SAFETY MANUAL SIL

Voltage Repeater
HiC2095, HiD2096

SIL
IEC 61508/61511

ISO9001

CE

SIL2

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"

2015-02

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.co**m** or by contacting your local Pepperl+Fuchs representative.

Mounting, installation, commissioning, operation, maintenance and disassembly of the device may only be carried out by appropriate trained and qualified personnel. The instruction manual must be read and understood.

When a fault is detected within the device, it must be taken out of service and action taken to protect against accidental use. Devices shall 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.

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

1.2 Intended Use

General

These isolated barriers are used for intrinsic safety applications.

The devices provide a floating output to power a vibration sensor (e. g., Bently Nevada) or accelerometer in a hazardous area and transfer the voltage signal from that sensor to the safe area.

The devices are designed to provide a voltage or current supply to the vibration sensor. Depending on DIP switch setting the device provides 3.7 mA, 5.3 mA, or 9.0 mA supply current for 2-wire sensors, or 18 V at 20 mA for 3-wire sensors.

HiC2095

This device is a 1-channel version and mounts on a HiC-system termination board.

HiD2096

This device is a 2-channel version and mounts on a HiD-system termination board.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

HiC2095
HiD2096

Up to SIL2

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 61326-1:2013
  - 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 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_1 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.

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

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:

- The device shall claim the following fraction of the total failure budget for a SIL2 safety loop.
  - less than 10 % in Low Demand Mode
  - less than 15 % in High Demand Mode
- 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 1.5×10^{-7} per hour.
- The safety-related device is considered to be of type **A** components with a Hardware Fault Tolerance of **0**.
- 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.
- 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.
- Any safe failures that occur (e. g. output in safe state) will be corrected within 24 hours (e. g. remove sensor fault).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (e. g. substitution by an equivalent device).
- The stress levels are average for an industrial environment and the 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. The humidity level is within manufacturer's rating.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 Class C with an average temperature over a long period of time of 40 °C. 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.
- Since the two outputs of the device use common components, these outputs must not be used in the same safety function.
- In a two channel device, a failure leading to a safe state in one channel can result in a wrong potential on the other channel. Therefore the safety PLC must assume that the output is incorrect on that other channel.

2.3 Safety Function and Safe State

Safety Function

The safety function of the device is fulfilled, as long as the output repeats the input voltage (0 V ... -20 V) with a tolerance of ±2 %.

Safe State

The safe state is defined as the output being -20 V and lower or -0.5 V and higher.

Safety Response Time

The time that is needed to transfer a signal step on the input of the device to its output according to the safety function.

DIP Switch Settings HiC2095

Function	S1	S2
Current 3.7 mA	ON	OFF
Current 5.3 mA	OFF	ON
Current 9.0 mA	ON	ON

Table 2.1

DIP Switch Settings HiD2096

Function	Channel 1		Channel 2	
	S1	S2	S1	S2
Current 3.7 mA	ON	OFF	ON	OFF
Current 5.3 mA	OFF	ON	OFF	ON
Current 9.0 mA	ON	ON	ON	ON

Table 2.2

Reaction Time

The reaction time for all safety functions is < 2 ms.

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables
Assessment type and documentation	FMEDA report
Device type	A (only hardware)
Mode of protection	Low Demand Mode or High Demand Mode
HFT	0
SIL (hardware)	2
λ_{safe} [1]	312 FIT
λ_{dd}	0 FIT
λ_{du}	126 FIT
$\lambda_{total\ (safety\ function)}$	438 FIT
$\lambda_{not\ part}$	38.4 FIT
SFF	71.3 %
MTBF [2]	240 years
PFH	1.26×10^{-7} 1/h
PFD_{avg} for T_1 = 1 year	5.50×10^{-4}
PFD_{avg} for T_1 = 3 years	1.10×10^{-3}
PFD_{avg} for T_1 = 5 years	2.75×10^{-3}
Safety response time	12.5 µs

[1] Failures in parts that are part of the safety function but do not influence the safety function are regarded as safe undetected.

[2] acc. to SN29500. This value includes failures which are not part of the safety function (MTTR = 8 h). The value is for the safety function of the device.

Table 2.3

The characteristic safety values like PFD, PFH, SFF, HFT and T_1 (proof test interval) are taken from the FMEDA. Please note, 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 Safety Recommendation

3.1 Interfaces

The device has the following interfaces. For corresponding terminals see data sheet.

- Safety relevant interfaces:
  - HiC2095: input, output
  - HiD2096: input I, input II, output I, output II
- Non-safety relevant interfaces: power supply

3.2 Configuration

The device must be configured through the user accessible DIP switches for the required input function before the start-up. During the functionality any change of the operating function (DIP switch modification) can invalidate the safety function behavior and must be avoided.

The devices provide a suitable cover to protect against accidental changes.

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.

2015-02

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 stated in the "Characteristic Safety Values" chapter (see chapter 2.4).

It is under the responsibility of the operator to define the type of proof test and the 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 > 90 %).

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.
- Oscilloscope
- Transformer with voltage output
- Power supply set at nominal voltage of 24 V DC.
- Apparatus suitable for generating the signals for test B.
- Load of 1.8 kΩ and 900 Ω for the input, 10 kΩ for the output.

Procedure

The proof test recognizes dangerous concealed faults that would affect the safety function of the plant.

It is possible that the device is used under other circumstances than specified within the assumptions for the FMEDA assessment. The calculations for the safety loop can also reveal that the device may claim a different amount of the PFD value (standard is 10 %). Both effects can have an influence on the proof test time.

It is the responsibility of the operator to select a suitable proof test time.

The entire measuring loop must be put out of service and the process held in safe condition by means of other measures.

Test A

Connect a multimeter between pins 5a and 1a. Connect multimeters between pins 5a and 7b and pins 1a and 3a for HiD2096.

The current must be calculated from the measured voltage. This current flowing must match the DIP switch setting. Try all three settings as given on the side of the device.

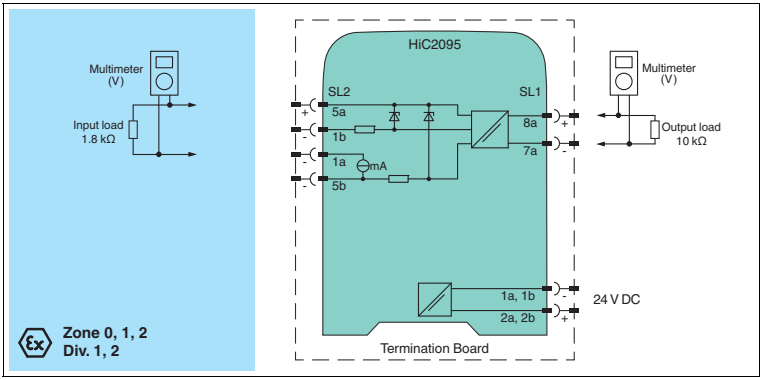

Figure 4.1 Set-Up for Proof Test A of HiC2095

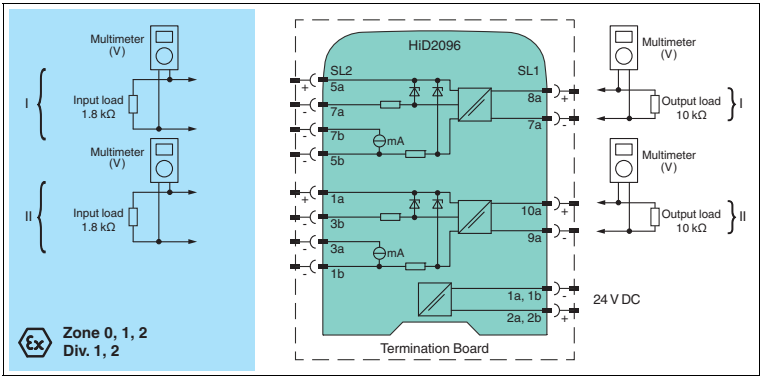

Figure 4.2 Set-Up for Proof Test A of HiD2096

Test B

- Connect a voltage source between pins 5a and 1b for HiC2095. Connect voltage sources between pins 5a and 7a and pins 1a and 3b for HiD2096.
- Attach input load 900 Ω between terminals 5a and 5b. For HiD2096, additionally attach input load 900 Ω between terminals 1a and 1b.

Apply voltages of -5 V, -10 V. -20 V at the input. The output voltage must be within ± 200 mV.

Input voltage	Output voltage
-5 V	-5 V ± 200 mV
-10 V	-10 V ± 200 mV
-20 V	-20 V ± 200 mV

Table 4.1

Test C

1. Apply -2 V DC + 1.414 V_{rms} sine wave at 20 kHz to the input.
2. Measure the amplitude of the sine wave at input and output.
   The output voltage amplitude must be at least 0.891 times the input voltage amplitude (i. e. the reduction in amplitude must not exceed 1 dB).

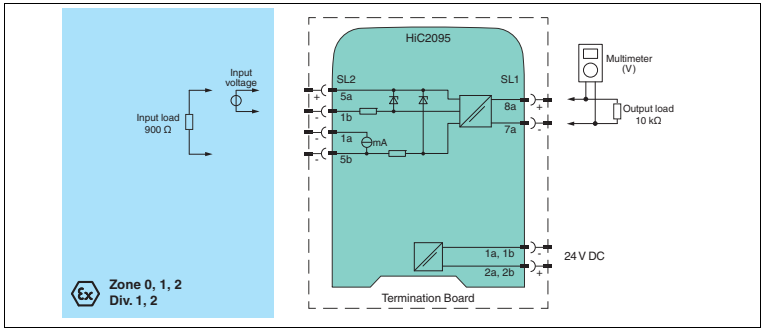

Figure 4.3 Set-Up for Proof Tests B and C of HiC2095

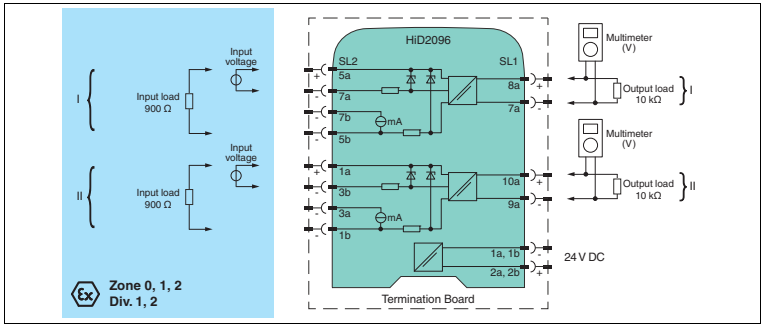

Figure 4.4 Set-Up for Proof Tests B and C of HiD2096

2015-02

Tip

Normally the easiest way to test HiC modules is by using a stand-alone HiCTB**-SCT-***-**-** termination board. The tester then has no need to disconnect wires in the existing application, so subsequent miswiring of the module is prevented.

Tip

Normally the easiest way to test HiD modules is by using a stand-alone HiDTB**-SCT-***-**-** termination board. The tester then has no need to disconnect wires in the existing application, so subsequent miswiring of the module is prevented.

End of Test

1. Disconnect the ancillary equipment.
2. Restore the safety loop.
3. Remove any bypass of safety function.

5 Abbreviations

DCS	**D**istributed **C**ontrol **S**ystem
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
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
$\mathbf{PFD}_{avg}$	Average **P**robability of **F**ailure on **D**emand
PFH	**P**robability of dangerous **F**ailure per **H**our
PLC	**P**rogrammable **L**ogic **C**ontroller
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
$\mathbf{T}_1$	Proof Test Interval

2015-02

2015-02

2015-02

2015-02

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

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

Subject to modifications
Copyright PEPPERL+FUCHS • Printed in Germany

DOCT-3677
02/2015