SAFETY MANUAL SIL

Switch Amplifier

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

SIL
IEC 61508/61511

ISO9001

CE

SIL2

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"

2014-09

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.

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 a fault is detected within the device, it must be taken out of service and action taken to protect against accidental use. Devices shall 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

The devices are available as safe area version (KCD2-SR-*(.LB)(.SP)) where they can be used as a signal conditioner providing isolation for non-intrinsically safe applications. Also the devices are available as hazardous area version (KCD2-SR-Ex*(.LB)(.SP), HiC282*) allowing use as isolated barriers for intrinsic safety applications.

The safe area versions transfer digital signals (NAMUR sensors/mechanical contacts) via a galvanic isolation. The hazardous area versions transfer these signals from a hazardous to a safe area.

The proximity sensor or switch controls a normally open relay output for the safe area load. The device output changes state when the input signal changes state. The normal output state can be reversed via DIP switches.

In the KCD2-SR-(Ex)1.LB(.SP) versions, output II can be switched to either follow output I or to detect faults on the input line (line break, short circuit).

Line fault detection (LFD) can be selected or disabled via a DIP switch.

During an error condition the outputs de-energize.

2014-09

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

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

The KCD2-SR-(Ex)*(.LB)(.SP) is a single device for DIN rail mounting while the HiC282* is a plug-in device to be inserted into a specific Termination Board.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

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

Up to SIL2

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 – 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.

2014-09

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.
- 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.
- 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).

2.3 Safety Function and Safe State

The safe state of each channel is "output de-energized", independent of the mode of operation.

The safety function has two modes of operation:

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

The one channel devices have two outputs where output II may be used in safety relevant applications if it is configured to follow output I.

Therefore the DIP switch settings for all channels used in safety relevant applications are:

DIP Switch Settings 1-channel Devices

Function	Mode	KCD2-SR-(Ex)1.LB(.SP)	HiC2821
Output I normal mode	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

[1] This mode 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.

Table 2.1

DIP Switch Settings 2-channel Devices

Function	Mode	KCD2-SR-(Ex)2(.SP)	HiC2822
Mode channel 1	normal mode	S1 position I	S1 position II
	inverted mode	S1 position II	S1 position I
Mode 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

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

Table 2.2

LB/SC Diagnosis

The input loop of all versions is supervised, if the line fault detection is active (mandatory, see data sheet). The related output goes to the safe state in case of line fault.

2014-09

Note!

The failure outputs are not safety relevant.

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	Full assessment	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0	
SIL	2	
Safety function	One relay output of one channel	Two relay outputs of a one channel device in series
λ_s	189 FIT	216 FIT
λ_{dd}	18 FIT	48 FIT
λ_{du}	47 FIT	45 FIT
$\lambda_{no\ effect}$	89 FIT	90 FIT
$\lambda_{total\ (safety\ function)}$	254 FIT	309 FIT
$\lambda_{not\ part}$	58 FIT	58 FIT
SFF	81.55 %	85.4 %
MTBF [1]	365 years	311 years
PFH	4.68×10^{-8} 1/h	4.51×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	2.05×10^{-4}	1.97×10^{-4}
PFD_{avg} for T_{proof} = 2 years	4.10×10^{-4}	3.95×10^{-4}
PFD_{avg} for T_{proof} = 5 years	1.02×10^{-3}	9.86×10^{-4}
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 2.3

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:
  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: output ERR

3.2 Configuration

The device must be configured through the user accessible DIP switches for the required output function before the start-up. During the functionality any change of the operating function (DIP switch modification) can invalidate the safety function behavior and must be avoided.

The KCD2 devices provide a suitable cover to protect against accidental changes while on the HiC devices the access to the DIP switch is permitted only through a small window on the side and by a small screw driver.

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.

2014-09

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

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 diagrams below.

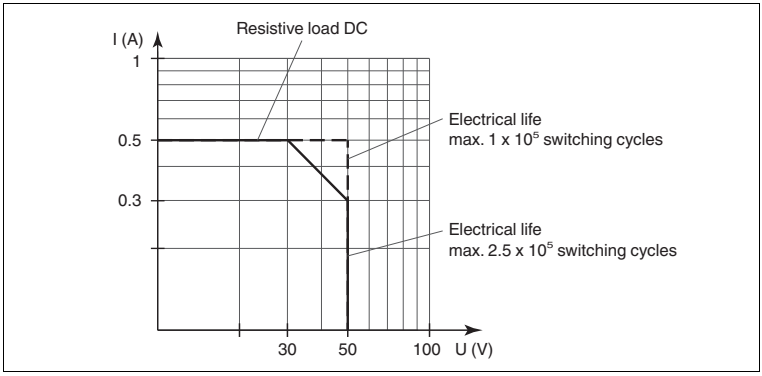

Figure 3.1 Maximum switching power of HiC282*

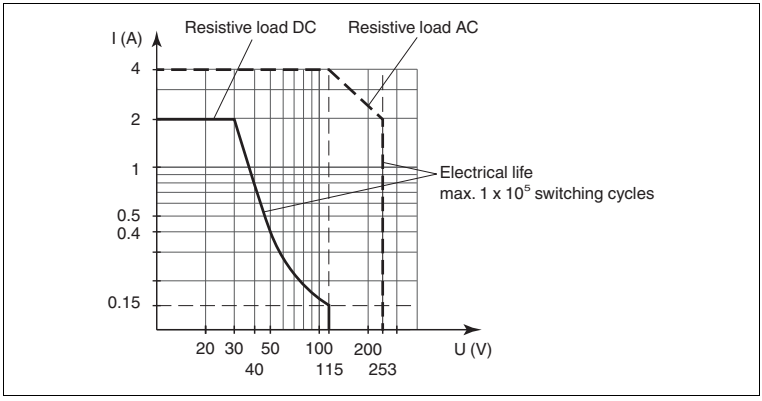

Figure 3.2 Maximum switching power of KCD2-SR-(Ex)*(.LB)(.SP)

2014-09

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 fails 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 intrinsically safe circuits must be used.

  Intrinsically safe circuits that were operated with non-intrinsically safe circuits 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:

Sensor state must be simulated by a potentiometer of 4.7 kΩ (threshold for normal operation), by a resistor of 220 Ω (short circuit detection) and by a resistor of 150 kΩ (lead breakage detection).

The input test needs to be done for each input channel individually. The threshold must be between 1.4 mA and 1.9 mA, the hysteresis must be between 170 µA and 250 µA.

- For normal mode of operation the relay must be activated (yellow LED on), if the input current is above the threshold.
- For inverse mode of operation the relay must be activated (yellow LED on), if the input current is below the threshold.

If the resistor R_{SC} (220 Ω) or the resistor R_{LB} (150 kΩ) is connected to the input, the unit must detect an external error. The red LED shall be flashing and the relay of the corresponding channel shall de-activate.

Both relay outputs need to be tested with a certain current, i. e. 100 mA. To avoid any electrical shock problems, we recommend to use 24 V DC for this test. For the philosophy of Functional Safety it is important to test, that the relay contacts are **definitely open**, if the relay is de-activated.

After the test the unit needs to be set back to the original settings for the current application. Further the switches for the settings need to be saved against undeliberate changes. This can be achieved by means of a (translucent) adhesive label, for HiC units across the hole where the switches are underneath, for KCD2 devices by fixing the label flap.

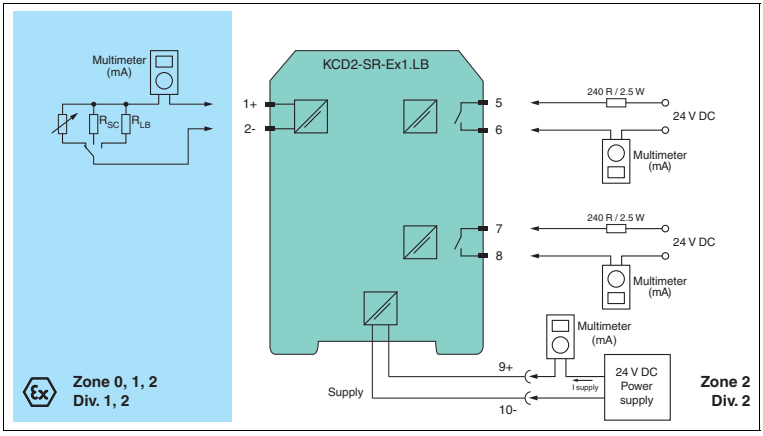

Figure 4.1 Proof test set-up for KCD2-SR-(Ex)1.LB(.SP)

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

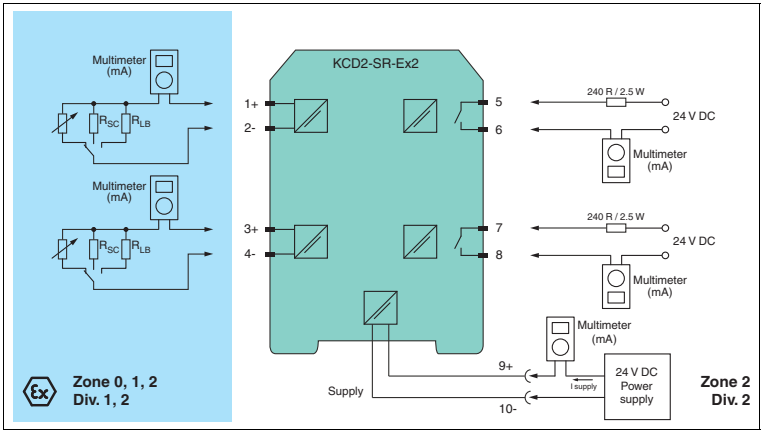

Figure 4.2 Proof test set-up for KCD2-SR-(Ex)2(.SP)

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

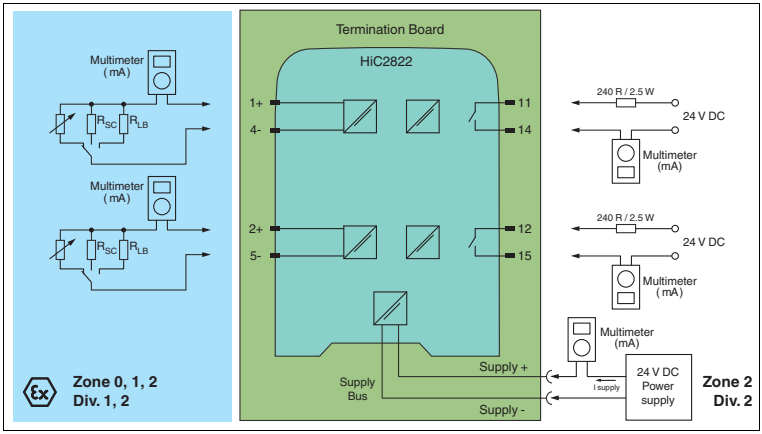

Figure 4.3 Proof test set-up for HiC2821, HiC2822

Channel 2 only for HiC2822.

Tip

Normally the easiest way to test H-System modules is by using a stand-alone HiCTB08-UNI-SC-SC Termination Board. The tester then has no need to disconnect wires in the existing application, so subsequent miswiring of the module is prevented.

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
ERR	Error
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

2014-09

2014-09

2014-09

2014-09

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-1595H
09/2014