PROCESS AUTOMATION

SAFETY MANUAL SIL

SWITCH AMPLIFIER

KFD2-SOT2-Ex1.N,
KFD2-SOT2-Ex1.R1

SIL
IEC 61508/61511

ISO9001

SIL2

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

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, commissioning, operation, maintenance and dismounting of any devices may only be carried out by trained, qualified personnel. The instruction manual must be read and understood.

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, 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

This isolated barrier is used for intrinsic safety applications.

The device transfers digital signals (NAMUR sensors or dry contacts) from a hazardous area to a safe area.

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

KFD2-SOT2-Ex1.N

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

The output has three defined states: 1-Signal = 1.6 kΩ, 0-Signal = 12 kΩ and fault > 100 kΩ

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

KFD2-SOT2-Ex1.R1

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

The output has three defined states: 1-Signal = 6.5 V voltage drop,
0-Signal = 39 kΩ and fault > 100 kΩ

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

The device may only be used with K-System Termination Boards and the 16-channel DI card SDV144 from Yokogawa.

For further information see chapter 3.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200
68307 Mannheim/Germany

KFD2-SOT2-Ex1.N
KFD2-SOT2-Ex1.R1

Up to SIL2

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 – 7, 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 – 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

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 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)

2011-07

2.2 Assumptions

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}.
- 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 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 ºC. 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 ºC. For a higher average temperature of 60 ºC, 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.
- 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).
- The device must be configured for the required safety function before the start-up using the DIP switches. During the operation any change of the configuration (modification of DIP switch settings) must be avoided.

2.3 Safety Function and Safe State

Safe State

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

Safety Function

- for the output:
  - S1 position I (normal operation)
    In this case the safety function is defined as **output is high impedant** (safe state), if **low current is at input**.
  - S1 position II (inverse operation)
    In this case the safety function is defined as **output is high impedant** (safe state), if **high current is at input**.

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

1. The response time for input to output safety functions is < 0.1 ms.
   load conditions:
   - KFD2-SOT2-Ex1.N: 8 V, 1 kΩ
   - KFD2-SOT2-Ex1.R1: 24 V, 2 kΩ
2. The fault detect and fault reaction time is < 100 ms.
   (failure diagnosis at the input leads to error state)
3. The failure output reaction time is < 100 ms.

Note!

The failure output is not safety relevant.

2011-07

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables
Assessment type and documentation	FMEDA report
Device type	A
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL (hardware)	2
MTBF [1]	132 years
Safety function [2]	
λ_{safe}	78.3 FIT
λ_{dd}	–
λ_{du}	21 FIT
$\lambda_{no\ effect}$	108 FIT
$\lambda_{total\ (safety\ function)}$	207 FIT
SFF	89.8 %
PFH	2.1×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	9.21×10^{-5}
T_{proof} max.	10 years

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

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

Table 2.1

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: input, output
- 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 operation any change of the configuration (DIP switch modification) can invalidate the safety function behavior and must be avoided.

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

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.

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 stated in chapter "Characteristic Safety Values" (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 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.
- Dual power supply, set to 24 V DC resp. 8 V DC (NAMUR voltage).

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 150 µA and 250 µA.

- For normal mode of operation the output must be low impedant (yellow LED on), if the input current is above the threshold.
- For inverse mode of operation the output must be low impedant (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 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** (see table "Table 4.1" on page 10, I_{off}), if the yellow LED is off.

Model Number	R	U	I_{on} (mA)	I_{off} (mA)	I_{err} (mA)
KFD2-SOT2-Ex1.N	1 kΩ	8 V	2.6 mA < I_{on} < 3.2 mA	0.5 mA < I_{off} < 0.6 mA	I_{err} < 0.05 mA
KFD2-SOT2-Ex1.R1	2 kΩ	24 V	8.0 mA < I_{on} < 9.2 mA	0.46 mA < I_{off} < 0.62 mA	I_{err} < 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, across the hole where the switches are underneath.

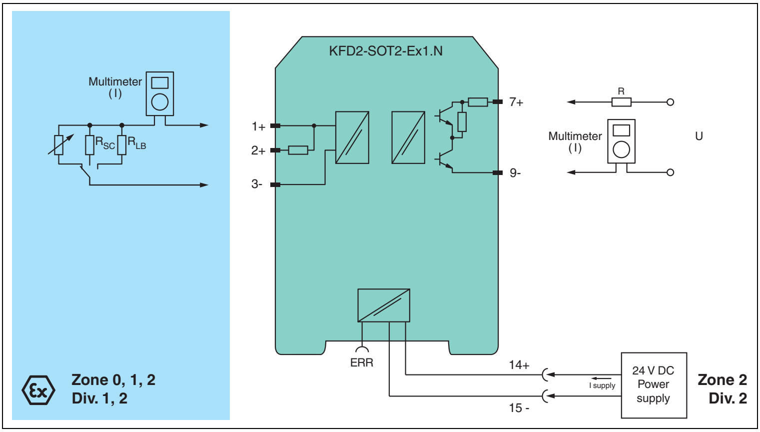

Figure 4.1 Proof test set-up for KFD2-SOT2-Ex1.N

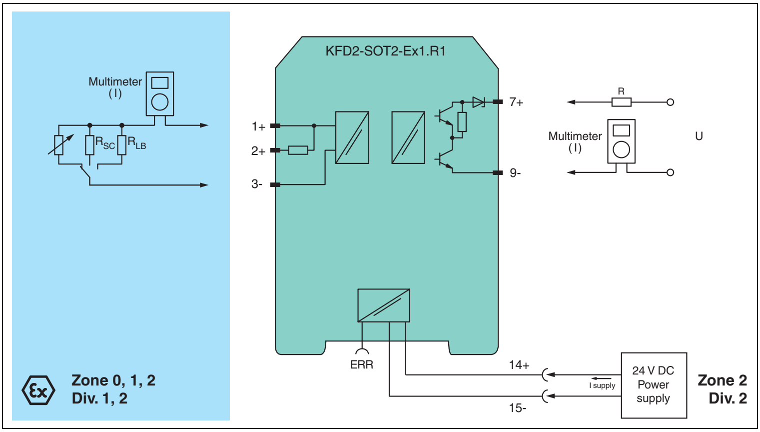

Figure 4.2 Proof test set-up for KFD2-SOT2-Ex1.R1

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**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

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

TDOCT-2505_ENG
07/2011