SAFETY MANUAL SIL

SOLENOID DRIVER
KFD2-RCI-(EX)1

SIL
IEC 61508/61511

ISO9001

CE

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"

1 Introduction 4
1.1 General Information 4
1.2 Intended Use 4
1.3 Manufacturer Information 4
1.4 Relevant Standards and Directives 5
2 Planning 6
2.1 System Structure 6
2.1.1 Low Demand Mode 6
2.1.2 High Demand Mode 6
2.2 Assumptions 7
2.3 Safety Function and Safe State 7
2.4 Characteristic Safety Values 8
3 Safety Recommendation 9
3.1 Interfaces 9
3.2 Configuration 9
3.3 Useful Life Time 9
3.4 Installation and Commissioning 9
4 Proof Test 10
4.1 Proof Test Procedure 10
5 Explanations to the Characteristic Safety Values 15
5.1 Proof Test Interval dependent PFD_{avg} 15
5.2 Safe Failure Fraction Calculation 16
6 Abbreviations 17

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.

Assembly, installation, commissioning, maintenance and operation of any devices may only be carried out by trained, qualified personnel who have read and understand the instruction manual.

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 isolated barrier is used for intrinsic safety applications. It supplies power to safety valve controller with HART capability. It is controlled by means of a logic circuit and loop powered.

This device provides the HART pass-through for maintenance and diagnostic of the solenoid valve. The HART communication is available both in ON condition and in OFF condition of the solenoid.

The KFD2-RCI-(Ex)1 is a single device for DIN rail mounting.

For further information see chapter 3 "Safety Recommendation".

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200
68307 Mannheim/Germany

KFD2-RCI-(Ex)1

Up to SIL3

223033 2010-06

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)

223033 2010-06

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)

223033 2010-06

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Failure rates are constant, wear out mechanisms are not included.
- 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.
- 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 °C. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 °C, 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.
- 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.
- 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 24 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).
- The HART protocol is not part of the safety function. It does not transmit safety relevant messages.
- The input signal is provided by a SIL3 safety PLC or any comparable system.

2.3 Safety Function and Safe State

Safety Function

The device provides the following type A safety function: The valve current controlling output (output I) is in low condition when the controlling input (input I) is in de-energized condition.

Safe State

The safety function is defined as the output is low/de-energized (safe state: ≤ 5.6 mA).

Reaction Time

The reaction time (switch off delay) of the safety function is < 100 ms.

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables
Assessment type and documentation	Full assessment
Pepperl+Fuchs FMEDA report [1]	FS-0035EA-20A
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
HFT	0
SIL (hardware)	3
$\lambda_{sd} + \lambda_{su}$	204 FIT
λ_{du}	1 FIT
$\lambda_{total\ (safety\ function)}$	205 FIT
SFF	99 %
PTC [2]	99 %
MTBF [3]	165 years
PFH (= λ_{du})	1 x 10^{-9} 1/h
PFD_{avg} for T_1 = 1 year	4.77 x 10^{-6}
PFD_{avg} for T_1 = 2 years	9.11 x 10^{-6}
PFD_{avg} for T_1 = 5 years	2.21 x 10^{-5}
T_{proof} max. [4]	20 years
[1] Pepperl+Fuchs documentation number	
[2] PTC (**P**roof **T**est **C**overage)	
[3] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h.	
[4] Even if not required by IEC 61508, it is recommended to perform the proof test at higher frequencies than T_{proof} max. (e. g. in combination with the valves proof test) especially as these tests can be done during normal operation of the loop (no shut-down necessary, see proof test section).	

Table 2.1: Characteristic safety values KFD2-RCI-(Ex)1

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. For further information see chapter 5 "Explanations to the Characteristic Safety Values".

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

223033 2010-06

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces. For corresponding terminals see data sheet.

- Safety relevant interfaces: input I, output I
- Non-safety relevant interfaces: power supply, Power Rail failure output, output II (HART communication)

3.2 Configuration

Via a DIP switch, it is possible to switch between test mode and normal mode. Make sure that this switch is set to normal mode (exception test procedure).

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.

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.

223033 2010-06

4 Proof Test

4.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potentially dangerous failures that are otherwise not detected by diagnostic tests.

The functionality of the subsystem must be verified at periodic intervals depending on the applied PFD_{avg} in accordance with the data stated in chapter "Characteristic Safety Values" (see chapter 2.4).

Purpose

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

To perform the online proof test, the operator needs a certified (intrinsically safe) multimeter with test probes of 2 ... 2.3 mm. The blue terminal block of the device is provided with integrated test points for connections by means of 2 ... 2.3 mm standard test connectors. The terminals 1 and 2 are specifically dedicated for the test of the output loop current by means of a multimeter (range ≥ 200 mA, internal resistance ≤ 10 Ω).

Warning!
Risk of short circuit

Wrong connection can shunt the output current from the safety valve.

Connect the multimeter only between the terminals 1 and 2.
Any other connection can shunt the output current from the safety valve and send the loop in shut-down state.

Caution!
Possibility of false alarm

During the online proof test the collective error message output (available on the Power Rail and on the module KFD2-EB2B) will be activated.

Be aware of this situation and take the necessary actions to avoid false alarms.

223033 2010-06

Procedure

The KFD2-RCI-Ex1 can operate in three different conditions depending on the specific use (3 possible) of the device. The proof test must be done accordingly.

1. Energized condition (supplied with 24 V DC):
   This is the more frequently situation where the output of the KFD2-RCI-Ex1 keeps the safety valve energized at a current of about 20.4 mA. The digital input (terminals 10,11) is at logic **1** (24 V) and the power supply is at 24 V DC (terminals 14,15). For this case please choose proof test procedure for energized condition (view Table 4.1 on page 12).
2. De-energized condition (supplied with 24 V DC):
   This condition represents the **safe state** or shut-down state where the output of the KFD2-RCI-Ex1 keeps the safety valve live with a low current of about 4.2 mA. The digital input (terminals 10,11) is at logic **0** (0 V) and the power supply is at 24 V DC (terminals 14,15). For this case please choose proof test procedure for de-energized condition (view Table 4.2 on page 13).
3. Energized (loop powered):
   This is the situation, not frequently used, where the safety valve is energized at a current of about 16.2 mA provided only by the loop powered section of the KFD2- RCI-Ex1. The digital input (terminals 10,11) is at logic **1** (24 V) and the power supply is not connected (terminals 14,15). This application is typically used when the safety valve is used only for ON/OFF application without any HART communication. For this case proof test is not necessary, since the SFF for this mode of operation is 100 %.

223033 2010-06

Energized Condition

Mandatory Tests (safety relevant)

- Open the transparent cover to access at the test switch.
- Connect a certified multimeter between the terminals 1(-) and 2(+) to measure the current flowing into the safety valve.

Recommended Tests (non safety relevant)

- Measure the output current at terminals 7, 8 (source mode) or 7, 9 (sink mode).
- Check the HART pass-through communication with a HART communicator (HHC – **H**and **H**eld **C**ommunicator) between the safe area (terminals 7, 8 or terminals 7, 9 – minimum load of 230 Ω) and the safety valve in the hazardous area.
- Check the collective error message via the fault bus, if the Power Feed Module KFD2-EB2.*** is installed.

Check the following conditions (view Figure 4.1 on page 14):

Position test switch	**Safety relevant**		**Non safety relevant**			
	Safety valve status	**Safety valve current**	**LED indication**	**Output current terminals 7, 8, 9**	**HART pass-through**	**Output fault bus**
Normal mode	energized	20.4 mA ± 0.2 mA	green = ON yellow = ON red = OFF	11.0 mA ± 0.5 mA	permitted	no fault
Test mode	energized	18.6 mA ± 0.3 mA	green = ON yellow = ON red = flashing	11.0 mA ± 0.5 mA	permitted but not guaranteed	fault

Table 4.1: Conditions that must be checked

If any of the safety relevant tests is not passed then the loop must be put immediately into the safe state and the KFD2-RCI-Ex1 must be replaced as soon as possible.

If any of the recommended non safety relevant tests is not passed means that the module is faulty, but the safety function is always available on demand. The module must be replaced as soon as possible.

Restore the test switch in the normal mode and close the transparent cover. Remove the multimeter from the terminals 1, 2.

223033 2010-06

De-energized Condition

Mandatory Tests (safety relevant)

- Open the transparent cover to access at the test switch.
- Connect a certified multimeter between the terminals 1(-) and 2(+) to measure the current flowing into the safety valve.

Recommended Tests (non safety relevant)

- Measure the output current at terminals 7, 8 (source mode) or 7, 9 (sink mode).
- Check the HART pass-through communication with a HART communicator (HHC – **H**and **H**eld **C**ommunicator) between the safe area (terminals 7, 8 or terminals 7, 9 – minimum load of 230 Ω) and the safety valve in the hazardous area.
- Check the collective error message via the fault bus, if the Power Feed Module KFD2-EB2.*** is installed.

Check the following conditions (view Figure 4.1 on page 14):

Position test switch	Safety relevant		Non safety relevant			
	Safety valve status	Safety valve current	LED indication	Output current terminals 7, 8, 9	HART pass-through	Output fault bus
Normal mode	de-energized	4.2 mA ± 0.2 mA	green = ON yellow = OFF red = OFF	11.0 mA ± 0.5 mA	permitted	no fault
Test mode	de-energized	2.6 mA ± 0.3 mA	green = ON yellow = OFF red = flashing	11.0 mA ± 0.5 mA	not permitted	fault

Table 4.2: Conditions that must be checked

If any of the safety relevant tests is not passed then the loop must be put immediately into the safe state and the KFD2-RCI-Ex1 must be replaced as soon as possible.

If any of the recommended non safety relevant tests is not passed means that the module is faulty, but the safety function is always available on demand. The module must be replaced as soon as possible.

Restore the test switch in the normal mode and close the transparent cover. Remove the multimeter from the terminals 1, 2.

223033 2010-06

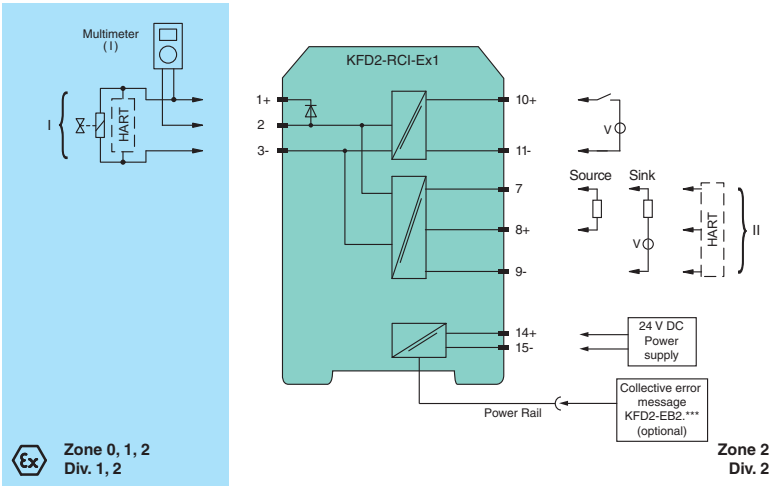


Figure 4.1: Proof test set-up for KFD2-RCI-(Ex)1
Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD2-RCI-Ex1.

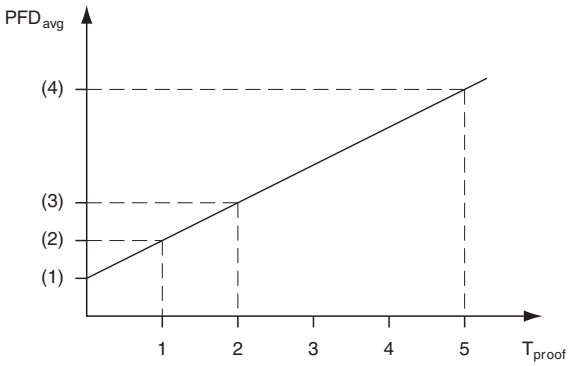
223033 2010-06

5 Explanations to the Characteristic Safety Values

5.1 Proof Test Interval dependent PFD_{avg}

The time dependent PFD_{avg} value behaves during the useful lifetime approximately linear. The following figure describes the calculation regulation to determine the proof test interval dependent PFD_{avg}.

The PFD_{avg} characteristic follows a standard linear equation: $PFD_{avg} = m \times T_{proof} + b$



General Formula

$$PFD_{avg\,(T_{proof})} = \frac{PTC \times \lambda_{du} \times 8760\ h/a}{2} \times T_{proof} + \frac{(1 - PTC) \times \lambda_{du} \times 8760\ h/a \times T_{lifetime}}{2}$$

$[T_{lifetime}] = a$ (years)

Example Calculation

For the example calculations below the following characteristic values are assumed:

$\lambda_{du} = 1$ FIT, PTC = 99 %, $T_{lifetime} = 10$ years

(1) PFD_{avg} ($T_{proof} = 0$) Proof time independent probability of failure, caused by failures which are not detectable during the proof test.

(2) PFD_{avg} for $T_1 = 1$ year: 4.77×10^{-6}

(3) PFD_{avg} for $T_1 = 2$ years: 9.11×10^{-6}

(4) PFD_{avg} for $T_1 = 5$ years: 2.21×10^{-5}

223033 2010-06

5.2 Safe Failure Fraction Calculation

The SFF value (**S**afe **F**ailure **F**raction value) is used as an architectural constraint for functional safety related elements. It expresses the ratio of safe failures to the total failure budget of the safety related element. This ratio is represented by the following equation:

$$SFF = \frac{\lambda_{safe} + \lambda_{dd}}{\lambda_{total\ (safety\ function)}} = \frac{\lambda_{sd} + \lambda_{su} + \lambda_{dd}}{\lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}}$$

223033 2010-06

6 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

223033 2010-06

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

223033 / DOCT-1940
06/2010