

SAFETY MANUAL SIL

SMART Transmitter Power Supply

HiD2025(SK), HiD2026(SK),
HiD2029(SK), HiD2030(SK)



SIL2



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	4
1.1	General Information	4
1.2	Intended Use	4
1.3	Manufacturer Information	5
1.4	Relevant Standards and Directives	5
2	Planning	6
2.1	System Structure	6
2.2	Assumptions	7
2.3	Safety Function and Safe State	8
2.4	Characteristic Safety Values	9
3	Safety Recommendation	12
3.1	Interfaces	12
3.2	Configuration	12
3.3	Useful Life Time	12
3.4	Installation and Commissioning	13
4	Proof Test	14
4.1	Proof Test Procedure	14
5	Abbreviations	17

1 Introduction

1.1 General Information

This manual contains information on using the device in control circuits that are related to functional safety.

The corresponding data sheets, the operating instructions, the system description, the declaration of conformity, the EC-Type Examination Certificate, and the applicable certificates (see data sheet) are an integral part of this document.

The stated documents are available at www.pepperl-fuchs.com or from 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.

In the event of a device fault, the devices must be taken out of operation and measures must be taken to protect them against unintentional startup. Devices may be repaired only by the manufacturer. Deactivating or bypassing safety functions, or failing to observe the instructions in this manual (which lead to faults or affect the safety functions), can damage property and the environment or cause personal injury, for which Pepperl+Fuchs GmbH accepts no liability.

The devices have been developed, manufactured, and tested according to the applicable safety standards. The devices may be used only for the applications described in the instructions under the specified ambient conditions and exclusively in connection with the approved peripherals.

1.2 Intended Use

General

These isolated barriers are used for intrinsic safety applications.

The devices supply 2-wire SMART transmitters in the hazardous area and repeat the current signal from the SMART transmitter to drive a safe area load.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

The versions without SK provide active outputs that can be configured as current or voltage output (supplied internally). The versions ending with SK are designed to provide a sink mode current output on the safe area terminals (supplied externally). While HiD2025(SK) and HiD2029(SK) are one channel versions, the HiD2026(SK) and the HiD2030(SK) provide two channels.

The devices are mounted on a HiD Termination Board.

HiD2025(SK), HiD2026(SK)

The output is isolated from the input and referenced to the power supply common.

HiD2029(SK), HiD2030(SK)

These devices can also be used with 2-wire current sources.

A separate fault indication output on the bus indicates that the input signal is outside the range 0.2 mA ... 24 mA. The fault conditions can be monitored via a Fault Indication Board.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

Up to SIL2	■ HiD2025(SK)
	■ HiD2026(SK)
	■ HiD2029(SK)
	■ HiD2030(SK)

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)

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.

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

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:

- Only one input and one output are part of the considered safety function (only 2-channel version).
- 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.
- The safety-related device is considered to be of type **A** components with a Hardware Fault Tolerance of **0**.
- It is assumed that the device will be used under average industrial ambient conditions, which are comparable with the classification "stationary mounted" in MIL-HDBK-217F. Alternatively, the following ambient conditions are assumed:
 - IEC 60654-1 Class C (sheltered location) with temperature limits in the range of the manufacturer's specifications and an average temperature of 40 °C over a long period. A moisture level within the manufacturer's specifications is assumed. For a higher average temperature of 60 °C, the failure rates must be multiplied by a factor of 2.5 based on empirical values. A similar multiplier must be used if frequent temperature fluctuations are expected.
- It is assumed that any safe failures that occur (e.g., output in safe condition) will be corrected within eight hours (e.g., correction of a sensor fault).
- While the device is being repaired, measures must be taken to maintain the safety function (e.g., by using a replacement device).
- The separate fault indication output of the HiD2029(SK) and HiD2030(SK) devices is not considered within the FMEDA.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.
- 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 (Safety Instrumented Function) 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 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.

2.3 Safety Function and Safe State

Safety Function

The safety function of the devices is the transfer of the analog signals from the input to the output with a tolerance of 2 %.

Input signals	Output signals
0/4 mA ... 20 mA	0/4 mA ... 20 mA
0/4 mA ... 20 mA	0/1 V ... 5 V

Table 2.1

Safe State

The user must ensure that the ESD system reacts adequately when the outputs are outside the range of 4 mA ... 20 mA for a current output or 1 V ... 5 V for a voltage output.

Reaction Time

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

2.4 Characteristic Safety Values

HiD2025, HiD2026

Parameters acc. to IEC 61508	Values
Assessment type	FMEDA report
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function ²	Transfer of analog values
HFT	0
SIL	2
λ_s ¹	216 FIT
λ_{dd}	0 FIT
λ_{du}	92 FIT
$\lambda_{no\ effect}$ ²	112 FIT
$\lambda_{not\ part}$	7.1 FIT
λ_{total} (safety function)	308 FIT
SFF	70 %
MTBF ³	362 years
PFH	9.2×10^{-8} 1/h
PFD _{avg} for T _{proof} = 1 year	4.04×10^{-4}
PFD _{avg} for T _{proof} = 2 years	8.07×10^{-4}
PFD _{avg} for T _{proof} = 5 years	2.02×10^{-3}

¹ "Not considered" failures are considered 50 % as dangerous undetected failures λ_{du} and 50 % as safe detected failures.

² "No effect" failures are not influencing the safety functions and are therefore added to the λ_s .

³ acc. to SN29500. This value includes failures which are not part of the safety function.

Table 2.2

HiD2025SK, HiD2026SK

Parameters acc. to IEC 61508	Values
Assessment type	FMEDA report
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function ²	Transfer of analog values
HFT	0
SIL	2
λ_s^1	228 FIT
λ_{dd}	0 FIT
λ_{du}	93 FIT
$\lambda_{no\ effect}^2$	117 FIT
$\lambda_{not\ part}$	7.1 FIT
λ_{total} (safety function)	321 FIT
SFF	70 %
MTBF ³	348 years
PFH	9.3×10^{-8} 1/h
PFD _{avg} for T _{proof} = 1 year	4.09×10^{-4}
PFD _{avg} for T _{proof} = 2 years	8.18×10^{-4}
PFD _{avg} for T _{proof} = 5 years	2.04×10^{-3}

¹ "Not considered" failures are considered 50 % as dangerous undetected failures λ_{du} and 50 % as safe detected failures.

² "No effect" failures are not influencing the safety functions and are therefore added to the λ_s .

³ acc. to SN29500. This value includes failures which are not part of the safety function.

Table 2.3

HiD2029(SK), HiD2030(SK)

Parameters acc. to IEC 61508	Values
Assessment type	FMEDA report
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function ²	Transfer of analog values
HFT	0
SIL	2
λ_s ¹	434 FIT
λ_{dd}	0 FIT
λ_{du}	95 FIT
$\lambda_{no\ effect}$ ²	167 FIT
$\lambda_{not\ part}$	28.4 FIT
$\lambda_{total\ (safety\ function)}$	528 FIT
SFF	82 %
MTBF ³	205 years
PFH	9.5×10^{-8} 1/h
PFD _{avg} for T _{proof} = 1 year	4.16×10^{-4}
PFD _{avg} for T _{proof} = 2 years	8.31×10^{-4}
PFD _{avg} for T _{proof} = 5 years	2.08×10^{-3}

¹ "Not considered" failures are considered 50 % as dangerous undetected failures λ_{du} and 50 % as safe detected failures.

² "No effect" failures are not influencing the safety functions and are therefore added to the λ_s .

³ acc. to SN29500. This value includes failures which are not part of the safety function.

Table 2.4

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 devices have the following interfaces. For corresponding terminals see data sheet.

■ Safety relevant interfaces:

Input I, output I	HiD2025(SK), HiD2029(SK)
Input I, input II, output I, output II	HID2026(SK), HID2030(SK)

■ Non-safety relevant interfaces:

- Power supply
- Fault indication output for HiD2029(SK), HiD2030(SK)
- HART communication

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.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.

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.

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. 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 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 this manual. see chapter 2.4.

It is under the responsibility of the operator to select the proof test and regard the defined interval time period.

With the following instructions a proof test can be performed which will reveal almost all of the possible dangerous faults (diagnostic coverage > 99 %).

- 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 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.
 - Power supply set at nominal voltage of 24 V DC
 - For SK versions: Power supply 24 V DC and lead resistor 250 Ω /1 W
 - Process calibrator with mA current source/sink feature (accuracy better than 20 μ A)
- 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 devices (view Figures). Choose the proper input terminals (passive input or active input) in accordance with the specific application and follow the steps indicated in the table below.
- Restore the safety loop. Any by-pass of the safety function must be removed.

Proof Test for all Channels

Step No.	Set input value (mA)	Measurement point	
		Output value (mA)	Output value (V)
1	20.0	20.0 \pm 0.4	5.0 \pm 0.1
2	12.0	12.0 \pm 0.4	3.0 \pm 0.1
3	4.0	4.0 \pm 0.4	1.0 \pm 0.1
4	23.0	23.0 \pm 0.4	5.75 \pm 0.1
5	0	< 0.2	< 0.05

Table 4.1

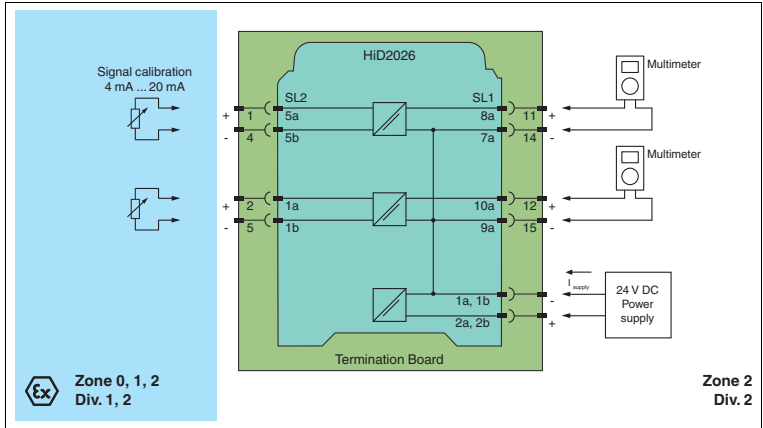


Figure 4.1 Proof test set-up for HiD2025, HiD2026

For HiD2025 do not regard the second channel.

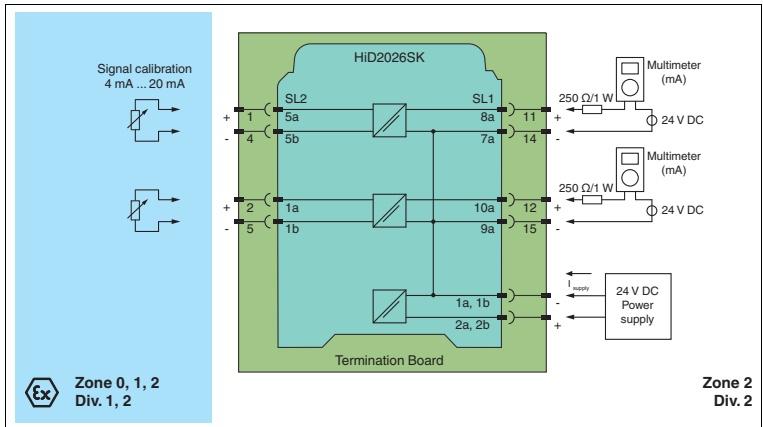


Figure 4.2 Proof test set-up for HiD2025SK, HiD2026SK

For HiD2025SK do not regard the second channel.

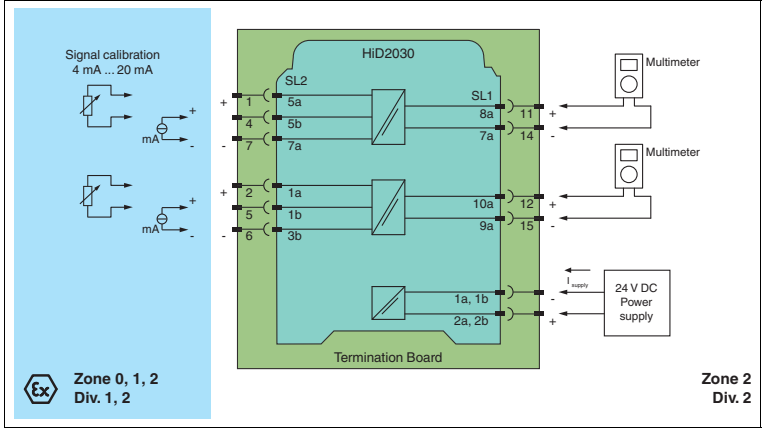


Figure 4.3 Proof test set-up for HiD2029, HiD2030

For HiD2029 do not regard the second channel.

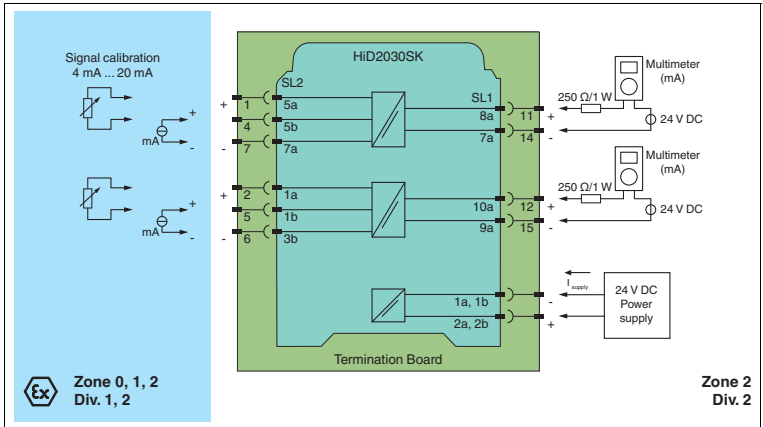


Figure 4.4 Proof test set-up for HiD2029SK, HiD2030SK

For HiD2029SK do not regard the second channel.

5 Abbreviations

DCS	D istributed C ontrol S ystem
ESD	E mergency S hutdown
FIT	F ailure I n T ime in 10^{-9} 1/h
FMEA	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
PFDAvg	A verage 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}	P roof T est I nterval



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

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

 **PEPPERL+FUCHS**
PROTECTING YOUR PROCESS

DOCT-3705
05/2014