PROCESS AUTOMATION

SAFETY MANUAL SIL

SOLENOID DRIVER

KFD0-SD2-(Ex)*.***,**
KCD0-SD-(Ex)1.**(.SP),**
HiC2871

SIL
IEC 61508/61511

ISO9001

SIL2
SIL3

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, 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 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

The devices are available as safe area version (KFD0-SD2-*.*****, KCD0-SD-1.****(.SP)) where they can be used as a signal conditioner providing isolation for non-intrinsically safe applications. The devices are also available as hazardous area version (KFD0-SD2-(Ex)*.*****, KCD0-SD-(Ex)1.****(.SP), HiC2871) allowing use as isolated barriers for intrinsic safety applications.

The safe area versions supply power to solenoids, LEDs, and audible alarms located in a safe area. The hazardous area versions supply power to solenoids, LEDs, and audible alarms located in a hazardous area.

The devices are loop powered, so the available energy at the output is received from the input signal. The output signal has a resistive characteristic. As a result the output voltage and current are dependent on the load and the input voltage.

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 KFD0-SD2-(Ex)*.***** and KCD0-SD-(Ex)1.****(.SP) are single devices with DIN rail mounting while the HiC2871 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

KFD0-SD2-(Ex)*.*****
KCD0-SD-(Ex)1.****(.SP)
HiC2871

Up to SIL3

The stars replace a combination of characters, depending on the product.

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)

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.

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Failure rate based on the Siemens SN29500 data base.
- 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 ºC. Humidity levels are assumed within manufacturer's rating. 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.
- 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 HART protocol is only used for setup, calibration, and diagnostic purposes, not during normal operation.

SIL3 application (loop powered)

- The device shall claim less than 10 % of the total failure budget for a SIL3 safety loop.
- For a SIL3 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^{-3}, hence the maximum allowable PFD_{avg} value would then be 10^{-4}.
- For a SIL3 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-7} per hour, hence the maximum allowable PFH value would then be 10^{-8} per hour.
- Since the circuit has a Hardware Fault Tolerance of **0** and it is a type **A** component, the SFF must be > 90 % according to table 2 of IEC 61508-2 for SIL3 (sub)system.

SIL2 application (bus powered)

- 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.
- 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.

2.3 Safety Function and Safe State

Safety Function

The output is de-energized if the input is in low condition.

Safe State

The safety function is defined as the output is low/de-energized (safe state: 0 V, 0 mA).

Reaction Time

The reaction time (switch off delay) for all safety functions is < 100 ms at $I_{out} > 10$ mA.

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables
Assessment type and documentation	Full assessment
Pepperl+Fuchs FMEDA report [1]	P+F 05/07-10a R030
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function	De-energized if the input is in low condition
HFT	0
SIL (hardware)	3
$\lambda_{sd} + \lambda_{su}$	114 FIT
λ_{dd}	0 FIT
λ_{du}	0 FIT
$\lambda_{\text{total (safety function)}}$	227 FIT
SFF	100 %
MTBF [2]	451 years
PFH [3]	0 1/h
PFD_{avg} for T_1 = 1 year [3]	0
T_{proof} max. [3]	Defined in Proof Test chapter but not necessary to validate the safety values. See chapter 4.1.
Reaction time	< 100 ms

[1] Pepperl+Fuchs documentation number

[2] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h.

[3] As the λ_d failure rate is 0 FIT, a PFD calculation yields a PFD of zero, independent from the proof test interval.

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 I, input II, output I, output II
- Non-safety relevant interfaces: none

3.2 Configuration

A configuration of the device is not necessary and not possible.

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 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.

As for these loop powered modules no dangerous failures can occur there is no recurring proof test necessary.

Nevertheless we recommend to perform a regular functional test (e. g. in combination with the proof test of the final element).

With the following instructions the correct working of the basic functionality can be tested.

- 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:

- The entire measuring loop must be put out of service and the process held in safe condition by means of other measures.
- Prepare a test set-up for testing the device and perform the tests in accordance to the respective chapter.
- Restore the safety loop. Any by-pass of the safety function must be removed.

4.1.1 Proof Test Procedure KFD0-SD2-(Ex)*.*****

- Connect the module specific load resistor between the terminals 1+ and 2- (and terminals 4+ and 5- for 2-channel device).
- Connect the power supply set at nominal 20 V DC between terminals 7 and 8.
- Measure the output voltage via multimeter. Compare the resulting value to the nominal value specified in the table below.
- Short circuit the load resistor and measure the short circuit current via multimeter. Compare the resulting value to the nominal value specified in the table below.
- If applicable, repeat the test procedure for output II by connecting the power supply between the terminals 9 and 8 instead of 7 and 8 and the repetition of the output voltage and short circuit test.

Module	Output resistor (Ω)	Output voltage (V)	Short circuit current (mA)
KFD0-SD2-(Ex)1.1180	150	> 11	$80 < I_{SC} < 90$
KFD0-SD2-(Ex)2.1045	270	> 10	$45 < I_{SC} < 50$
KFD0-SD2-(Ex)1.1065	180	> 10	$65 < I_{SC} < 75$
KFD0-SD2-(Ex)1.10100	100	> 9.5	$95 < I_{SC} < 105$
KFD0-SD2-(Ex)1.1045	270	> 10	$45 < I_{SC} < 50$
KFD0-SD2-(Ex)2.1245	270	> 12	$45 < I_{SC} < 50$

Table 4.1

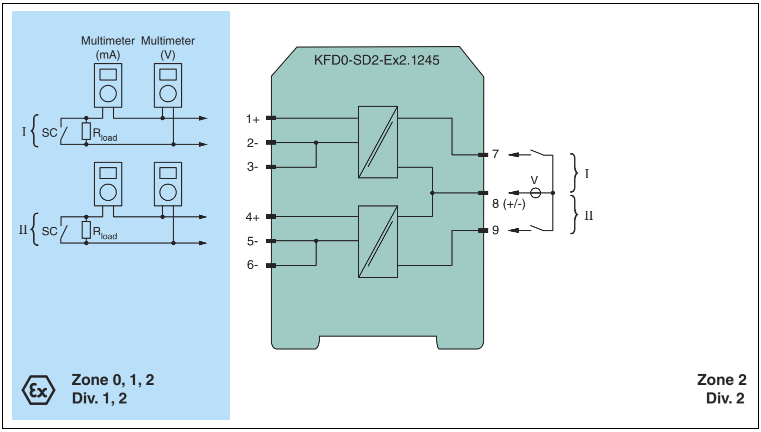

Figure 4.1 Proof test set-up for KFD0-SD2-(Ex)*.*****

Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD0-SD2-Ex*.*****.

4.1.2 Proof Test Procedure KCD0-SD-(Ex)1.****(.SP)

- Connect the module specific load resistor between the terminals 1+ and 2-.
- Connect the power supply set at nominal 20 V DC between terminals 5+ and 6-.
- Measure the output voltage via multimeter. Compare the resulting value to the nominal value specified in the table below.
- Short circuit the load resistor and measure the short circuit current via multimeter. Compare the resulting value to the nominal value specified in the table below.

Module	Output resistor (Ω)	Output voltage (V)	Short circuit current (mA)
KCD0-SD-(Ex)1.1245(.SP)	270	> 12	$45 < I_{SC} < 55$

Table 4.2

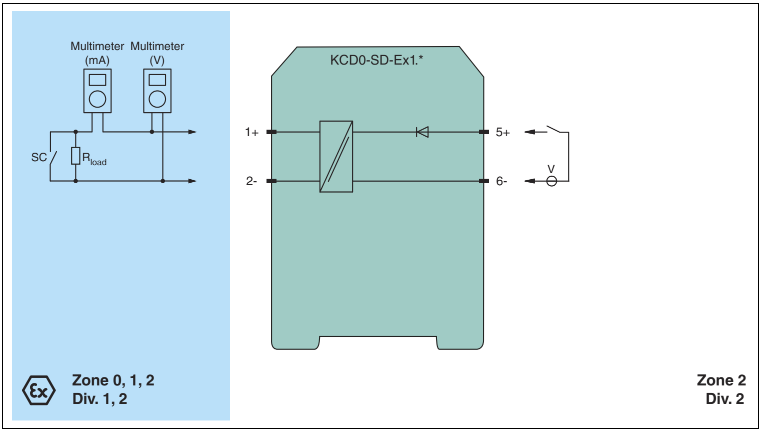

Figure 4.2 Proof test set-up for KCD0-SD-(Ex)1.****(.SP)

Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD0-SD-Ex1.****(.SP).

4.1.3 Proof Test Procedure HiC2871

- Connect the module specific load resistor between the terminals 1+ and 4-.
- Connect the power supply set at nominal 20 V DC between terminals 11+ and 14-.
- Measure the output voltage via multimeter. Compare the resulting value to the nominal value specified in the table below.
- Short circuit the load resistor and measure the short circuit current via multimeter. Compare the resulting value to the nominal value specified in the table below.

Module	Output resistor (Ω)	Output voltage (V)	Short circuit current (mA)
HiC2871	270	> 12	$45 < I_{SC} < 55$

Table 4.3

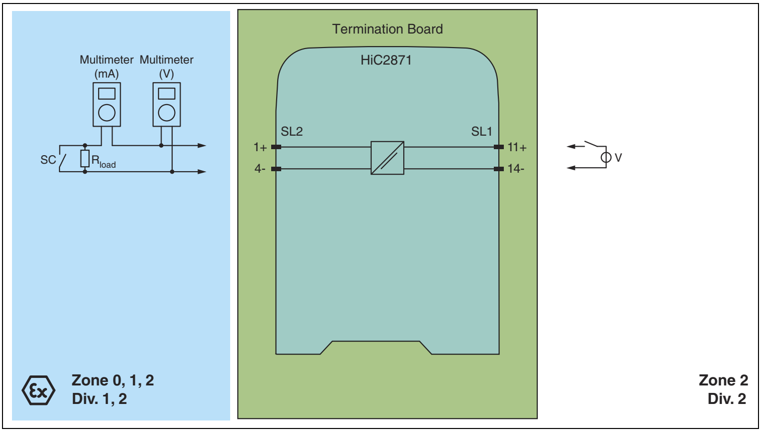

Figure 4.3 Proof test set-up for HiC2871

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

FIT	**F**ailure **I**n **T**ime
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
$\lambda_{\text{no effect}}$	Probability of failures of components in the safety path that have no effect on the safety function
$\lambda_{\text{not part}}$	Probability of failure of components that are not in the safety path
$\lambda_{\text{total (safety function)}}$	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$_{\textbf{avg}}$	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$_{\textbf{proof}}$	Proof Test Interval

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