SAFETY MANUAL SIL

Switch Amplifier
KCD2-SON-Ex*(.R1)(.SP)

SIL
IEC 61508/61511

ISO9001

CE

SIL2

Ex

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"

2013-06

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

General

The devices are used for intrinsic safety applications.

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

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 devices are single devices for DIN rail mounting.

KCD2-SON-Ex1(.SP)

The input controls two passive transistor outputs with a resistive output characteristic (acc. to EN60947-5-6).

The outputs have three defined states: 1-Signal = 1.8 kΩ, 0-Signal = 14 kΩ and fault > 100 kΩ

This output characteristic offers line fault transparency on the signal lines.

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

KCD2-SON-Ex1.R1

The input controls two passive transistor outputs with a resistive output characteristic.

The outputs have three defined states: 1-Signal = 6.5 V voltage drop, 0-Signal = 33 kΩ and 6.5 V voltage drop and fault > 100 kΩ

This output characteristic offers line fault transparency on the signal lines.

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

KCD2-SON-Ex2(.SP)

Each input controls a passive transistor output with a resistive output characteristic (acc. to EN60947-5-6).

The outputs have three defined states: 1-Signal = 1.8 kΩ, 0-Signal = 14 kΩ and fault > 100 kΩ

This output characteristic offers line fault transparency on the signal lines.

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

KCD2-SON-Ex2.R1

Each input controls a passive transistor output with a resistive output characteristic.

The outputs have three defined states: 1-Signal = 6.5 V voltage drop, 0-Signal = 33 kΩ and 6.5 V voltage drop and fault > 100 kΩ

This output characteristic offers line fault transparency on the signal lines.

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

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

KCD2-SON-Ex1, KCD2-SON-Ex1.R1, KCD2-SON-Ex1.SP, KCD2-SON-Ex2, KCD2-SON-Ex2.R1, KCD2-SON-Ex2.SP

Up to SIL2

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 – 7, edition 2010:
  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)

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 IEC 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 level 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 value of the device is given in this document for reference.

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- 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.
- 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.
- 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.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 24 hours (e. g. remove sensor fault).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (e. g. substitution by an equivalent device).
- The stress levels are average for an industrial environment and 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.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 Class C with an average temperature over a long period of time of 40 °C. 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 two outputs of the device use common components, these outputs must not be used in the same safety function.
- 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

Safe State

The safe state of output I and output II is the high impedant state or the error state.

The error state is an open circuit. The high impedant state is defined as 0-signal in the respective data sheet.

Safety Function

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-SON-Ex1(.R1)(.SP)
Output mode	normal mode	S1 position I
	inverted mode	S1 position II
Line fault detection	ON	S3 position I
	OFF[1]	S3 position II

[1] 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-SON-Ex2(.R1)(.SP)
Mode channel I	normal mode	S1 position I
	inverted mode	S1 position II
Mode channel II	normal mode	S2 position I
	inverted mode	S2 position II
Line fault detection channel I	ON	S3 position I
	OFF[1]	S3 position II
Line fault detection channel II	ON	S4 position I
	OFF[1]	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 safety function is defined as the outputs are in error state (safe state), if there is a line fault detected.

Reaction Time

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

Note!

The collective error message output is not safety relevant.

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables	
Assessment type and documentation	Full assessment	
Device type	A	
Mode of operation	Low Demand Mode or High Demand Mode	
HFT	0	
SIL (hardware)	2	
MTBF [1]	328 years	
Safety function	inverse operation [2]	normal operation [2]
λ_{safe} [3]	108 FIT	109 FIT
λ_{dd}	3.3 FIT	3.3 FIT
λ_{du} [3]	26.0 FIT	24.2 FIT
$\lambda_{total\ (safety\ function)}$	137 FIT	136 FIT
SFF	81 %	82 %
PFH	2.60×10^{-8} 1/h	2.42×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	1.14×10^{-4}	1.12×10^{-4}
PFD_{avg} for T_1 = 2 years	2.28×10^{-4}	2.24×10^{-4}
PFD_{avg} for T_1 = 5 years	5.69×10^{-4}	5.59×10^{-4}

[1] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h. The value is for one channel only.

[2] The device can be used in two modes of operation, inverse operation and normal operation.

[3] "Annunciation failures" do not directly influence the safety function and are therefore not considered.

Table 2.3

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.

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-SON-Ex1(.R1)(.SP): input I, output I, output II (optional)
  KCD2-SON-Ex2(.R1)(.SP): 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 devices provide a suitable cover to protect against accidental changes.

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

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 or the safety integrity of the process must be maintained by using loop redundancy. 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 failures 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 without special accuracy
  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.
- Dual power supply, set to 24 V DC resp. 8 V DC (NAMUR voltage).
- Load resistor R see Table 4.1.
- 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 settings have to be verified after the configuration by means of suitable tests.

Procedure:

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 150 µA and 250 µA.

- For normal mode of operation the output(s) must be low impedant (yellow LED on), if the input current is above the threshold. See table below, values I_{on}.
- For inverse mode of operation the output(s) must be low impedant (yellow LED on), if the input current is below the threshold. See table below, values I_{on}.

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 output of the corresponding channel shall be in error state.

For the philosophy of Functional Safety it is important to test, that the outputs are **definitely high impedant** if the yellow LED is off. See table below, values I_{off}.

Model Number	R	U	I_{on}	I_{off}	I_{err}
KCD2-SON-Ex*(.SP)	1 kΩ	8 V	2.6 mA < I_{on} < 3.2 mA	0.5 mA < I_{off} < 0.6 mA	< 0.05 mA
KCD2-SON-Ex*.R1	2 kΩ	24 V	8.0 mA < I_{on} < 9.2 mA	0.46 mA < I_{off} < 0.62 mA	< 0.05 mA

Table 4.1

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.

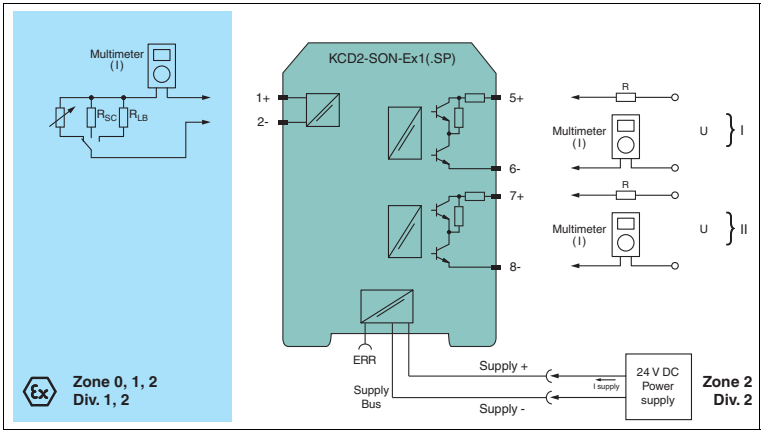

Figure 4.1 Proof test set-up for KCD2-SON-Ex1(.SP)

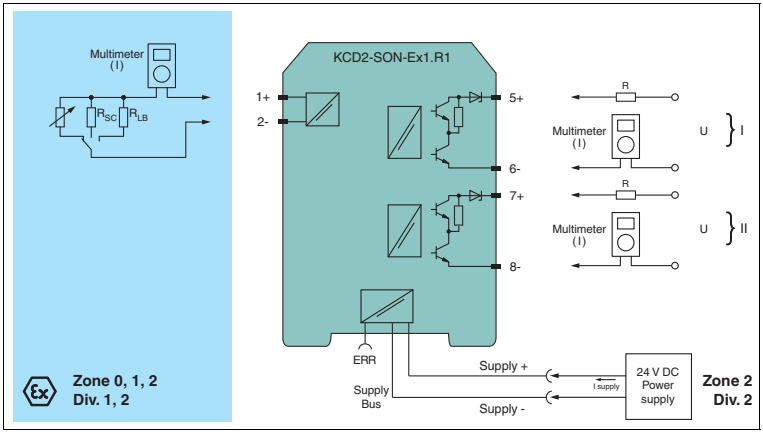

Figure 4.2 Proof test set-up for KCD2-SON-Ex1.R1

2013-06

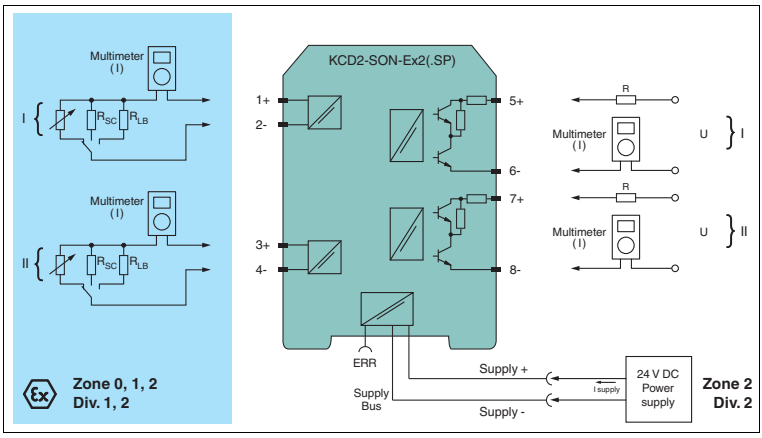

Figure 4.3 Proof test set-up for KCD2-SON-Ex2(.SP)

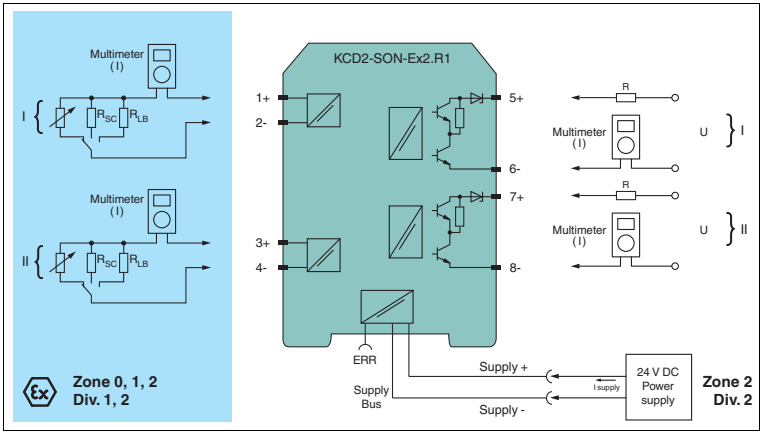

Figure 4.4 Proof test set-up for KCD2-SON-Ex2.R1

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

2013-06

2013-06

2013-06

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/contact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

TDOCT3087__ENG
06/2013