SAFETY MANUAL SIL

Relay Module

KFD0-RSH-1(-Y2), KFD2-SL-4

SIL
IEC 61508/61511

ISO9001

CE

SIL2
SIL3

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"

2014-07

1 Introduction

1.1 General Information

This manual contains information on using the device in control circuits that are related to functional safety.

The corresponding data sheets, the operating instructions, the system description, the declaration of conformity, the EC-Type Examination Certificate, and the applicable certificates (see data sheet) are an integral part of this document.

The stated documents are available at **www.pepperl-fuchs.com** or from 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.

In the event of a device fault, the devices must be taken out of operation and measures must be taken to protect them against unintentional startup. Devices may be repaired only by the manufacturer. Deactivating or bypassing safety functions, or failing to observe the instructions in this manual (which lead to faults or affect the safety functions), can damage property and the environment or cause personal injury, for which Pepperl+Fuchs GmbH accepts no liability.

The devices have been developed, manufactured, and tested according to the applicable safety standards. The devices may be used only for the applications described in the instructions under the specified ambient conditions and exclusively in connection with the approved peripherals.

1.2 Intended Use

General

The devices are single devices for DIN rail mounting.

KFD0-RSH-1(-Y2)

These signal conditioners provides the galvanic isolation between field circuits and control circuits.

The devices are relay modules that are suitable for safely switching applications of a load circuit. The devices isolate load circuits up to 230 V and the 24 V control interface.

The devices can also be used as interfaces in output loops for ESD (**E**mergency **S**hut **D**own) systems classified as SIL3. The safe state in this application is de-energized to safe. The output has three relays that are of diverse design, but have a common effect on the output. An additional fuse in series to the relay contacts is available.

The KFD0-RSH-1-Y2 is protected against high pulses during OFF state, low pulses during ON state and a load impedance check.

2014-07

KFD2-SL-4

The devices are 4-channel signal conditioners with outputs that switch up to 600 mA to high-power solenoids. The devices are also used as power amplifier up to a switching frequency of 1 kHz.

For functional safety applications, the common disable input is used to switch off all outputs when de-energized. The devices can be used for applications up to SIL2

Two channels per module can be paralleled. The output current of a parallel combination is 1.2 A. If the supply voltage falls below 18 V, the outputs will be switched off. The outputs are sustained short-circuit proofed and overload-proofed.

Line fault detection can be enabled via DIP switch. Fault LED and collective error output via Power Rail behave as described within the data sheet of the device.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

KFD0-RSH-1, KFD0-RSH-1-Y2

Up to SIL3

KFD2-SL-4

Up to SIL2

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 of Operation

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 the T_{proof} value (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)

2.1.2 High Demand or Continuous Mode of Operation

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:

- 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 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:

- 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 loop 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 a SIL2 (sub)system.
- Since the loop 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 a SIL3 (sub)system.
- It is assumed that 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 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. A moisture level within the manufacturer's specifications is assumed. For a higher average temperature of 60 °C, the failure rates must be multiplied by a factor of 2.5 based on empirical values. A similar multiplier must be used if frequent temperature fluctuations are expected.

- It is assumed that any safe failures that occur (e.g., output in safe condition) will be corrected within eight hours (e.g., correction of a sensor fault).
- While the device is being repaired, measures must be taken to maintain the safety function (e.g., by using a replacement device).
- The indication of a dangerous fault (via fault bus) is detected within 1 hour by the programmable logic controller (PLC).
- Since the two outputs of the device use common components, these outputs must not be used in the same safety function.
- For the KFD0-RSH devices, the relay outputs need protection by a fuse initiating at 80 % of the rated current to avoid contact welding.

2.3 Safety Function and Safe State

Safety Function

KFD0-RSH-1(-Y2): Whenever the input of the device is de-energized, the output is de-energized.

KFD2-SL-4: Whenever the common disable input is de-energized, all outputs are de-energized.

Safe State

The safe state is defined as all outputs being de-energized (not conducting)

The KFD2-SL-4 is configurable. The settings do not influence the safety function. The settings only cause reactions on the additional error output.

Switching Frequency

The maximum switching frequency in the safety relevant input (for KFD2-SL-4 the common disable input) is 10 Hz.

For the KFD2-SL-4, the maximum switching frequency for the not safety relevant signal transfer is 1 kHz.

2014-07

2.4 Characteristic Safety Values

KFD0-RSH-1

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
SIL	3
Safety function	Output relay in OFF state when input is de-energized
λ_s	251.6 FIT
λ_{dd}	0 FIT
λ_{du}	0.4 FIT
$\lambda_{no\ effect}$	69.6 FIT
$\lambda_{total\ (safety\ function)}$	252 FIT
SFF	99.8 %
MTBF [1]	452 years
PFH	4.00×10^{-10} 1/h
PFD_{avg} for T_{proof} = 1 year	1.75×10^{-6}
PFD_{avg} for T_{proof} = 2 years	3.50×10^{-6}
PFD_{avg} for T_{proof} = 5 years	8.76×10^{-6}
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.

Table 2.1

KFD0-RSH-1-Y2

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
SIL	3
Safety function	Output relay in OFF state when input is de-energized
λ_s	255 FIT
λ_{dd}	0 FIT
λ_{du}	4.4 FIT
$\lambda_{no\ effect}$	72.8 FIT
$\lambda_{total\ (safety\ function)}$	259 FIT
$\lambda_{not\ part}$	0 FIT
SFF	98.3 %
MTBF [1]	440 years
PFH	4.38×10^{-9} 1/h
PFD_{avg} for T_{proof} = 1 year	1.91×10^{-5}
PFD_{avg} for T_{proof} = 2 years	3.82×10^{-5}
PFD_{avg} for T_{proof} = 5 years	9.59×10^{-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.

Table 2.2

KFD2-SL-4

Parameters acc. to IEC 61508	Values
Assessment type and documentation	FMEDA report
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function	Outputs de-energized when common disable input is de-energized
HFT	0
SIL	2
$\lambda_{sd} + \lambda_{su}$	324 FIT
λ_{dd}	0 FIT
λ_{du}	1.0 FIT
$\lambda_{total\ (safety\ function)}$	325 FIT
SFF	99.69 %
MTBF [1]	351 years
PFH	1.0×10^{-9} 1/h
PFD_{avg} for T_{proof} = 1 year	4.39×10^{-6}
PFD_{avg} for T_{proof} = 2 years	8.81×10^{-6}
PFD_{avg} for T_{proof} = 5 years	2.22×10^{-5}
Reaction time [2]	< 20 ms

[1] acc. to SN29500. This value includes failures which are not part of the safety function. Value for one channel only.

[2] Time between fault detection and fault reaction.

Table 2.3

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:

- KFD0-RSH-1(-Y2): input, output
- KFD2-SL-4: inputs, outputs, common disable input

3.2 Configuration

KFD0-RSH-1(-Y2)

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

KFD2-SL-4

The device is configurable. The settings do not influence the safety function. For further information see 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.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.

2014-07

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.

Maximum Switching Power of Output Contacts (KFD0-RSH-1(-Y2) only)

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.

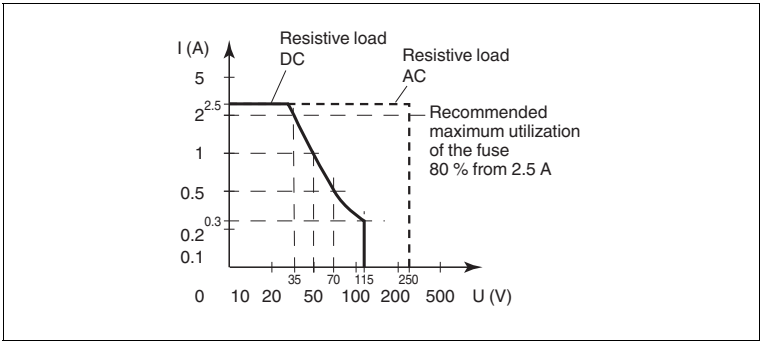

Figure 3.1

This is valid for 2 x 10^5 electrical switching cycles at maximum load. This number can be higher depending on the load attached.

3.4 Installation and Commissioning

During installation all aspects regarding the SIL level of the loop must be considered. The safety function must be tested to ensure the expected outputs are given. When replacing a device, the loop must be shut down. In all cases, devices must be replaced by the same type.

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:

- KFD0-RSH-1(-Y2)
  - 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
- KFD2-SL-4
  - A digital multimeter (without special accuracy) will be used as voltmeter to check switching of the transistor output. It needs a measuring range of at least 24 V DC.
  - Power supply set at nominal voltage of 24 V DC
  - A load resistor of 1 kΩ ± 10 % is necessary.

Procedure

For the proof test the tests have to be done as shown in the following tables and pictures. Test each separate channel that is used in the safety function application and the respective safety path.

KFD0-RSH-1(-Y2)

Test No.	Input	Output
1	24 V DC	0 Ω
2	0 V DC	OL (overload)

Table 4.1

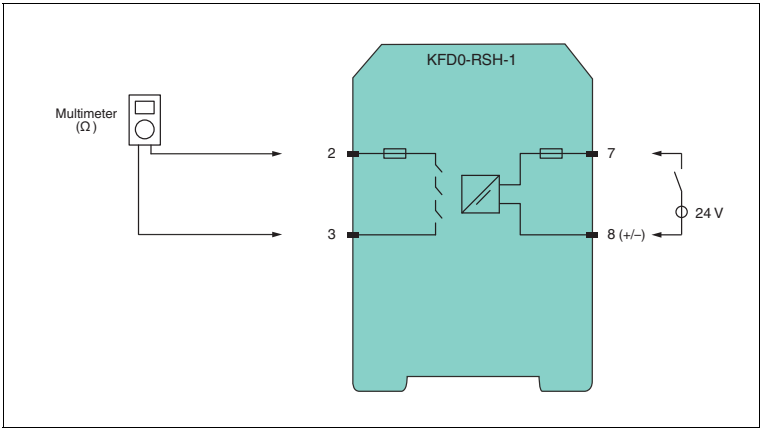

Figure 4.1 Proof test set-up for KFD0-RSH-1

The same set-up is used for KFD0-RS-1-Y2.

Within the test, the switches are used. The correct settings for the application must be established again subsequent to the test.

KFD2-SL-4

Test No.	Procedure	Input and common disable output	Output
1	Attach the input voltage subsequently to each input and check if only the related output is activated. For this test, the line fault detection DIP switches must be in OFF position (position II).	■ 24 V DC between terminals 11, 12 ■ load resistor on output	Multimeter shows 24 V DC
2	Attach the input voltage subsequently to each input and check that no output is switching. For this test, the line fault detection DIP switches must also be in OFF position (position II). The OFF LED is blinking.	■ 0 V DC between terminals 11, 12 ■ load resistor on output	Multimeter shows 0 V DC
3	For this test, the line fault detection DIP switches must be in ON position (position I) for all four signal paths. Deactivate all inputs. The OFF LED and the four channel switching status LEDs must be blinking red.	■ 24 V DC between terminals 11, 12 ■ load resistance removed	–

Table 4.2

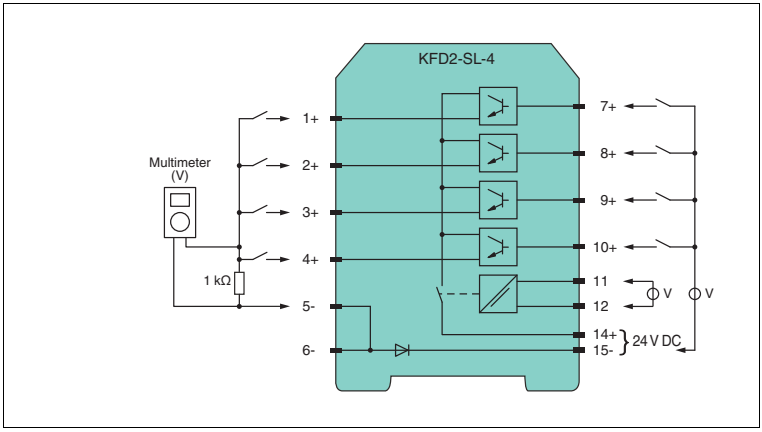

Figure 4.2 Proof test set-up for KFD2-SL-4

5 Abbreviations

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 failure 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
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
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
ETS	**E**nergized **T**o **S**afe State

2014-07

2014-07

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-2867A
07/2014