

Functional Safety

**SMART Current Driver
KFD2-SCD2-Ex*.LK,
HiD2038**

Manual

SIL

IEC 61508/61511



CE SIL 2 

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"

Worldwide

Pepperl+Fuchs Group

Lilienthalstr. 200

68307 Mannheim

Germany

Phone: +49 621 776 - 0

E-mail: info@de.pepperl-fuchs.com

North American Headquarters

Pepperl+Fuchs Inc.

1600 Enterprise Parkway

Twinsburg, Ohio 44087

USA

Phone: +1 330 425-3555

E-mail: sales@us.pepperl-fuchs.com

Asia Headquarters

Pepperl+Fuchs Pte. Ltd.

P+F Building

18 Ayer Rajah Crescent

Singapore 139942

Phone: +65 6779-9091

E-mail: sales@sg.pepperl-fuchs.com

<https://www.pepperl-fuchs.com>

1	Introduction	5
1.1	Content of this Document	5
1.2	Safety Information	6
1.3	Symbols Used	7
2	Product Description	8
2.1	Validity	8
2.2	Function	8
2.3	Interfaces	9
2.4	Marking	9
2.5	Standards and Directives for Functional Safety	9
3	Planning	10
3.1	System Structure	10
3.2	Assumptions	11
3.3	Safety Function and Safe State	11
3.4	Characteristic Safety Values	12
3.5	Useful Lifetime	13
4	Mounting and Installation	14
4.1	Configuration	14
5	Operation	15
5.1	Proof Test	15
6	Maintenance and Repair	18
7	List of Abbreviations	19

1 Introduction

1.1 Content of this Document

This document contains information for usage of the device in functional safety-related applications. You need this information to use your product throughout the applicable stages of the product life cycle. These can include the following:

- Product identification
- Delivery, transport, and storage
- Mounting and installation
- Commissioning and operation
- Maintenance and repair
- Troubleshooting
- Dismounting
- Disposal



Note

This document does not substitute the instruction manual.



Note

For full information on the product, refer to the instruction manual and further documentation on the Internet at www.pepperl-fuchs.com.

The documentation consists of the following parts:

- Present document
- Instruction manual
- Manual
- Datasheet

Additionally, the following parts may belong to the documentation, if applicable:

- EU-type examination certificate
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- FMEDA report
- Assessment report
- Additional documents

For more information about Pepperl+Fuchs products with functional safety, see www.pepperl-fuchs.com/sil.

1.2 Safety Information

Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismantling lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismantling of the product. The personnel must have read and understood the instruction manual and the further documentation.

Intended Use

The device is only approved for appropriate and intended use. Ignoring these instructions will void any warranty and absolve the manufacturer from any liability.

The device is developed, manufactured and tested according to the relevant safety standards.

Use the device only

- for the application described
- with specified environmental conditions
- with devices that are suitable for this safety application

Improper Use

Protection of the personnel and the plant is not ensured if the device is not used according to its intended use.

1.3 Symbols Used

This document contains symbols for the identification of warning messages and of informative messages.

Warning Messages

You will find warning messages, whenever dangers may arise from your actions. It is mandatory that you observe these warning messages for your personal safety and in order to avoid property damage.

Depending on the risk level, the warning messages are displayed in descending order as follows:



Danger!

This symbol indicates an imminent danger.

Non-observance will result in personal injury or death.



Warning!

This symbol indicates a possible fault or danger.

Non-observance may cause personal injury or serious property damage.



Caution!

This symbol indicates a possible fault.

Non-observance could interrupt the device and any connected systems and plants, or result in their complete failure.

Informative Symbols



Note

This symbol brings important information to your attention.



Action

This symbol indicates a paragraph with instructions. You are prompted to perform an action or a sequence of actions.

2 Product Description

2.1 Validity

This manual is only valid for devices with a part number **greater than #295000**.
Contact your Pepperl+Fuchs representative for information about older devices.

2.2 Function

General

This isolated barrier is used for intrinsic safety applications.

Digital signals are superimposed on the analog values at the field side or control side and are transferred bi-directionally.

An open or short field circuit presents a high impedance to the control side to allow alarm conditions to be monitored by the control system.

KFD2-SCD2-Ex1.LK

The device drives SMART I/P converters, electrical valves, and positioners in hazardous areas.

Current transferred across the DC/DC converter is repeated at terminals 1 and 2. Terminals 2 and 3 are used when no short circuit detection is required.

If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

A fault is signaled by LEDs and a separate collective error message output.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

KFD2-SCD2-Ex2.LK

The device drives SMART I/P converters, electrical valves, and positioners in hazardous areas.

Current transferred across the DC/DC converter is repeated at terminals 1, 2 and 4, 5. Terminals 2, 3 and 5, 6 are used when no short circuit detection is required.

If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

A fault is signaled by LEDs and a separate collective error message output.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

HiD2038

The device repeats the input signal from a control system to drive HART I/P converters, electrical valves, and positioners located in a hazardous area.

Current transferred across the DC/DC converter is repeated at the terminals 5a, 5b (1a, 1b). The terminals 5b, 7a (1b, 3b) are used when no short-circuit detection is required.

Line fault detection of the field circuit is indicated by a red LED and an output on the fault bus. The fault conditions are monitored via a Fault Indication Board.

This device mounts on a HiD Termination Board.

2.3 Interfaces

The device has the following interfaces.

- Safety relevant interfaces:

Input I, output I	KFD2-SCD2-Ex1.LK
Input I, Input II, output I, output II	KFD2-SCD2-Ex2.LK, HiD2038

- Non-safety relevant interfaces: none
The HART communication is not relevant for functional safety.



Note

For corresponding connections see datasheet.

2.4 Marking

Pepperl+Fuchs Group Lilienthalstraße 200, 68307 Mannheim, Germany	
Internet: www.pepperl-fuchs.com	
KFD2-SCD2-Ex1.LK, KFD2-SCD2-Ex2.LK	Up to SIL 2
HiD2038	



Note

If you design the safety loops in homogeneous redundancy (HFT = 1), you can use the devices in applications up to SIL 3.

2.5 Standards and Directives for Functional Safety

Device specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 7, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)
-------------------	---

System-specific standards and directives

Functional safety	IEC 61511-1:2016+COR1:2016+A1:2017 EN 61511-1:2017+A1:2017 Functional safety – Safety instrumented systems for the process industry sector (user)
-------------------	---

3 Planning

3.1 System Structure

3.1.1 Low Demand Mode of Operation

If there are two control 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 dangerous **F**ailure on **D**emand) and the T₁ value (proof test interval that has a direct impact on the PFD_{avg} value)
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.2 High Demand or Continuous Mode of Operation

If there is only one safety loop, which combines the standard operation and safety-related operation, then usually the demand rate for this safety 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)

3.1.3 Safe Failure Fraction

The safe failure fraction describes the ratio of all safe failures and dangerous detected failures to the total failure rate.

$$\text{SFF} = (\lambda_s + \lambda_{dd}) / (\lambda_s + \lambda_{dd} + \lambda_{du})$$

A safe failure fraction as defined in IEC/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 the elements and subsystems, but not of a single device.

Nevertheless the SFF of the device is given in this document for reference.

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rate based on the Siemens standard SN 29500.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- The safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- The device will be used under average industrial ambient conditions comparable to the classification "stationary mounted" according to MIL-HDBK-217F.

Alternatively, operating stress conditions typical of an industrial field environment similar to IEC/EN 60654-1 Class C with an average temperature over a long period of time of 40 °C may be assumed. For a higher average temperature of 60 °C, the failure rates must be multiplied by a factor of 2.5 based on experience. A similar factor must be used if frequent temperature fluctuations are expected.

- The application program in the programmable logic controller (PLC) is configured to detect line faults (lead breakage or lead short circuit).
- If you are using the HART communication, observe that the HART signal superimposes an analog signal on the signal line that can influence the measured value. Verify that all devices on the signal line are HART compatible when activating HART communication in one of the devices.

3.3 Safety Function and Safe State

Safety Function

The safety function of the device is fulfilled, as long as the output repeats the input current (4 mA to 20 mA) with a tolerance of 2 %.

A dangerous detected failure is present if the output current is less than 4 mA due to the line fault detection.

A dangerous undetected failure is present if the tolerance limit for the signal transfer is exceeded and the output current is between 4 mA and 20 mA.

Safe State

The safe state is present when the output current is < 4 mA. The safe state is adopted in all cases of dangerous detected failures.

Reaction Time

The safety reaction time is the maximum time required from the occurrence of the fault to the reaction of the outputs in normal operation without faults.

The combined fault detection and fault reaction time is the time in which the device outputs react to an occurred fault. See chapter 3.4.



Note

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

Parameters	Characteristic values
Assessment type	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL ¹	2
SC	3
Safety function	Transfer of the analog signals
λ_s	0 FIT
λ_{dd}	153 FIT
λ_{du}	36.9 FIT
λ_{total} (safety function)	190 FIT
SFF	80 %
MTBF ²	216 years
PFH	3.69×10^{-8} 1/h
PFD _{avg} for $T_1 = 1$ year	1.62×10^{-4}
PFD _{avg} for $T_1 = 2$ years	3.23×10^{-4}
PFD _{avg} for $T_1 = 5$ years	8.08×10^{-4}
PFD _{avg} for $T_1 = 10$ years	1.62×10^{-3}
PTC	100 %
Safety reaction time ³ Fault reaction time ³	< 20 ms < 1000 ms

Table 3.1

¹ The statement for the SIL rating is based on SFF, HFT and the assumption that this device typically uses 10 % of the failure budget for the safety loop.

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

³ Time between fault detection and fault reaction

The characteristic safety values like PFD, SFF, HFT and T_1 are taken from the SIL report/FMEDA report. Observe that PFD and T_1 are related to each other.

The function of the devices has to be checked within the proof test interval (T_1).

3.5 Useful Lifetime

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful lifetime of components is not exceeded. Beyond this useful lifetime, the result of the probabilistic estimation is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular. For example, electrolytic capacitors can be very sensitive to the operating 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 lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation and therefore the assumption of a constant failure rate during the useful lifetime is valid.

However, according to IEC/EN 61508-2, a useful lifetime, based on general experience, should be assumed. Experience has shown that the useful lifetime often lies within a range period of about 8 to 12 years.

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

Our experience has shown that the useful lifetime of a Pepperl+Fuchs product can be higher if the ambient conditions support a long life time, for example if the ambient temperature is significantly below 60 °C.

Please note that the useful lifetime refers to the (constant) failure rate of the device. The effective life time can be higher.

The estimated useful lifetime is greater than the warranty period prescribed by law or the manufacturer's guarantee period. However, this does not result in an extension of the warranty or guarantee services. Failure to reach the estimated useful lifetime is not a material defect.

4 Mounting and Installation



Mounting and Installing the Device

1. Observe the safety instructions in the instruction manual.
2. Observe the information in the manual.
3. Observe the requirements for the safety loop.
4. Connect the device only to devices that are suitable for this safety application.
5. Check the safety function to ensure the expected output behavior.

4.1 Configuration

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

5 Operation



Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.



Operating the device

1. Observe the safety instruction in the instruction manual.
2. Observe the information in the manual.
3. Use the device only with devices that are suitable for this safety application.
4. Correct any occurring safe failures within 24 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test

This section describes a possible proof test procedure. The user is not obliged to use this proposal. The user may consider different concepts with an individual determination of the respective effectiveness, e. g. concepts according to NA106:2018.

According to IEC/EN 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous failures that are not detected otherwise.

Check the function of the subsystem at periodic intervals depending on the applied PFD_{avg} in accordance with the characteristic safety values. See chapter 3.4.

It is under the responsibility of the plant operator to define the type of proof test and the interval time period.

Conditions

- Digital multimeter with an accuracy better than 0.1 %
Use for the proof test of the intrinsic safety side of the device a special digital multimeter for intrinsically safe circuits.
If intrinsically safe circuits are operated with non-intrinsically safe circuits, they must no longer be used as intrinsically safe circuits.
- Power supply set to nominal voltage of 24 V DC
- Process calibrator with current source function with an accuracy better than 20 μ A



Proof Test Procedure

1. Put out of service the entire safety loop. Protect the application by means of other measures.
2. Prepare a test set-up, see figures below.
3. Test the devices. Verify the current values as given in table below.
4. Set back the device to the original settings for the application after the test.

Step No.	Set input value (mA)	Set output value R_{load} (Ω)	Mandatory measuring points (safety-relevant) output value (mA)
1	20.00	470	20.00 ± 0.40
2	12.00	470	12.00 ± 0.40
3	4.00	470	4.00 ± 0.40
4	23.00	470	23.00 ± 0.40
5	0	470	< 0.30
6	12.0	< 30	2.00 ± 1.00
7	12.00	> 100000	< 0.30
8	12.00	Restored as step 2	

Table 5.1 Steps to be performed for the proof test

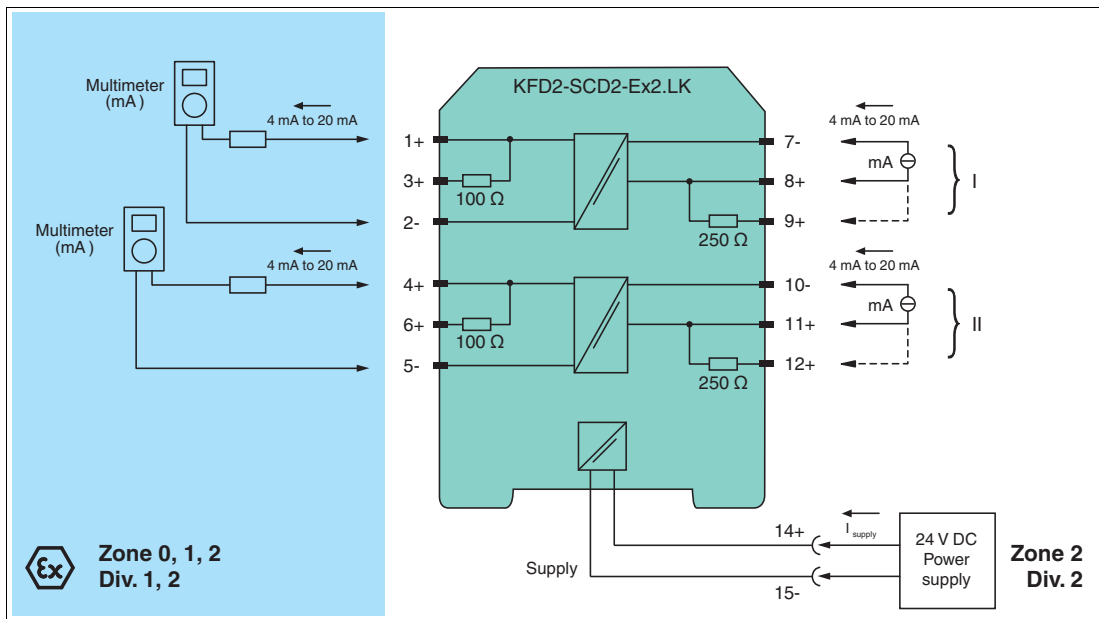


Figure 5.1 Proof test set-up for KFD2-SCD2-Ex*.LK
Channel II only for KFD2-SCD2-Ex2.LK

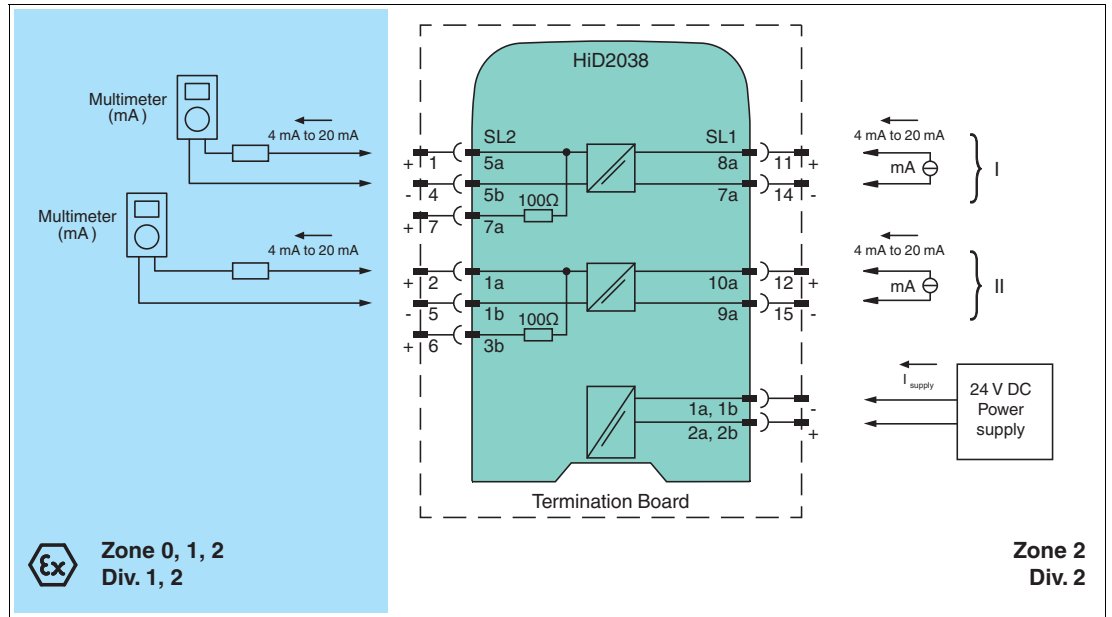


Figure 5.2 Proof test set-up for HiD2038



Tip

The easiest way to test HiD devices by using a stand-alone HiDTB**-SCT-***-**-** termination board. In this test, it is not necessary to disconnect the wiring of the existing application. Faults in a subsequent wiring can be avoided.

6 Maintenance and Repair



Danger!

Danger to life from missing safety function

Changes to the device or a defect of the device can lead to device malfunction.
The function of the device and the safety function is no longer guaranteed.

Do not repair, modify, or manipulate the device.



Maintaining, Repairing or Replacing the Device

In case of maintenance, repair or replacement of the device, proceed as follows:

1. Implement appropriate maintenance procedures for regular maintenance of the safety loop.
2. While the device is maintained, repaired or replaced, the safety function does not work.
Take appropriate measures to protect personnel and equipment while the safety function is not available.
Secure the application against accidental restart.
3. Do not repair a defective device. A defective device must only be repaired by the manufacturer.
4. If there is a defect, always replace the device with an original device.

7 List of Abbreviations

ESD	Emergency Shutdown
FIT	Failure In Time in 10^{-9} 1/h
FMEDA	Failure Mode, Effects, and Diagnostics Analysis
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 loop that have no effect on the safety function.
$\lambda_{not\ part}$	Probability of failure of components that are not in the safety loop
$\lambda_{total\ (safety\ function)}$	Probability of failure of components that are in the safety loop
HFT	Hardware Fault Tolerance
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PCS	Process Control System
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of dangerous failure per hour
PLC	Programmable Logic Controller
PTC	Proof Test Coverage
SC	Systematic Capability
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T₁	Proof Test Interval

Your automation, our passion.

Explosion Protection

- Intrinsic Safety Barriers
- Signal Conditioners
- FieldConnex® Fieldbus
- Remote I/O Systems
- Electrical Ex Equipment
- Purge and Pressurization
- Industrial HMI
- Mobile Computing and Communications
- HART Interface Solutions
- Surge Protection
- Wireless Solutions
- Level Measurement

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

Pepperl+Fuchs Quality

Download our latest policy here:

www.pepperl-fuchs.com/quality

