SAFETY MANUAL SIL

SWITCH AMPLIFIER

KCD2-SR-(EX)*.(LB), 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"

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, commissioning, operation, maintenance and dismounting of any devices may only be carried out by trained, qualified personnel who have read and understood 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 or the environment 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

These isolated barriers are used for intrinsic safety applications. They transfer digital signals (NAMUR sensors/mechanical contacts) from a hazardous area (KCD2-SR-1.LB and KCD2-SR-2 from a non-hazardous area) to a safe area.

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

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

The KCD2-SR-(Ex)*.(LB) 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

68301 Mannheim/Germany

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

Up to SIL2

212352 2009-07

1.4 Relevant Standards and Directives

The devices are tested and developed in accordance to the standards listed below:

- Functional safety IEC 61508 part 1-7:
  Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)
- Functional safety IEC 61511 part 1-3:
  Standard of functional safety: safety instrumented systems for the process industry sector (user)

212352 2009-07

2 Planning

2.1 System Structure

2.1.1 Definition 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 Definition 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)

2.2 Assumptions

The Hardware assessment consists of a **F**ailure **M**odes, **E**ffects and **D**iagnostics **A**nalysis (FMEDA). From the FMEDA, failure rates are determined and consequently the **S**afe **F**ailure **F**raction (SFF) is calculated for the device.

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 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}.
- 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.

212352 2009-07

- The safety-related device is considered to be of type **A** components with a Hardware Fault Tolerance of **0**.
- Since the circuit 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 SIL2 (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 8 hours (e. g. remove sensor burnout).
- 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).
- For the calculation it was also assumed that the indication of a dangerous error (via fault bus) would be detected within 1 hour by the logic solver (SPS).

2.3 Safety Function and Safe State

Safety Function 1-channel Devices

KCD2-SR-(Ex)1.LK	**HiC2821**
S1 position I (normal operation)	SW1-1 position off (normal operation)
S2 position I (output II assigned to output I)	SW1-3 position on (output II assigned to output I)
For the 1-channel device the output II will follow output I. In this case the safety function is defined as both outputs are low/de-energized (safe state), if the input is in **low** condition.	
S1 position II (inverse operation)	SW1-1 position on (inverse operation)
S2 position I (output II assigned to output I)	SW1-3 position on (output II assigned to output I)
For the 1-channel device the output II will follow output I. In this case the safety function is defined as both outputs are low/de-energized (safe state), if the input is in **high** condition.	

Safety Function 2-channel Devices

KCD2-SR-(Ex)2	**HiC2822**
S1 position I (normal operation)	SW1-1 position off (normal operation)
S2 position I (normal operation)	SW1-3 position off (normal operation)
The safety function is defined as the output is low/de-energized (safe state), if the input is in **low** condition.	
S1 position II (inverse operation)	SW1-1 position on (inverse operation)
S2 position II (normal operation)	SW1-3 position on (inverse operation)
The safety function is defined as the output is low/de-energized (safe state), if the input is in **high** condition.	

LB/SC Diagnosis

The input loop of all versions is supervised, if the line fault detection is active (mandatory, see data sheet) The related safety function is defined as the outputs are low/de-energized (safe state), if there is a line fault detected.

212352 2009-07

Note!

The failure outputs are not safety relevant.

Reaction Time

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

212352 2009-07

3 Safety Recommendation

3.1 Interfaces

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

- Safety relevant interfaces:
  KFD2-SR-(Ex)1, HiC2821: input I, output I, output II
  KFD2-SR-(Ex)2, 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.

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.

212352 2009-07

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.

212352 2009-07

4 Proof Test

4.1 Characteristic Safety Values

For the characteristic safety values like PFD/PFH, SFF, HFT and T_{proof} please refer to 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}).

4.2 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 the safety certificate available on our webpage www.pepperl-fuchs.com.

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 intrinsic safety circuits must be used. Intrinsic safety circuits that were operated with circuits of other types of protection 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_{LK} (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.

212352 2009-07

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 KCD units by fixing the label flap.

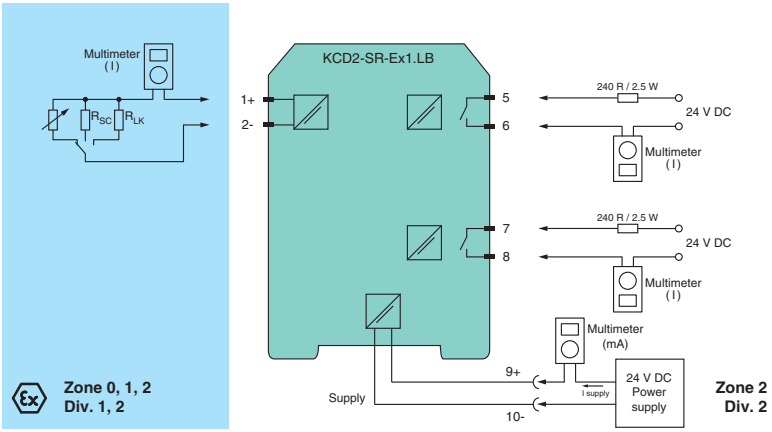

Figure 4.1: Proof test set-up for KCD-SR-(Ex)1.LB
Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD-SR-Ex1.LB.

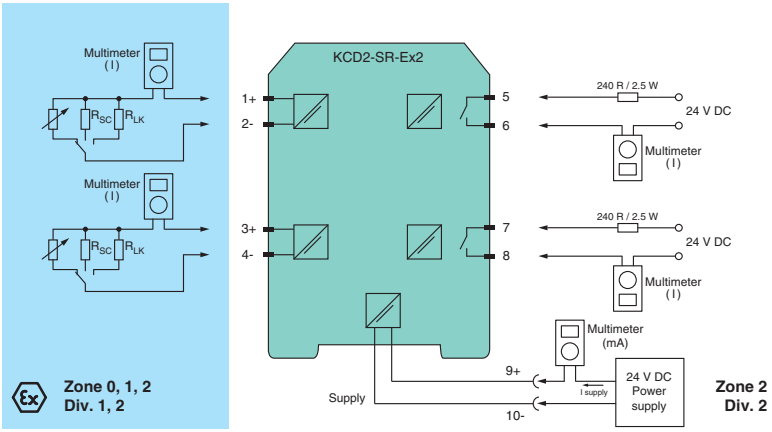

Figure 4.2: Proof test set-up for KCD-SR-(Ex)2
Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD-SR-Ex2.

212352 2009-07

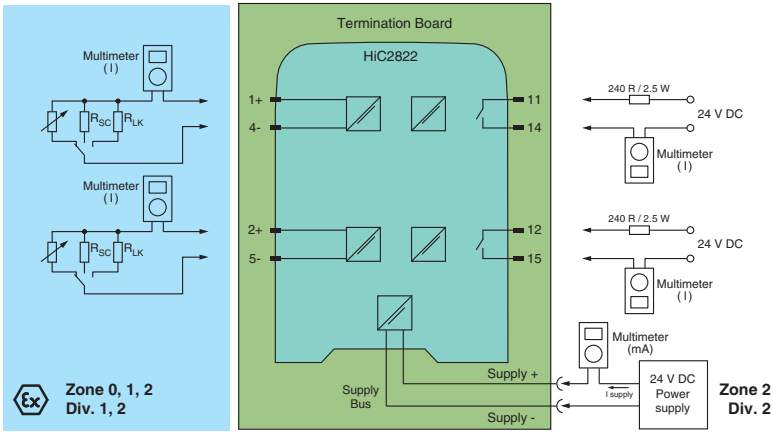

Figure 4.3: Proof test set-up for HiC2821, HiC2822
Channel 2 only for HiC2822.

Tip

For easier implementation of the test of H-System modules we propose to use a stand-alone HiCTB08-UNI-SC-SC Termination Board. By doing so a miswiring of the single module is avoided and the tester has no need to unconnect wires in an existing application.

5 Abbreviations

FMEDA	**F**ailure **M**ode, **E**ffects and **D**iagnostics **A**nalysis
HFT	**H**ardware **F**ault **T**olerance
PFD_{avg}	Average **P**robatility of **F**ailure on **D**emand
PFH	**P**robatility of dangerous **F**ailure per **H**our
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

212352 2009-07

212352 2009-07

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

For the Pepperl+Fuchs representative
closest to you check www.pepperl-fuchs.com/pfcontact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

212352 / DOCT-1595A
07/2009