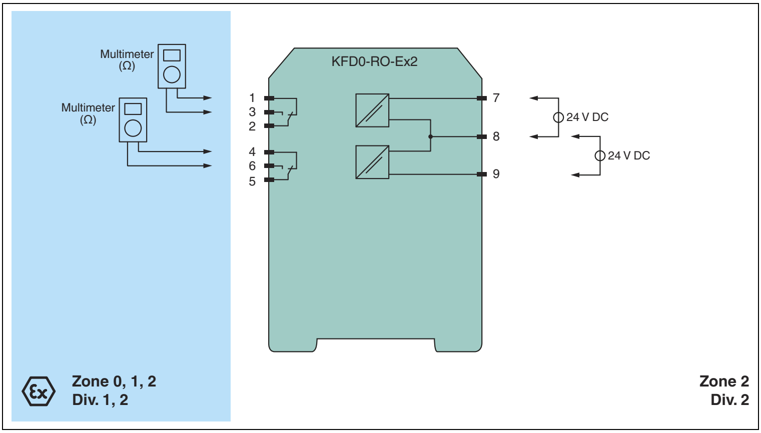

Figure 4.1 Proof test set-up for KFD0-RO-Ex2

Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD0-RO-Ex*.

5 Abbreviations

DTS	**D**e-energized **T**o **S**afe State
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_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{\text{total (safety function)}}$	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
PFD$_{\textbf{avg}}$	Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
SFF	**S**afe **F**ailure **F**raction
SIL	**S**afety **I**ntegrity **L**evel
T$_{\textbf{proof}}$	Proof Test Interval

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

TDOCT-2763_ENG
07/2012