SAFETY MANUAL SIL

Switch Amplifier

HiD282*, HiD284*

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"

2012-12

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.com** or by contacting 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.

When it is not possible to correct faults, the devices must be taken out of service and action taken to protect against accidental use. Devices should 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.

1.2 Intended Use

General

These isolated barriers are used for intrinsic safety applications.

The devices transfer digital signals (NAMUR sensors/mechanical contacts) from a hazardous area to a safe area.

During an error condition the outputs de-energize.

A fault is signalized by LEDs acc. to NAMUR NE44 and a separate collective error message output.

The devices are plug-in devices to be inserted into a specific Termination Board.

HiD2821, HiD2822, HiD2824

A proximity sensor or switch controls normally open contact outputs for the safe area load. The output changes state when the input signal changes state. The normal output state can be reversed using DIP switches.

Line fault detection (LFD) can be selected or disabled via a DIP switch (not for HiD2821).

2012-12

HiD2842, HiD2844

A proximity sensor or switch controls passive transistors for the safe area load. The output changes state when the input signal changes state. The normal output state can be reversed using DIP switches.

Line fault detection (LFD) can be selected or disabled via a DIP switch.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

HiD2821, HiD2822, HiD2824
HiD2842, HiD2844

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 61326-1:2006
  - 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

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 T_{proof} (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 architecture)

2.1.2 High Demand Mode

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:

- PFH (**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 analysis:

- Only one input and one output are part of the considered safety function (only 2-channel version).
- 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 (**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 10^{-7} per hour.
- 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**.
- Since the circuit 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 SIL2 (sub)system.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HNBK-217F. Alternatively, the assumed 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. Humidity levels are assumed within manufacturer's rating. 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.
- The appearance of a safe error (e. g. output in safe state) is repaired within 8 hours (e. g. remove sensor burnout).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (for example: substitution by an equivalent device).
- The indication of a dangerous error (via fault bus) is detected within 1 hour by the logic solver (SPS).

2.3 Safety Function and Safe State

The safe state of each channel is "output de-energized". The safety function of the device is defined: whenever the input of the device is de-energized the output is not conducting.

A safety function can only be implemented in the normal mode of operation (close-energized). Line fault detection (LFD) must be activated.

HiD2821

- Switch S1 in "OFF" position.

HiD2822, HiD2824, HiD2842, HiD2844

- Switch "Phase" of the used channel in "OFF" position.
- Switch "LFD" in "ON" position.

LB/SC Diagnosis

The input loop of all versions is supervised, if the line fault detection is active (mandatory, see data sheet). The related output goes to the safe state in case of line fault.

Note!

The failure output is not evaluated for safety applications.

Reaction Time

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

2.4 Characteristic Safety Values

HiD282*

Parameters acc. to IEC 61508	Values
Assessment type and documentation	FMEDA report
Device type	A
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL	2
Safety function	Relay opens when input goes to off
λ_s	153 FIT
λ_{du}	40.0 FIT
$\lambda_{no\ effect}$	65.7 FIT
$\lambda_{total\ (safety\ function)}$	193 FIT
$\lambda_{not\ part}$	6.0 FIT
SFF	79.2 %
MTBF [1]	573 years
PFH	4.0×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.75×10^{-4}
PFD_{avg} for T_{proof} = 2 years	3.50×10^{-4}
PFD_{avg} for T_{proof} = 5 years	8.76×10^{-4}
Reaction time [2]	< 20 ms

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

[2] Time between fault detection and fault reaction.

Table 2.1

HiD284*

Parameters acc. to IEC 61508	Values
Assessment type and documentation	FMEDA report
Device type	A
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL	2
Safety function	Output de-energized when input is de-energized
λ_s	138 FIT
λ_{du}	22.0 FIT
$\lambda_{no\ effect}$	64.3 FIT
$\lambda_{total\ (safety\ function)}$	160 FIT
$\lambda_{not\ part}$	6.0 FIT
SFF	86.3 %
MTBF [1]	613 years
PFH	2.2×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	9.57×10^{-5}
PFD_{avg} for T_{proof} = 2 years	1.91×10^{-4}
PFD_{avg} for T_{proof} = 5 years	4.78×10^{-4}
Reaction time [2]	< 20 ms

[1] acc. to SN29500. This value includes failures which are not part of the safety function. Value for one channel only.

[2] Time between fault detection and fault reaction.

Table 2.2

The characteristic safety values like PFD, 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 device has the following interfaces. For corresponding terminals see data sheet.

- Safety relevant interfaces:
  - HiD2821: input I, output I, output II
  - HiD2822, HiD2842: input I, input II, output I, output II
  - HiD2824, HiD2844: input I, input II, input III, input IV, output I, output II, output III, output IV
- Non-safety relevant interfaces: output ERR

3.2 Configuration

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

The access to the DIP switches is permitted only through a small window on the side and by a small screw driver.

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.

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.

Maximum Switching Power of Output Contacts (HiD282* only)

The useful life time is limited by the maximum number of switching cycles under load conditions. The maximum number of switching cycles is depending on the electrical load and may be higher when reduced currents and voltages are applied. You can see the relationship between the maximum switching power and the load conditions in the diagram below.

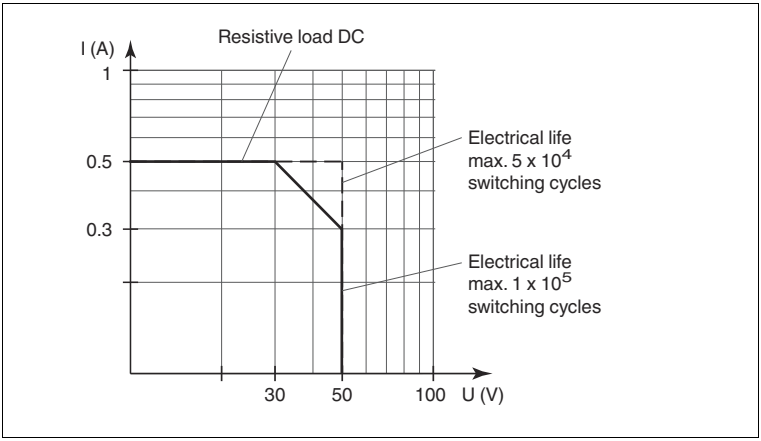

Figure 3.1

3.4 Installation and Commissioning

Installation has to consider all aspects regarding the SIL level of the loop. During installation or replacement of the device the loop has to shut down. Devices have to be replaced by the same type of devices.

4 Proof Test

4.1 Proof Test Procedure

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

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.

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 intrinsic safety circuits must be used. Intrinsic safety circuits that were operated with circuits of other types of protection may not be used as intrinsically safe circuits afterwards.
- Power supply set at nominal voltage of 24 V DC
- 220 Ω/15 kΩ for testing lead breakage and short circuit detection
- 4.7 kΩ potentiometer as input load
- 240 Ω/2.5 W as output load for HiD282* devices or 2.4 kΩ as output load for HiD284* devices

The settings have to be verified after the configuration by means of suitable tests.

Procedure:

Sensor state must be simulated by a potentiometer of 4.7 kΩ (threshold for normal operation), by a resistor of 220 Ω (short circuit detection) and by a resistor of 150 kΩ (lead breakage detection).

The input test needs to be done for each input channel individually. The threshold must be between 1.4 mA and 1.9 mA, the hysteresis must be between 170 µA and 250 µA. As the device is driven in normal mode of operation, the relay must be activated (yellow LED on), if the input current is above the threshold.

If the resistor R_{SC} (220 Ω) or the resistor R_{LB} (150 kΩ) is connected to the input, the unit must detect an external error. The red LED shall be flashing and the relay of the corresponding channel shall de-activate.

In case of the HiD282* the relay output in the safety path needs to be tested with a certain current, i. e. 100 mA. To avoid any electrical shock problems, we recommend to use 24 V DC for this test. For the philosophy of Functional Safety it is important to test, that the relay contacts are **definitely open**, if the relay is de-activated. For the HiD284* the current must be in the allowed current range as given in the data sheet, as example 10 mA are chosen.

After the test the unit needs to be set back to the original settings for the current application. Further the switches for the settings need to be saved against undeliberate changes. This can be achieved by means of a (translucent) adhesive label. For HiD units across the hole where the switches are underneath.

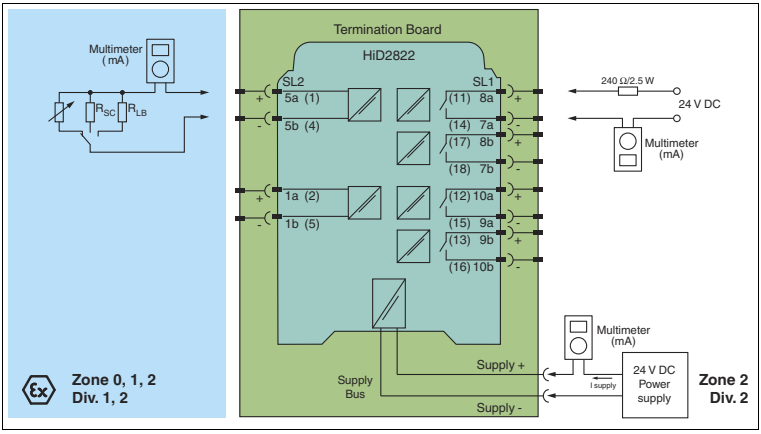

Figure 4.1 Proof test set-up for HiD2822

This example shows the test of one NAMUR input and the first relay output. For all HiD282* devices test the input and output that are used in the safety function application and the respective safety path.

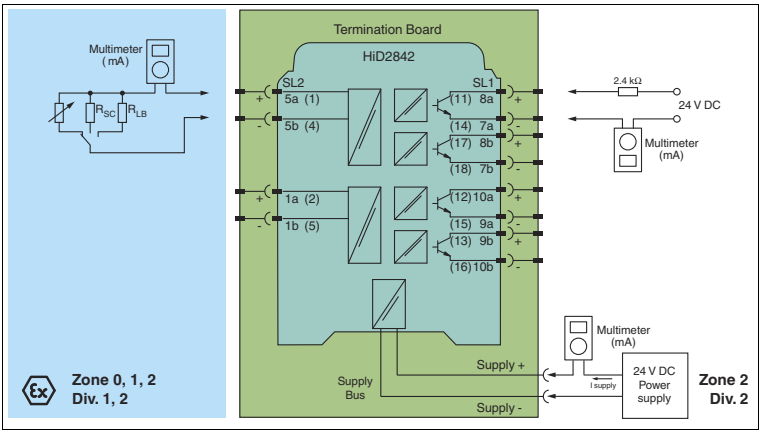

Figure 4.2 Proof test set-up for HiD2842

This example shows the test of one NAMUR input and the first relay output. For all HiD284* devices test the input and output that are used in the safety function application and the respective safety path.

Tip

Normally the easiest way to test H-System modules is by using a stand-alone HiDTB08-UNI-SC-SC Termination Board. The tester then has no need to disconnect wires in the existing application, so subsequent miswiring of the module is prevented.

5 Abbreviations

DCS	**D**istributed **C**ontrol **S**ystem
ESD	**E**mergency **S**hut**d**own
FIT	**F**ailure **I**n **T**ime
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
PFD_{avg}	Average **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}	Proof Test Interval
ERR	Error
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

2012-12

2012-12

2012-12

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

TDOCT-2866AENG
12/2012