SAFETY MANUAL SIL

SOLENOID DRIVER

KFD2-SL2-(EX)1*
KFD2-SL2-(EX)2*

SIL
IEC 61508/61511

ISO9001

CE

SIL2
SIL3

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"

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, installation, commissioning, maintenance and operation of any devices may only be carried out by trained, qualified personnel who have read and understand 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, 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

These isolated barriers are used for intrinsic safety applications. They supply power to solenoids, LEDs, and audible alarms located in a hazardous area.

The device can be bus powered or loop powered. Bus powered means that the device is powered with an auxiliary power supply. Loop powered means that the device is switched off via the supply terminals. This is shown in the "Proof Test" chapter (view Figure 4.3 on page 14). This mode of operation is only available for the single channel device versions.

It is controlled by means of a logic circuit. The 1-signal and 0-signal must be within defined ranges.

Line fault detection of the field circuit and the error bus is indicated by a red LED.

The KFD2-SL2-(Ex)1* and KFD2-SL2-(Ex)2* are single devices with DIN rail mounting.

221342 2010-01

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200
68307 Mannheim/Germany

KFD2-SL2-(Ex)1*, KFD2-SL-(Ex)2*

Up to SIL2 (bus powered, normal operation)

Up to SIL3 (loop powered, conditions see chapter 2.3)

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 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)

221342 2010-01

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)

221342 2010-01

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Failure rates are constant, wear out mechanisms are not included.
- 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.
- 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 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.

221342 2010-01

2.3 Safety Function and Safe State

Safety Function SIL2 (bus powered)

The safety function of the device is fulfilled, as long as the output represents safe state (de-energized) if the input is in low condition.

Safety Function SIL3 (loop powered)

The safety function of the device is fulfilled, as long as the output shows safe state (de-energized) if the device is switched off via the supply terminals. The wiring suitable for this mode of operation is shown in the "Proof Test" chapter (view Figure 4.3 on page 14).

Safe State

The safe state is defined, as the output being < 0.5 mA (test current in off condition).

Reaction Time

The reaction time for all safety functions is < 1 s.

221342 2010-01

2.4 Characteristic Safety Values

KFD2-SL2-(Ex)1.LK

Parameters acc. to IEC 61508	**Variables**	
Assessment type and documentation	Hardware assessment	
Pepperl+Fuchs documentation number [1]	P+F 06/09-23 R029	
Device type	A	
Demand mode	Low Demand Mode or High Demand Mode	
Safety function	bus powered [2]	loop powered [2]
HFT	0	0
SIL (hardware)	2	3
$\lambda_{sd} + \lambda_{su}$	338 FIT	338 FIT
λ_{dd}	0 FIT	0 FIT
λ_{du}	10.3 FIT	0 FIT
$\lambda_{total\ (safety\ function)}$	714.3 FIT	714.3 FIT
SFF	98 %	100 %
MTBF [3]	160 years	160 years
PFH	1.03×10^{-8} 1/h	0 1/h
PFD_{avg} for T_1 = 1 year	4.49×10^{-5}	0
T_{proof} max.	22 years	no proof test necessary
Reaction time [4]	< 1 sec	
[1] Pepperl+Fuchs documentation number for further reference if an additional documentation from an independent notified body can be requested.		
[2] The device can be used in two operating modes, bus powered and loop powered. In the loop powered mode no dangerous faults can occur, since the safe state of the connected solenoid is de-energized. This operating mode is not mentioned explicitly in the hardware assessment report P+F 06/09-23 R029.		
[3] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.		
[4] Step response time		

Table 2.1

221342 2010-01

KFD2-SL2-(Ex)*(.B)

Parameters acc. to IEC 61508	Variables	
Assessment type and documentation	Hardware assessment	
Pepperl+Fuchs documentation number [1]	P+F 06/09-23 R029	
Device type	A	
Demand mode	Low Demand Mode or High Demand Mode	
Safety function	bus powered [2]	loop powered [2]
HFT	0	0
SIL (hardware)	2	3
$\lambda_{sd} + \lambda_{su}$	320 FIT	320 FIT
λ_{dd}	0 FIT	0 FIT
λ_{du}	9.7 FIT	0 FIT
$\lambda_{total\ (safety\ function)}$	651.7 FIT	651.7 FIT
SFF	98 %	100 %
MTBF [3]	175 years	175 years
PFH	9.7 x 10^{-9} 1/h	0 1/h
PFD_{avg} for T_1 = 1 year	4.25 x 10^{-5}	0
T_{proof} max.	23 years	no proof test necessary
Reaction time [4]	< 1 sec	
[1] Pepperl+Fuchs documentation number for further reference if an additional documentation from an independent notified body can be requested.		
[2] The single channel device can be used in two operating modes, bus powered and loop powered. In the loop powered mode no dangerous faults can occur, since the safe state of the connected solenoid is de-energized. This operating mode is not mentioned explicitly in the hardware assessment report P+F 06/09-23 R029.		
[3] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.		
[4] Step response time		

Table 2.2

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}).

221342 2010-01

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: error output

3.2 Configuration

A configuration of the device is possible via switch S1 for output loop monitoring on/off (not safety relevant).

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.

221342 2010-01

4 Proof Test

4.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potentially dangerous failures that are otherwise not detected by diagnostic tests.

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 documentation 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.

Periodical verification of the function

Device connected to 24 V supply, green LED on

- input energized – output energized, yellow LED on
- input de-energized – output de-energized (safety relevant), yellow LED off

24 V supply disconnected, green LED off

- input energized – output de-energized, yellow LED off
- input de-energized – output de-energized (safety relevant), yellow LED off

Output loop powered will not work, red LED off

With the following instructions a proof test can be performed which will reveal almost all of the possible dangerous faults (diagnostic coverage > 90 %).

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.
- Power supply set at nominal voltage of 24 V DC
- 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 KFD2-SL2-(Ex)1* device (view Figure 4.1 on page 13), KFD2-SL2-(Ex)1* device (SIL3, loop powered) (view Figure 4.3 on page 14) or the KFD2-SL2-(Ex)2* device (view Figure 4.2 on page 13).
- Restore the safety loop. Any by-pass of the safety function must be removed.

Step No.	Supply	Input value (V)	Output value (mA)
1	24 V	High (24 v)	On/I_{max}, depends on device version
2	24 V	Low (5 V)	Off/< 0.5 mA (SIL2)
3	0 V	–	Off/0 mA (SIL3)

Table 4.1: Steps to be performed for the proof test

221342 2010-01

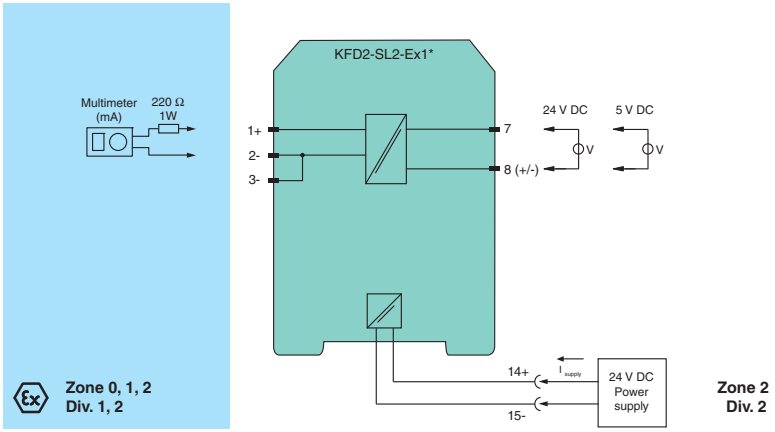

Figure 4.1: Proof test set-up for KFD2-SL2-Ex1*
Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD2-SL2-Ex1*.

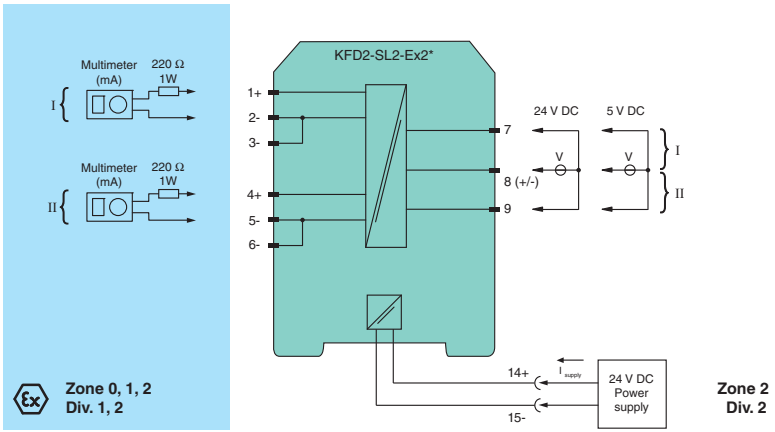

Figure 4.2: Proof test set-up for KFD2-SL2-Ex2*
Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD2-SL2-Ex2*.

221342 2010-01

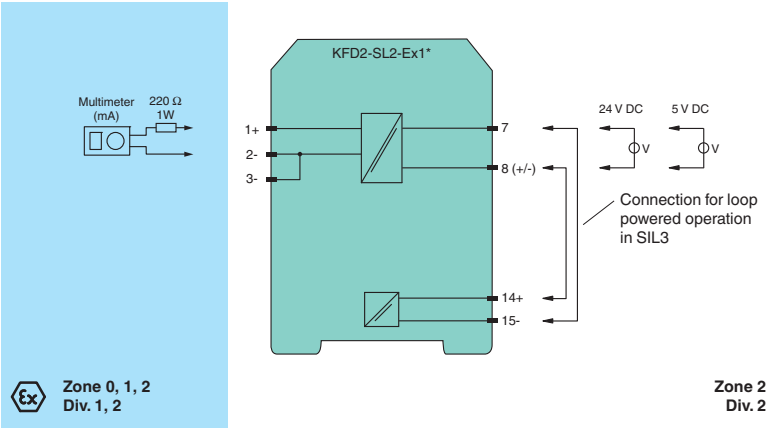

Figure 4.3: Proof test set-up for KFD2-SL2-Ex1* (SIL3, loop powered)
Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD2-SL2-Ex1*.

Note!

Figure 4.3. shows the wiring of two operation modes:

1. For SIL2 operation the logic signal has to be connected to terminals 7 and 8 while the device can be powered with a separate power supply via terminals 14 and 15 or Power Rail.
2. For SIL3 emergency shut down safety functions the logic signal has to be connected to terminals 7 and 15 and to 8 and 14. No external power supply and no DIN rail with Power Rail functionality must be used.

221342 2010-01

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
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

221342 2010-01

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

221342 / DOCT-1907
01/2010