Functional Safety

SMART Transmitter Power Supply/SMART Current Driver HiC2422

Manual

SIL

IEC 61508/61511

ISO**9001**

C E   **SIL** 2   Ex

Your automation, our passion.

PEPPERL+FUCHS

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"

PEPPERL+FUCHS

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

i

Note

This document does not substitute the instruction manual.

i

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:

i

Note

For specific device information such as the year of construction, scan the QR code on the device. As an alternative, enter the serial number in the serial number search at www.pepperl-fuchs.com.

- 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.

PEPPERL+FUCHS

1.2 Safety Information

Target Group, Personnel

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

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismounting 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.

PEPPERL+FUCHS

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.

PEPPERL+FUCHS

2 Product Description

2.1 Function

This isolated barrier is used for intrinsic safety applications.

Each device channel works as a transmitter power supply or a current driver.

The device transfers data by using a current signal.

The device supports a bi-directional communication for SMART devices that use current modulation to transmit data and voltage modulation to receive data.

For current driver operation, an open field circuit presents a high impedance to the control side to allow lead breakage to be monitored by control systems.

This device mounts on a HiC termination board.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input I, input II, output I, output II
- Non-safety relevant interfaces: none
  The HART communication is not relevant for functional safety.

Note

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs Group Lilienthalstraße 200, 68307 Mannheim, Germany
Internet: www.pepperl-fuchs.com

HiC2422	Up to SIL 2

2.4 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)

PEPPERL+FUCHS

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 T_1 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.

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

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.

PEPPERL+FUCHS

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 ºC may be assumed. For a higher average temperature of 60 ºC, 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.

- Only one input and one output are part of the safety function.
- The application program in the programmable logic controller (PLC) is configured to detect the following line faults:
  - Lead breakage or lead short circuit for analog input
  - Lead breakage for analog output
- 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.

2023-02

PEPPERL+FUCHS

3.3 Safety Function and Safe State

Safe State

Device as an Analog Input

The safe state is present when the output current is < 3.6 mA or > 21.5 mA.

Device as an Analog Output

The safe state is present when the output current is < 4 mA.

Safety Function

Device as an Analog Input

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 undetected failure is present if the tolerance limits for the signal transfer are exceeded and the output current is between 4 mA and 20 mA.

The safety instrumented system (SIS) must ensure suitable reaction when the output current of the device is < 3.6 mA or > 21.5 mA.

Device as an Analog Output

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 undetected failure is present if the tolerance limits for the signal transfer are exceeded and the output current is between 4 mA and 20 mA.

Switch settings

Function		Switch			
		Channel 1		Channel 2	
Field side	Control side	S1	S2	S3	S4
Analog input	Current source	I	II	I	II
Analog input	Current sink	II	I	II	I
Analog output		II	I	II	I

Table 3.1

Reaction Times

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.

PEPPERL+FUCHS

3.4 Characteristic Safety Values

Device as an Analog Input in 1oo1 Structure

Parameters	Characteristic values
Assessment type and documentation	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL [1]	2
SC	3
Safety function	Control side output value of < 3.6 mA or > 21.5 mA
λ_s	0 FIT
λ_{dd}	151 FIT
λ_{du}	32.5 FIT
λ_{FH} [2]	5.5 FIT
λ_{FL} [2]	145 FIT
$\lambda_{total\ (safety\ function)}$	183 FIT
$\lambda_{not\ part}$	134 FIT
SFF	82.24 %
PTC	100 %
MTBF [3]	233 years
PFH	3.25×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	1.42×10^{-4}
PFD_{avg} for T_1 = 2 years	2.85×10^{-4}
PFD_{avg} for T_1 = 5 years	7.12×10^{-4}
Reaction time [4]	< 1 s

Table 3.2

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. FH (fail high) denotes failures that lead to outputs above 21.5 mA.
   FL (fail low) denotes failures that lead to outputs below 3.6 mA.
   These failures were added to form the λ_{dd}. If this assumption is not correct for your application distribute them as required.

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

4. Time between fault detection and fault reaction

PEPPERL+FUCHS

Device as an Analog Output in 1oo1 Structure

Parameter	Characteristic values
Assessment type and documentation	Full assessment
Device type	A
Mode of operation	Low demand mode or high demand mode
HFT	0
SIL [1]	2
SC	3
Safety function	Field side output value of < 4.0 mA
λ_s	0 FIT
λ_{dd}	150 FIT
λ_{du}	39.2 FIT
$\lambda_{total\ (safety\ function)}$	189 FIT
$\lambda_{not\ part}$	119 FIT
SFF	79,28 %
PTC	100 %
MTBF [2]	233 years
PFH	3.92×10^{-8} 1/h
PFD$_{avg}$ for T_1 = 1 year	1.72×10^{-4}
PFD$_{avg}$ for T_1 = 2 years	3.43×10^{-4}
PFD$_{avg}$ for T_1 = 5 years	8.58×10^{-4}
Reaction time [3]	< 1 s

Table 3.3

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 = 8 h.
3. Time between fault detection and fault reaction

i **Note**

The characteristic values apply to all modes of operation that can be set on the device.

The characteristic safety values like PFD, PFH, SFF, HFT and T_1 are taken from the 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).

PEPPERL+FUCHS

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 the maximum ambient temperature.

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

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.

2023-02

PEPPERL+FUCHS

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

Configuring the Device

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the side of the device.

1. De-energize the device before configuring the device.
2. Remove the device.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Secure the DIP switches to prevent unintentional adjustments.
5. Mount the device.
6. Connect the device again.

Note

See corresponding datasheets for further information.

PEPPERL+FUCHS

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 instructions 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 8 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 µA

2023-02

PEPPERL+FUCHS

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 the tables below.

4. Set back the device to the original settings for the application after the test.

Device as an Analog Input

Step No.	Set input value (mA)	Set output value R_{load} (Ω)	Mandatory measuring points (safety-relevant) output value (mA)
1	20.00	250	20.00 ± 0.40
2	12.00	250	12.00 ± 0.40
3	4.00	250	4.00 ± 0.40
4	23.00	250	23.00 ± 0.40
5	0	250	< 0.30
6	12.00	> 100000	< 0.30
7	12.00	Restored as step 2	

Table 5.1   Steps to be performed for the proof test
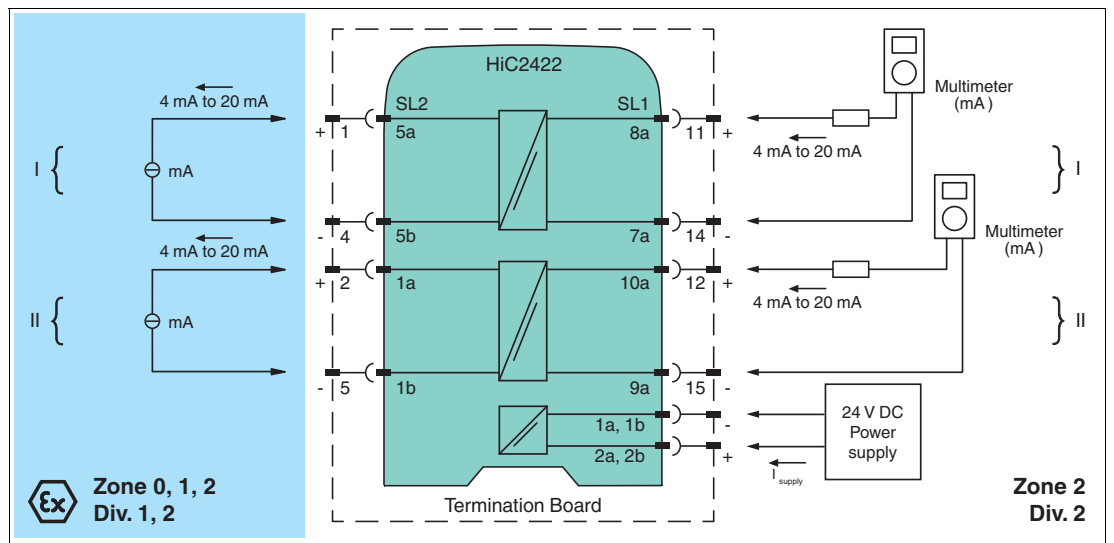
Figure 5.1   Proof test set-up for the device as an analog input

PEPPERL+FUCHS

Device as an Analog Output

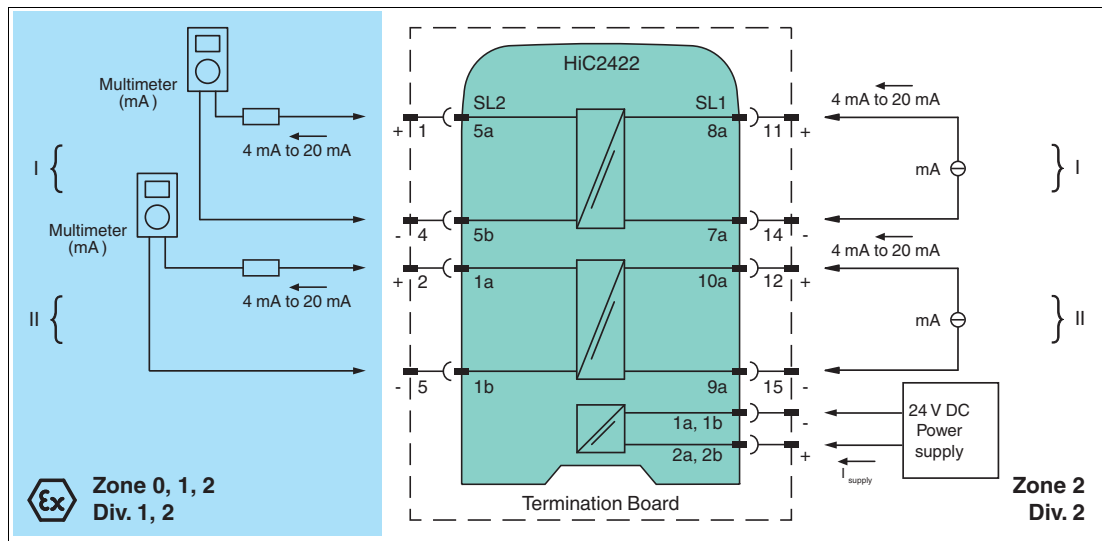| Step No.	Set input value (mA)	Set output value R_{load} (Ω)	Mandatory measuring points (safety-relevant) output value (mA)
1	20.00	500	20.00 ± 0.40
2	12.00	500	12.00 ± 0.40
3	4.00	500	4.00 ± 0.40
4	23.00	500	23.00 ± 0.40
5	0	500	< 0.30
6	12.00	> 100000	< 0.30
7	12.00	Restored as step 2	

Table 5.2

Figure 5.2   Proof test set-up for the device as an analog output

PEPPERL+FUCHS

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.

Reporting Device Failure

If you use the device in a safety loop according to IEC/EN 61508, it is required to inform the device manufacturer about possible systematic failures.

Report all failures in the safety function that are due to functional limitations or a loss of device function – especially in the case of possible dangerous failures.

In these cases, contact your local sales partner or the Pepperl+Fuchs technical sales support (service line).

It is not necessary to report failures in the safety function that are due to external influences or damage.

2023-02

PEPPERL+FUCHS

7 List of Abbreviations

ESD	**E**mergency **S**hut**d**own
FIT	**F**ailure **I**n **T**ime in 10^{-9} 1/h
FMEDA	**F**ailure **M**ode, **E**ffects, and **D**iagnostics **A**nalysis
$\lambda_{\textbf{s}}$	Probability of safe failure
$\lambda_{\textbf{dd}}$	Probability of dangerous detected failure
$\lambda_{\textbf{du}}$	Probability of dangerous undetected failure
$\lambda_{\textbf{no effect}}$	Probability of failures of components in the safety loop that have no effect on the safety function.
$\lambda_{\textbf{not part}}$	Probability of failure of components that are not in the safety loop
$\lambda_{\textbf{total (safety function)}}$	Probability of failure of components that are in the safety loop
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
MTTR	**M**ean **T**ime **T**o **R**estoration
PCS	**P**rocess **C**ontrol **S**ystem
PFD$_{\textbf{avg}}$	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure per hour
PLC	**P**rogrammable **L**ogic **C**ontroller
PTC	**P**roof **T**est **C**overage
SC	**S**ystematic **C**apability
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
$\textbf{T}_{\textbf{1}}$	Proof Test Interval

PEPPERL+FUCHS

PEPPERL+FUCHS

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