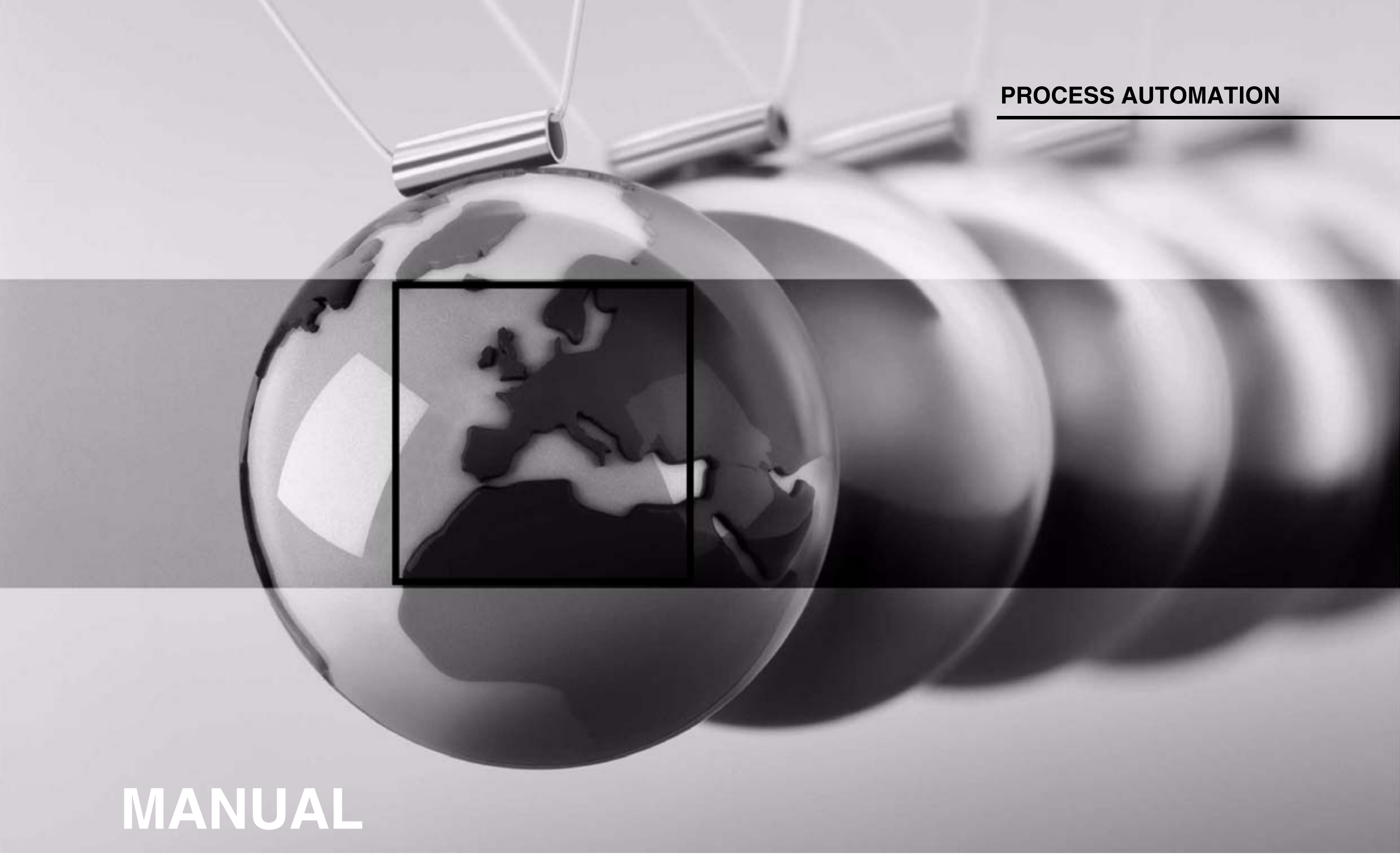
PROCESS AUTOMATION



MANUAL

Functional Safety

Switch Amplifier
KCD2-SR-(Ex)*(.LB)(.SP), HiC282*

SIL

IEC 61508/61511

ISO9001

SIL 2

PEPPERL+FUCHS

PROTECTING YOUR PROCESS

PEPPERL+FUCHS

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 dismounting lies with the plant operator.

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

KCD2-SR-1.LB(.SP)

This signal conditioner provides the galvanic isolation between field circuits and control circuits. The device transfers digital signals (NAMUR sensors or dry contacts) from the field to the control system.

The proximity sensor or the mechanical contact controls the normally open relay output for the control side load. The device output changes the state when the input signal changes the state.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

Via switch the function of the second output can be defined as a signal output or a fault indication output.

During an error condition, the relay reverts to its de-energized state and the LEDs indicate the fault according to NAMUR NE44.

If the device is operated via Power Rail, additionally a collective error message is available.

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

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

KCD2-SR-Ex1.LB(.SP)

This isolated barrier is used for intrinsic safety applications. The device transfers digital signals from NAMUR sensors or dry contacts from the hazardous area to the non-hazardous area.

The device transfers digital signals (NAMUR sensors or dry contacts) from the field to the control system.

The proximity sensor or the mechanical contact controls the normally open relay output for the control side load. The device output changes the state when the input signal changes the state.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

Via switch the function of the second output can be defined as a signal output or a fault indication output.

During an error condition, the relay reverts to its de-energized state and the LEDs indicate the fault according to NAMUR NE44.

If the device is operated via Power Rail, additionally a collective error message is available.

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

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

KCD2-SR-2(.SP)

This signal conditioner provides the galvanic isolation between field circuits and control circuits. The device transfers digital signals (NAMUR sensors or dry contacts) from the field to the control system.

The proximity sensor or the mechanical contact controls the normally open relay output for the control side load. The device output changes the state when the input signal changes the state.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

During an error condition, the relay reverts to its de-energized state and the LEDs indicate the fault according to NAMUR NE44.

If the device is operated via Power Rail, additionally a collective error message is available.

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

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

KCD2-SR-Ex2(.SP)

This isolated barrier is used for intrinsic safety applications. The device transfers digital signals from NAMUR sensors or dry contacts from the hazardous area to the non-hazardous area.

The device transfers digital signals (NAMUR sensors or dry contacts) from the field to the control system.

The proximity sensor or the mechanical contact controls the normally open relay output for the control side load. The device output changes the state when the input signal changes the state.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

During an error condition, the relay reverts to its de-energized state and the LEDs indicate the fault according to NAMUR NE44.

If the device is operated via Power Rail, additionally a collective error message is available.

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

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

HiC2821

This isolated barrier is used for intrinsic safety applications. The device transfers digital signals from NAMUR sensors or dry contacts from the hazardous area to the non-hazardous area.

The proximity sensor or the mechanical contact controls the normally open relay output for the control side load. The device output changes the state when the input signal changes the state.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

Via switch the function of the second output can be defined as a signal output or a fault indication output.

During an error condition, the relay reverts to the de-energized state and LEDs indicate the fault according to NAMUR NE44. A separate output bus is available.The fault conditions are monitored via a Fault Indication Board.

This device mounts on a HiC termination board.

HiC2822

This isolated barrier is used for intrinsic safety applications. The device transfers digital signals from NAMUR sensors or dry contacts from the hazardous area to the non-hazardous area.

The proximity sensor or the mechanical contact controls the normally open relay output for the control side load. The device output changes the state when the input signal changes the state.

Via switches the mode of operation can be reversed and the line fault detection can be switched off.

During an error condition, the relay reverts to the de-energized state and LEDs indicate the fault according to NAMUR NE44. A separate output bus is available.The fault conditions are monitored via a Fault Indication Board.

This device mounts on a HiC termination board.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces:
  KCD2-SR-(Ex)1.LB(.SP), HiC2821: input I, output I, output II
  KCD2-SR-(Ex)2(.SP), HiC2822: input I, input II, output I, output II
- Non-safety relevant interfaces: fault output

Note!
For corresponding connections see datasheet.

2.3 Marking

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

KCD2-SR-1.LB(.SP), KCD2-SR-Ex1.LB(.SP) KCD2-SR-2(.SP), KCD2-SR-Ex2(.SP) HiC2821, HiC2822	Up to SIL 2

2.4 Standards and Directives for Functional Safety

Device-specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 2, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1, edition 2003: 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.
- Only one input and one output are part of the safety function (only for 2-channel version).
- 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 ºC may be assumed. For a higher average temperature of 60 ºC, 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 indication of a dangerous failure (via fault bus) is detected within 1 hour by the programmable logic controller (PLC).

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

Safe State

The safe state is the de-energized state of the outputs, independent of the mode of operation.

Safety Function

The safety function has 2 modes of operation:

- normal operation (output follows input)
- inverted operation (output inverts input)

The 1-channel devices have 2 outputs where output II may be used in safety-relevant applications if output II is configured to follow output I.

Use the following DIP switch settings for safety-related applications:

DIP Switch Settings 1-channel Devices

Function	Mode	KCD2-SR-(Ex)1.LB(.SP)	HiC2821
Mode of operation output I	normal mode	S1 position I	S1 position II
	inverted mode	S1 position II	S1 position I
Assignment output II	follow output I	S2 position I	S3 position I
	LB/SC detection [1]	S2 position II	S3 position II
Line fault detection	ON	S3 position I	S2 position I
	OFF [2]	S3 position II	S2 position II

Table 3.1

1 This switch setting may not be used if output II is used for safety-relevant applications.
2 This switch setting may not be used if the device is used for safety-relevant applications.

DIP Switch Settings 2-channel Devices

Function	Mode	KCD2-SR-(Ex)2(.SP)	HiC2822
Mode of operation channel 1	normal mode	S1 position I	S1 position II
	inverted mode	S1 position II	S1 position I
Mode of operation channel 2	normal mode	S2 position I	S3 position II
	inverted mode	S2 position II	S3 position I
Line fault detection channel 1	ON	S3 position I	S2 position I
	OFF [1]	S3 position II	S2 position II
Line fault detection channel 2	ON	S4 position I	S4 position I
	OFF [1]	S4 position II	S4 position II

Table 3.2

1 This switch setting may not be used if the channel is used for safety-relevant applications.

LB/SC Diagnosis

The input loops of all versions are supervised, if the line fault detection is active (mandatory, see datasheet). The related safety function is defined as the outputs are in fault state (safe state), if there is a line fault detected.

Note!
The fault indication output is not safety relevant.

Reaction Time

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

Note!
See corresponding datasheets for further information.

3.4 Characteristic Safety Values

Parameters	Characteristic values	
Assessment type and documentation	Full assessment	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0	
SIL (SC)	2	
Safety function	1 relay output for 1 channel	2 relay outputs for a 1-channel device
λ_s	99 FIT	126 FIT
λ_{dd}	18.2 FIT	47.5 FIT
λ_{du}	40.3 FIT	11.1 FIT
$\lambda_{total\ (safety\ function)}$ [1]	158 FIT	184 FIT
$\lambda_{not\ part}$	58 FIT	58 FIT
SFF [1]	74.5 %	93.99 %
PTC	100 %	100 %
MTBF [2]	366 years	310 years
PFH	4.03×10^{-8} 1/h	1.11×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.93×10^{-4}	5.34×10^{-5}
PFD_{avg} for T_{proof} = 2 years	3.85×10^{-4}	1.06×10^{-4}
PFD_{avg} for T_{proof} = 5 years	5.77×10^{-4}	1.59×10^{-4}
Reaction time [3]	< 20 ms	

Table 3.3

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. The value is calculated for one safety function of the device.
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 Life Time

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.

Maximum Switching Power of Output Contacts

The useful life time is limited by the maximum number of switching cycles under load conditions. The maximum number of switching cycles is depending on the electrical load and may be higher when reduced currents and voltages are applied.
You can see the relationship between the maximum switching power and the load conditions in the figures below.

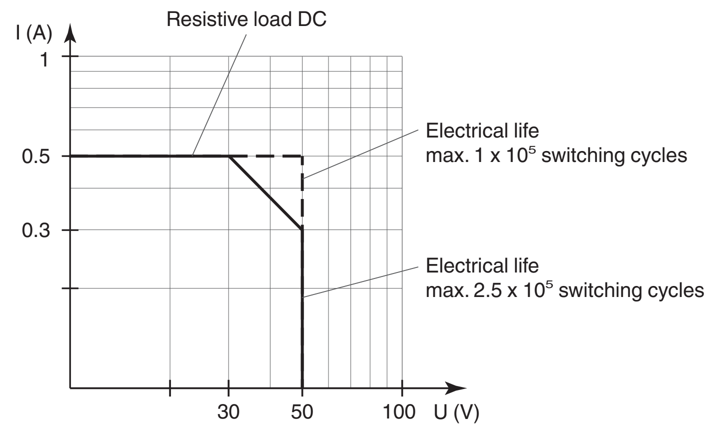


Figure 3.1 Maximum switching power of HiC282*

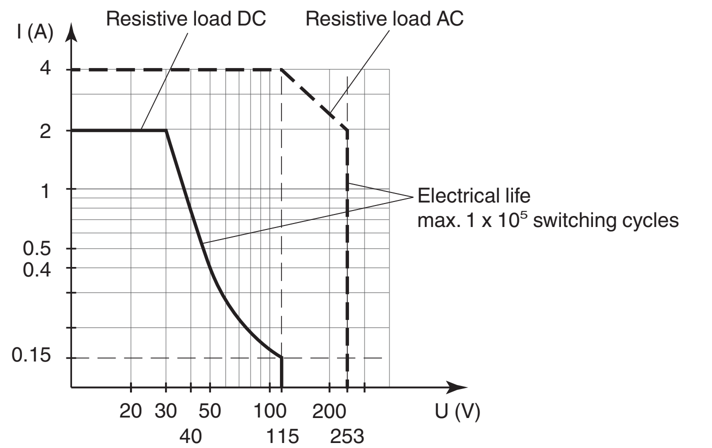


Figure 3.2 Maximum switching power of KCD2-SR-(Ex)*(.LB)(.SP)

Note!

See corresponding datasheets for further information.

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 Devices with DIP Switches on the Device Side

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the side of the device.

1. De-energize the device before configuring the device.
2. Remove the device.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Secure the DIP switches to prevent unintentional adjustments.
5. Mount the device.
6. Connect the device again.

Configuring the Devices with DIP Switches on the Front Side

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the front of the device.

1. De-energize the device before configuring the device.
2. Open the cover.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Close the cover.
5. Secure the DIP switches 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

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.

  Intrinsically safe circuits that were operated with non-intrinsically safe circuits may not be used as intrinsically safe circuits afterwards.
- Power supply set to nominal voltage of 24 V DC

Proof Test Procedure

1. Put out of service the entire safety loop. Protect the application by means of other measures.
2. Prepare a test set-up, see figures below.
3. Simulate the sensor state by connecting a potentiometer, a resistor for short circuit detection or by a resistor for lead breakage detection.
   Test each input channel individually.
4. Connect a potentiometer of 4.7 kΩ (threshold for normal operation) to the input.

   ↳ The threshold must be between 1.4 mA and 1.9 mA, the hysteresis must be between 170 µA and 250 µA.
   - If the input current is above the threshold the relay must be activated for normal mode of operation. The yellow LED lights up.
   - If the input current is below the threshold the relay must be activated for inverted mode of operation. The yellow LED lights up.
5. Connect a resistor R_{SC} of 220 Ω or a resistor R_{LB} of 150 kΩ to the input.

   ↳ The device detects an external fault. The relay of the corresponding channel must be de-activated. The red LED flashes.
6. Test both relay outputs with a specific current, e. g. 100 mA. To avoid electric shock, use a test voltage of 24 V DC. Check that the relay contacts are open.

   ↳ The relays must be de-activated. The relay contacts must **definitely open**.
7. Set back the device to the original settings for the application after the test.
8. Check the correct behavior of the safety loop. Is the configuration correct?
9. Secure the DIP switches to prevent unintentional adjustments.

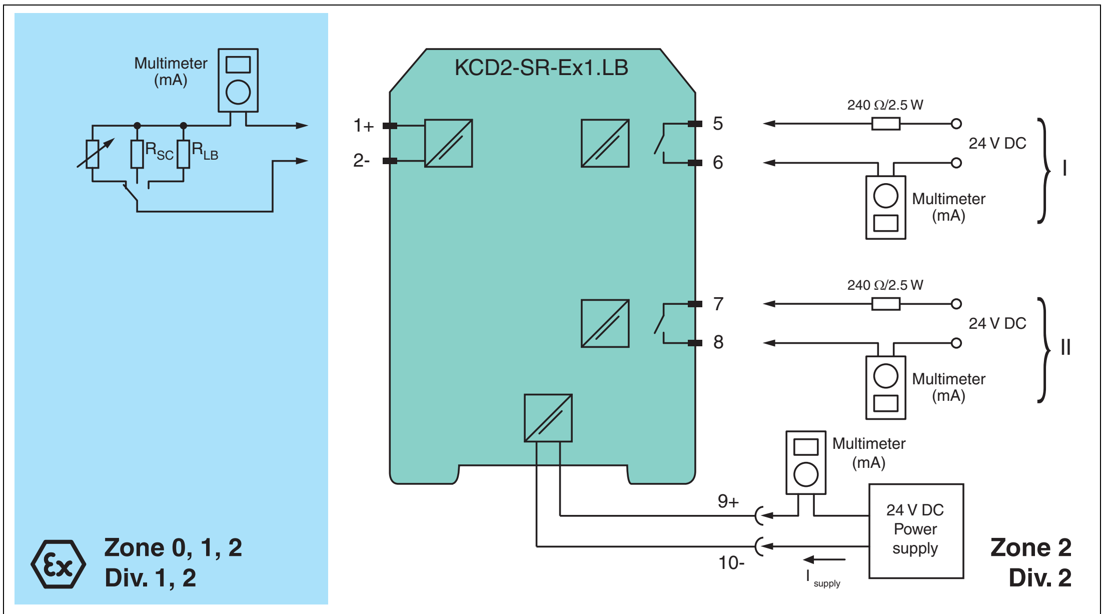


Figure 5.1 Proof test set-up for KCD2-SR-(Ex)1.LB(.SP)

Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD2-SR-Ex1.LB(.SP).

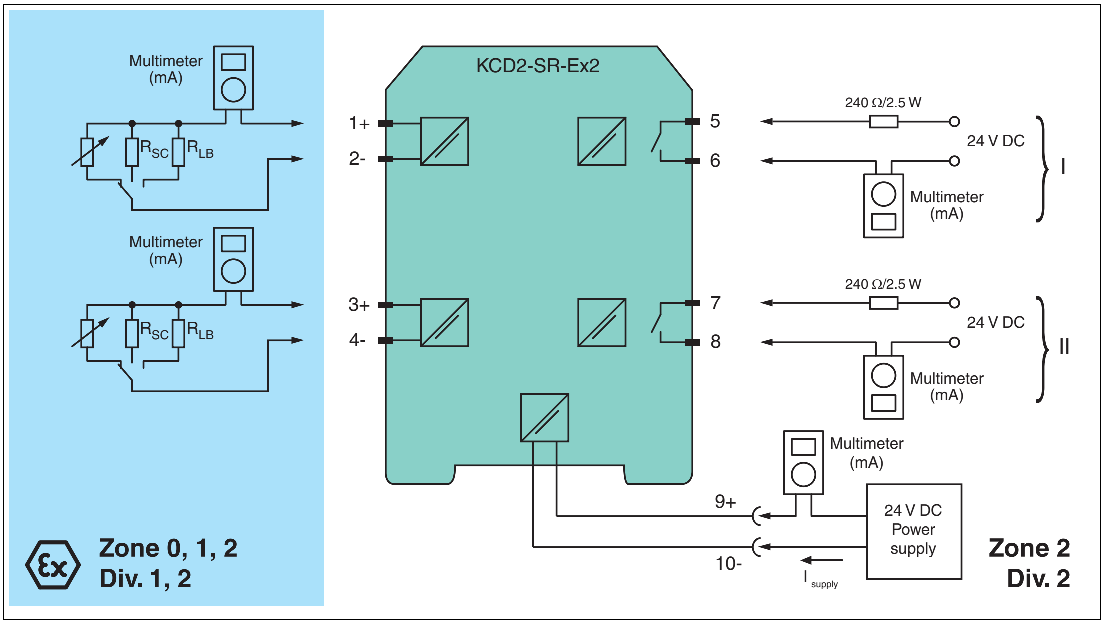


Figure 5.2 Proof test set-up for KCD2-SR-(Ex)2(.SP)

Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD2-SR-Ex2(.SP).

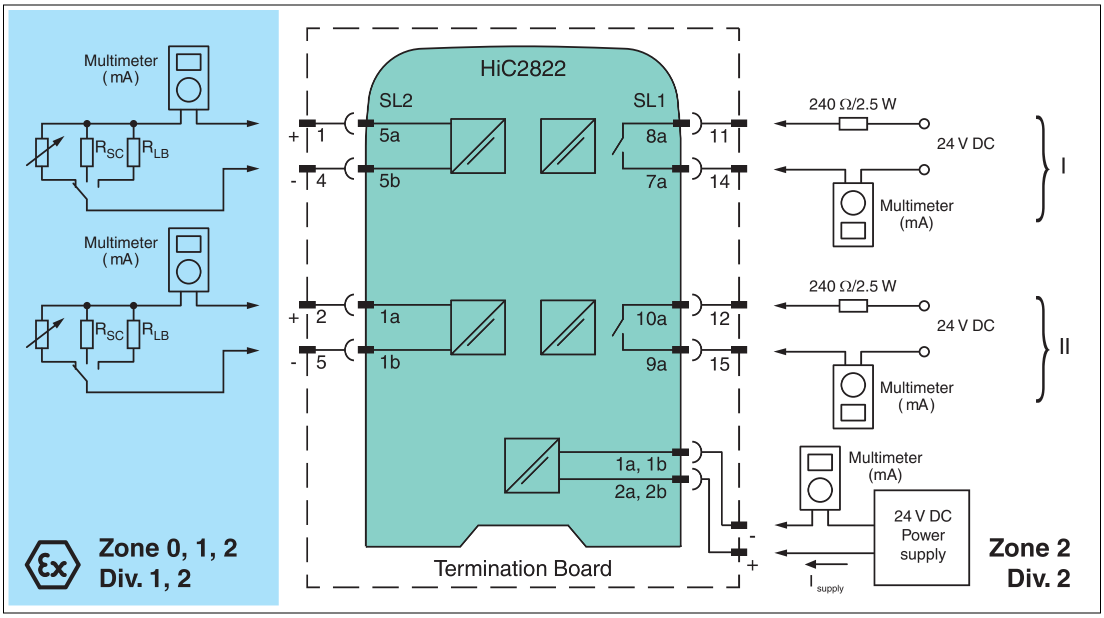


Figure 5.3 Proof test set-up for HiC2821, HiC2822

Channel 2 only for HiC2822.

Tip

The easiest way to test HiC devices is by using a stand-alone HiCTB**-SCT-***-**-** termination board. In this test, it is not necessary to disconnect the wiring of the existing application. Faults in a subsequent wiring can be avoided.

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	**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 loop that have no effect on the safety function. The no effect failure is not used for calculation of SFF.
$\lambda_{not\ part}$	Probability of failure of components that are not in the safety loop
$\lambda_{total\ (safety\ function)}$	Probability of failure of components that are in the safety loop
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
MTTR	**M**ean **T**ime **T**o **R**estoration
PCS	**P**rocess **C**ontrol **S**ystem
PFD$_{avg}$	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
PLC	**P**rogrammable **L**ogic **C**ontroller
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
SIL (SC)	**S**afety **I**ntegrity **L**evel (**S**ystematic **C**apability)
SIS	**S**afety **I**nstrumented **S**ystem
T$_1$	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

PEPPERL+FUCHS

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-1595J
12/2018