SAFETY MANUAL SIL

SMART Universal Barrier
HiC2441

SIL
IEC 61508/61511

ISO9001

CE

SIL 2

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"

2015-11

1 Introduction

1.1 General Information

This manual contains information for application of the device in functional safety related control loops.

The corresponding datasheets, instruction manuals, EU declarations of conformity, EC-type-examination certificates, certificates, control drawings, and the functional safety assessment if applicable supplement this document. You can find this information under www.pepperl-fuchs.com.

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

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

Use the device only with the approved external devices.

In the case of a device fault, proceed as follows:

- Take the device out of operation.
- Secure the device against accidental restart.
- If there is a defect, the device must be repaired by the manufacturer.

If the safety control loop is interrupted, the safety function is no longer guaranteed. This interruption can cause personal injury or property damage.

- Do not de-activate the device.
- Do not bypass the safety function.
- Do not repair, change or maipulate the device.

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

1.2 Intended Use

This isolated barrier is used for intrinsic safety applications.

The device combines the functionalities of standard AI/AO and DI/DO isolated barriers. The device is transparent to signals in both directions and provides the galvanic isolation for separating the hazardous area from the safe area.

The device requires no configuration and adapts itself automatically to the function of the active input/output of the connected process control system.

The device permits the bi-directional pass-through of the HART communication.

The device is designed primarily for use with universal I/O cards.

This device mounts on a HiC Termination Board.

2015-11

The following applications are supported:

Analog input

The device transfers a 4 mA to 20 mA analog signal of a transmitter in the hazardous area to the DCS. The input (field side) works as current input with supply for current sink transmitters and as current input for current source transmitters. The output (control side) works as current sink.

The device is transparent to SMART communication signals between the input and the output.

Analog output

The device transfers the 4 mA to 20 mA signal of the DCS to an I/P converter in the hazardous area. The output (field side) works as current source. The input (control side) works as current sink.

The device is transparent to SMART communication signals between the input and the output.

Digital input

The device transfers the input current of a NAMUR sensor or dry contact located in the hazardous area to the DCS. The input (field side) works as current input with a voltage source within the NAMUR specification (EN 60947-5-6). The output (control side) works as current sink.

Digital output

The device transfers the 24 V/45 mA signal of the DCS to a solenoid/valve in the intrinsically safe area. The output (field side) works as voltage source. The transferred voltage is limited according to the intrinsically safe requirements. The input (control side) works as voltage input.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

HiC2441
Up to SIL2

1.4 Relevant Standards and Directives

Device specific standards and directives

Electromagnetic compatibility	EN 61326-1:2013 (industrial locations), EN 61326-3-2:2008 (specified environment), NE 21:2006
Functional safety	IEC 61508 part 1 – 7, edition 2010: Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)

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 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)

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)

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 control loop. The device under consideration is always part of a safety control loop but is not regarded as a complete element or subsystem.

For calculating the SIL of a safety control 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 safety-related device is considered to be of type **A** element with a hardware fault tolerance of **0**.
- Failure rate based on the Siemens standard SN29500.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- Any safe failures that occur (e. g., output in safe condition) will be corrected within 8 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 stress levels are average for an industrial environment and the environment is similar to 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. 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 70 °C, the failure rates must be multiplied by a factor of 3.3 based on experience. A similar factor must be used if frequent temperature fluctuations are expected.
- The HART function is not part of the safety function. The HART function does not transmit safety-relevant messages.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.

SIL 2 application

- The device shall claim less than 10 % of the total failure budget for a SIL 2 safety control loop.
- For a SIL 2 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 SIL 2 application operating in high demand mode 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 control loop has a hardware fault tolerance of **0** and it is a type **A** element, the SFF must be > 60 % according to table 2 of IEC 61508-2 for a SIL 2 (sub) system.

2015-11

2.3 Safety Function and Safe State

Safe State

- Analog input: output current at terminals 8a (11) and 7a (14), < 3.6 mA or > 21.5 mA
- Analog output: output current at terminals 5a (1) and 5b (4), < 3.6 mA
- Digital input: output current at terminals 8a (11) and 7a (14), < 0.3 mA or > 6 mA
- Digital output: output current at terminals 5a (1) and 5b (4), < 0.3 mA

Safety Function

- Analog input:
  The output at terminals 8a (11), 7a (14) repeats the input current at terminals 5a (1), 5b (4) or terminal 5a (1),1b (5) with an accuracy of 2 %.
- Analog output:
  The output at terminals 5a (1), 5b (4) repeats the input current at terminals 8a (11), 7a (14) with an accuracy of 2 %.
- Digital input:
  The output at terminals 8a (11), 7a (14) repeats the input current at terminals 5a (1), 1a (2) with an accuracy of 2 %.
- Digital output:
  The output at terminals 5a (1), 5b (4) changes the state based on the voltage at the input at terminals 8a (11), 7a (14) of 19 V to 30 V or 0 V to 5 V, to
  - ON state (19 V to 30 V input) → The maximum possible current is driven at the output, depending on the output load, with an accuracy of 2 %.
  - OFF state (0 V to 5 V input) → A current < 0.1 mA is driven at the output, independent of the output load.

Reaction Time

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

2.4 Characteristic Safety Values

Parameters acc. to IEC 61508	Variables			
Assessment type and documentation	Full assessment			
Device type	A			
Demand mode	Low Demand Mode or High Demand Mode			
HFT	0			
SIL (hardware)	2			
SC	2			
Total failure rate (only safety function)	530 FIT			
Total failure rate (whole device)	541 FIT			
MTBF [1]	211 years			
Function	Analog input	Analog output	Digital input	Digital output
$\lambda_{sd} + \lambda_{su}$	309 FIT	312 FIT	306 FIT	297 FIT
λ_{dd}	171 FIT	169 FIT	165 FIT	167 FIT
λ_{du}	49.9 FIT	48.8 FIT	58.8 FIT	65.3 FIT
$\lambda_{no\ effect}$	292 FIT	297 FIT	290 FIT	276 FIT
$\lambda_{not\ part}$	11 FIT	11 FIT	11 FIT	11 FIT
SFF	78 %	79 %	75 %	74 %
PTC	99 %	99 %	99 %	99 %
PFH (= λ_{du})	4.99×10^{-8} 1/h	4.88×10^{-8} 1/h	5.88×10^{-8} 1/h	6.53×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	2.19×10^{-4}	2.14×10^{-4}	2.58×10^{-4}	2.86×10^{-4}
PFD_{avg} for T_1 = 2 years	4.37×10^{-4}	4.27×10^{-4}	5.15×10^{-4}	5.72×10^{-4}
PFD_{avg} for T_1 = 5 years	1.09×10^{-3}	1.07×10^{-3}	1.29×10^{-3}	1.43×10^{-3}

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

Table 2.1

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).

3 Safety Instructions

3.1 Interfaces

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

- Safety relevant interfaces: input, output
- Non-safety relevant interfaces: power supply
  The HART communication is not relevant for functional safety.

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 lifetime of elements 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 element itself and its operating conditions – temperature in particular. For example, the 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 elements.

Therefore it is obvious that failure calculation is only valid for elements that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each element.

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 61508-2, a useful lifetime, based on experience, should be assumed. Experience has shown that the useful lifetime often lies within a range period of about 8 ... 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 there are no elements with reduced life time in the safety path (for example electrolytic capacitors, relays, flash memories, optocoupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful lifetime 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 or the safety integrity of the process must be maintained by using loop redundancy. 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 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 > 99 %).

The ancillary equipment required:

- 2 digital multimeters with an accuracy better than 20 µA in the mA/DC range
  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.
- 1 variable power supply 0 V DC to 24 V DC (required values are 5 V and 24 V)
- either two decade box resistors 0 kΩ to 10 kΩ,or the following set of resistors: 300 Ω, 820 Ω, 1500 Ω, 3300 Ω, 4700 Ω (1 %, ≥ 0.25 W)

Test Procedure

- 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 device as showed in next figure.
- Follow the steps indicated in the tables below.
- Restore the safety loop. Any by-pass of the safety function must be removed.

Connected field side terminals 1 and 4

Step No.	Conditions of test (field terminals between 1 and 4)			Measurement points		Notes
	R_L (Ω)	R_S (Ω)	V_S (V)	A1 (mA)	A2 (mA)	
1	0	3300	24	3.4 mA < A1 < 4.6 mA	as A1 ±0.05 mA	Simulation of analog output
2	3300	3300	24	3.4 mA < A1 < 4.6 mA	as A1 ±0.05 mA	
3	300	0	24	40.5 mA < A1 < 42.5 mA	as A1 ±0.10 mA	Simulation of digital output
4	0	0	24	40.5 mA < A1 < 42.0 mA	as A1 ±0.10 mA	
5	open	0	24	0 mA (open circuit)	< 0.10 mA	
6	300	0	5	< 0.10 mA	< 0.10 mA	
7	820	0	24	19.5 mA < A1 < 20.7 mA	as A1 ±0.05 mA	Simulation of analog input (2-wire Tx)
8	1500	0	24	11.8 mA < A1 < 12.8 mA	as A1 ±0.05 mA	
9	4700	0	24	4.0 mA < A1 < 4.7 mA	as A1 ±0.05 mA	

Table 4.1

Connected field side terminals 5 and 4

Step No.	Conditions of test (field terminals between 5 and 4)			Measurement points		Notes
	R_L (Ω)	R_S (Ω)	V_S (V)	A1 (mA)	A2 (mA)	
10	4700	0	24	3.9 mA < A1 < 4.6 mA	as A1 ±0.05 mA	Simulation of analog input (4-wire Tx)
11	820	0	24	18.5 mA < A1 < 19.7 mA	as A1 ±0.05 mA	

Table 4.2

Connected field side terminals 1 and 2

Step No.	Conditions of test (field terminals between 1 and 2)			Measurement points		Notes
	R_L (Ω)	R_S (Ω)	V_S (V)	A1 (mA)	A2 (mA)	
12	0	0	24	8.5 mA < A1 < 10.5 mA	as A1 ±0.05 mA	Simulation of digital input
13	1500	0	24	3.4 mA < A1 < 4.3 mA	as A1 ±0.05 mA	
14	4700	0	24	1.4 mA < A1 < 2.1 mA	as A1 ±0.05 mA	
15	open	0	24	0 mA (open circuit)	< 0.10 mA	

Table 4.3

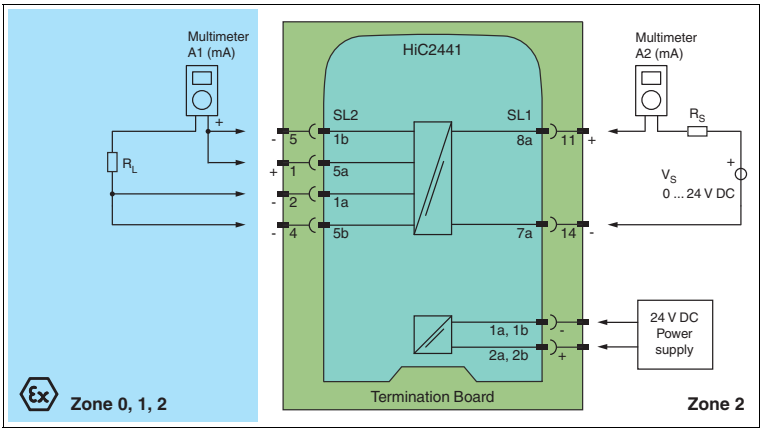

Figure 4.1 Proof test set-up for HiC2441

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.

5 List of Abbreviations

PCS	**P**rocess **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_{sd}	Probability of safe detected failure
λ_{su}	Probability of safe undetected failure
λ_{d}	Probability of dangerous failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{no\ effect}$	Probability of failures of elements in the safety control loop that have no effect on the safety function. The no effect failure is not used for calculation of SFF.
$\lambda_{not\ part}$	Probability of failure of elements that are not in the safety control loop
$\lambda_{total\ (safety\ function)}$	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**estoration
PFD_{avg}	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
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
T_1	Proof Test Interval

2015-11

2015-11

2015-11

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

DOCT-4679
11/2015