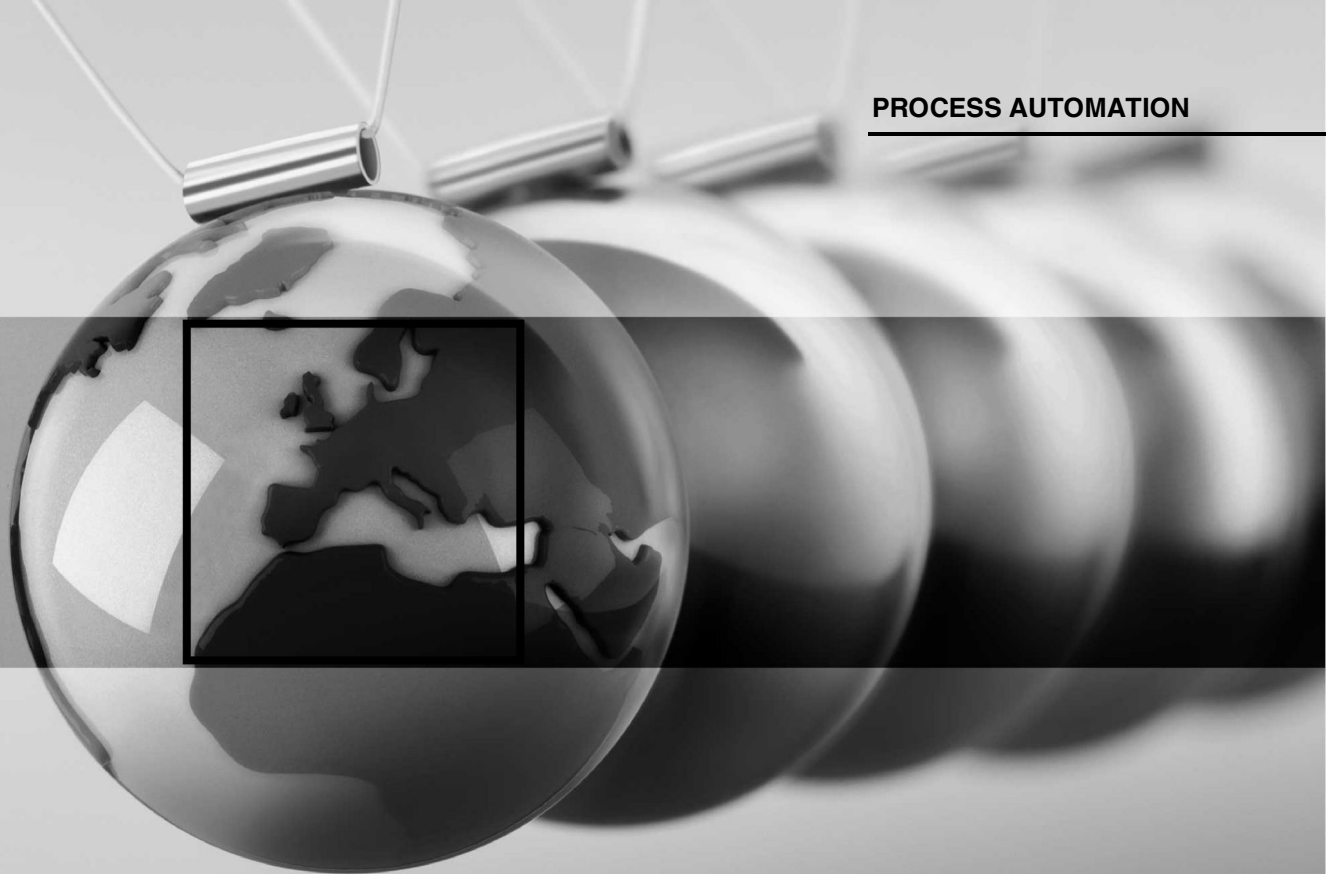




MANUAL

Functional Safety Resistance Repeater KCD2-RR2-Ex1(.SP)

SIL

IEC 61508/61511



SIL 2





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	Content of this Document.	4
1.2	Safety Information	5
1.3	Symbols Used	6
2	Product Description	7
2.1	Function	7
2.2	Interfaces	7
2.3	Marking	7
2.4	Standards and Directives for Functional Safety	7
3	Planning	8
3.1	System Structure	8
3.2	Assumptions	9
3.3	Safety Function and Safe State	10
3.4	Characteristic Safety Values	11
3.5	Useful Lifetime	12
4	Mounting and Installation	13
4.1	Configuration	13
5	Operation	14
5.1	Proof Test	14
6	Maintenance and Repair	17
7	List of Abbreviations	18



1 Introduction

1.1 Content of this Document

This document contains information for usage of the device in functional safety-related applications. 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!

This document does not substitute the instruction manual.



Note!

For full information on the product, refer to the instruction manual and 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 examination certificate
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- FMEDA report
- Assessment report
- Additional documents

For more information about Pepperl+Fuchs products with functional safety, see www.pepperl-fuchs.com/sil.



1.2 Safety Information

Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismantling lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismantling of the product. The personnel must have read and understood the instruction manual and 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

This isolated barrier is used for intrinsic safety applications.

It transfers resistance values of RTDs or potentiometers from hazardous areas to safe areas.

The device supports 2-, 3-, or 4-wire technique depending on the required accuracy.

The input card of the control system measures the same load as if it were connected directly to the resistance in a hazardous area.

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

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input and output



Note!

For corresponding connections see datasheet.

2.3 Marking

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

KCD2-RR2-Ex1(.SP)	Up to SIL 2
-------------------	-------------

2.4 Standards and Directives for Functional Safety

Device specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 7, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)
-------------------	--

System-specific standards and directives

Functional safety	IEC 61511-1:2016+COR1:2016+A1:2017 EN 61511-1:2017+A1:2017 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:

- Failure rate based on the Siemens standard SN 29500.
- 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**.
- The device will be used under average industrial ambient conditions comparable to the classification "stationary mounted" according to MIL-HDBK-217F.
Alternatively, operating stress conditions typical of an industrial field environment similar to IEC/EN 60654-1 Class C with an average temperature over a long period of time of 40 °C may be assumed. 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.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.
- The device does not have a fault bus.

SIL 2 Application

- 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.



3.3 Safety Function and Safe State

Safety Function

The device transfers analog signals from the input to the output with a tolerance of 2 % related to the full signal range.

The attached PLC must recognize a fault when the resistance drops below 15 Ω or rises above 400 Ω (for Pt100) or above 4 k Ω (for Pt1000).

The switch position of the DIP switch on the device has no influence on the safety function.

Safe State

The safe state of the output is the high impedance state ($> 100 \text{ k}\Omega$) or the fault state ($< 15 \Omega$).

Reaction Time

The reaction time for all safety functions is $< 20 \text{ ms}$.



Note!

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

Parameters	Characteristic values
Assessment type	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL	2
SC	3
Safety function	Transfer of the resistance values with an accuracy of 2%.
λ_s^1	0 FIT
λ_{dd}	134 FIT
λ_{du}	54.4 FIT
$\lambda_{total} \text{ (safety function)}^1$	188 FIT
$\lambda_{not \text{ part}}$	377 FIT
SFF ¹	71.1 %
MTBF ²	164 years
PFH	5.44×10^{-8} 1/h
PFD _{avg} for $T_1 = 1$ year	2.38×10^{-4}
PFD _{avg} for $T_1 = 2$ years	4.77×10^{-4}
PFD _{avg} for $T_1 = 3$ years	7.15×10^{-4}
PTC	100 %
Reaction time ³	< 20 ms

Table 3.1

¹ "No effect failures" are not influencing the safety function and are therefore not included in SFF and in the failure rates of the safety function.

² acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.

³ Time between fault detection and fault reaction

The characteristic safety values like PFD, SFF, HFT and T_1 are taken from the SIL report/FMEDA report. Observe that 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).



3.5 Useful Lifetime

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.

The estimated useful lifetime is greater than the warranty period prescribed by law or the manufacturer's guarantee period. However, this does not result in an extension of the warranty or guarantee services. Failure to reach the estimated useful lifetime is not a material defect.



4 Mounting and Installation



Mounting and 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



Configuring the Device

The device is configured via DIP switch. The DIP switch is on the front of the device. The switch position of the DIP switch on the device has no influence on the safety function.

1. De-energize the device before configuring the device.
2. Open the cover.
3. Configure the device via the DIP switch.
4. Close the cover.
5. Secure the DIP switch to prevent unintentional adjustments.
6. Connect the device again.



Note!

See corresponding datasheets for further information.



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

This section describes a possible proof test procedure. The user is not obliged to use this proposal. The user may consider different concepts with an individual determination of the respective effectiveness, e. g. concepts according to NA106:2018.

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 %
Use for the proof test of the intrinsic safety side of the device a special digital multimeter for intrinsically safe circuits.
If intrinsically safe circuits are operated with non-intrinsically safe circuits, they must no longer be used as intrinsically safe circuits.
- Power supply set to nominal voltage of 24 V DC
- Process calibrator with current source and current sink function with an accuracy better than 20 μ A



Proof Test Procedure

1. Put out of service the entire safety loop. Protect the application by means of other measures.
2. Connect a current source to terminals 7 and 8, see figure. Depending on the application, the current source should supply 200 μ A to 10 mA.
3. Connect a RTD simulator, see figure. Configure the device via the DIP switch according to the application.
 - For 4-wire connection: to terminals 1, 2, 3 and 4, DIP switch S1 in position II
 - For 3-wire connection: to terminals 2, 3 and 4, DIP switch S1 in position I
 - For 2-wire connection: to terminals 2 and 4, DIP switch S1 in position II
4. Secure the DIP switch to prevent unintentional adjustments. Close the cover.
5. Connect the digital multimeter to terminals 7 and 8, see figure.
6. Set the combinations of excitation currents and resistances, see table.
Use the current source and the RTD simulator.
 - ↳ The proof test is passed if the following voltage values are measured, see table.
7. To test the correct lead breakage detection, open the connections at terminals 1, 2, 3 and 4 **individually**.
 - ↳ The proof test is passed if the resistance signaled on the digital multimeter for all excitation currents is between $< 15 \Omega$ or $> 400 \Omega$.
 - ↳ The proof test is passed if the resistance signaled on the digital multimeter for a excitation current $< 1 \text{ mA}$ is between $< 15 \Omega$ or $> 4 \text{ k}\Omega$.
8. To test the correct lead breakage detection, open **all** connections at terminals 1, 2, 3 and 4.
 - ↳ The proof test is passed if the resistance signaled on the digital multimeter for all excitation currents is between $< 15 \Omega$ or $> 400 \Omega$.
 - ↳ The proof test is passed if the resistance signaled on the digital multimeter for a excitation current $< 1 \text{ mA}$ is between $< 15 \Omega$ or $> 4 \text{ k}\Omega$.
9. Set back the device to the original settings for the application after the test.

Resistance	Excitation current		
	200 μ A	1 mA	10 mA
100 Ω	0.02 V $\pm$ 1.25 mV	0.1 V $\pm$ 0.25 mV	1 V $\pm$ 2.5 mV
400 Ω	0.08 V $\pm$ 5 mV	0.4 V $\pm$ 1 mV	4 V $\pm$ 10 mV
1 k Ω	0.24 V $\pm$ 15 mV	1.2 V $\pm$ 3 mV	–
4 k Ω	0.8 V $\pm$ 50 mV	4 V $\pm$ 10m V	–

Table 5.1 Resistance values, excitation currents and resulting voltages to test correct operation

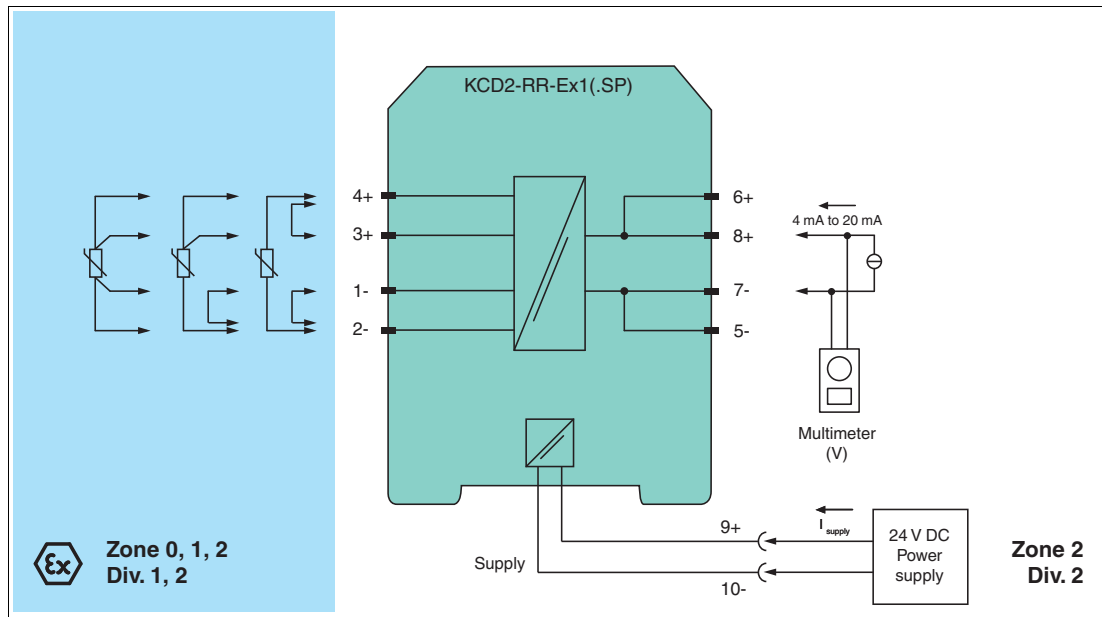


Figure 5.1 Proof test set-up for KCD2-RR2-Ex1(.SP)

6 Maintenance and Repair



Danger!

Danger to life from missing safety function

Changes to the device or a defect of the device can lead to device malfunction.
The function of the device and the safety function is no longer guaranteed.

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. While the device is maintained, repaired or replaced, the safety function does not work.
Take appropriate measures to protect personnel and equipment while the safety function is not available.
Secure the application against accidental restart.
3. Do not repair a defective device. A defective device must only be repaired by the manufacturer.
4. If there is a defect, always replace the device with an original device.



7

List of Abbreviations

ESD	Emergency Shutdown
FIT	Failure In Time in 10^{-9} 1/h
FMEDA	Failure Mode, Effects, and Diagnostics Analysis
λ_s	Probability of safe failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{\text{no effect}}$	Probability of failures of components in the safety loop that have no effect on the safety function. The no effect failure is not used for calculation of SFF.
$\lambda_{\text{not part}}$	Probability of failure of components that are not in the safety loop
$\lambda_{\text{total (safety function)}}$	Probability of failure of components that are in the safety loop
HFT	Hardware Fault Tolerance
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PCS	Process Control System
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of dangerous failure per hour
PLC	Programmable Logic Controller
PTC	Proof Test Coverage
SC	Systematic Capability
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T₁	Proof Test Interval



PROCESS AUTOMATION – PROTECTING YOUR PROCESS



Worldwide Headquarters

Pepperl+Fuchs Group
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

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

 **PEPPERL+FUCHS**
PROTECTING YOUR PROCESS

DOCT-6482A
11/2019