PROCESS AUTOMATION

SAFETY MANUAL SIL

Current Driver

HiD2033, HiD2034, HiD2037, HiD2038(Y)

SIL
IEC 61508/61511

ISO9001

SIL2

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

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 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.

1.2 Intended Use

General

These isolated barriers are used for intrinsic safety applications.

The devices are mounted on a HiD Termination Board.

HiD2033, HiD2034

The devices repeat a 4 mA ... 20 mA input signal from a control system to drive I/P converters, valve actuators, and displays located in a hazardous area.

The devices are loop powered with a low voltage drop and permit detection of line faults by the control system.

An open field circuit presents a high impedance to the control side to allow alarm conditions to be monitored by control systems.

The HiD2033 is a 1-channel device, the HiD2034 is a 2-channel device.

HiD2037, HiD2038(Y)

The devices repeat a 4 mA ... 20 mA input signal from a control system to drive SMART I/P converters, valve actuators, and displays located in a hazardous area.

The devices are bus powered.

Digital signals may be superimposed on the analog values in the hazardous or safe area, which are transferred bidirectionally.

An open field circuit presents a high impedance to the control side to allow alarm conditions to be monitored by control systems.

Line fault detection of the field circuit is indicated by a red LED and an output on the fault bus (only HiD2037 and HiD2038 devices). The fault conditions can be monitored via a Fault Indication Board.

The HiD2037 is a 1-channel device, the HiD2038(Y) is a 2-channel device.

The HiD2038Y device is designed for use with Yokogawa DCS systems.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

HiD2033
HiD2034
HiD2037
HiD2038(Y)

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 – 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_{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.

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

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:

- 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}.
- 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 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.
- 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 ºC over a long period. A moisture level within the manufacturer's specifications is assumed. For a higher average temperature of 60 ºC, 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 will be corrected within eight hours.
- While the device is being repaired, measures must be taken to maintain the safety function.
- The HART protocol is only used for setup, calibration, and diagnostic purposes, not during operation.

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 current (4 mA ... 20 mA) with a tolerance of 2 %.

Safe State

The safe state is defined as the output being < 4 mA.

Reaction Time

The reaction time for all safety functions is < 100 ms.

2.4 Characteristic Safety Values

HiD2033, HiD2034

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	Signal transfer
λ_s [1]	160 FIT
λ_{dd}	0 FIT
λ_{du}	36.9 FIT
$\lambda_{no\ effect}$	105 FIT
$\lambda_{total\ (safety\ function)}$	197 FIT
$\lambda_{not\ part}$	41.6 FIT
SFF	81.25 %
MTBF [2]	579 years
PFH	3.69×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.61×10^{-4}
PFD_{avg} for T_{proof} = 2 years	3.23×10^{-4}
PFD_{avg} for T_{proof} = 5 years	8.07×10^{-4}
PTC	100 %
Reaction time [3]	< 100 ms

[1] Not considered failures are considered 50 % as dangerous undetected and 50 % as "No effect". "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[2] acc. to SN29500. This value is calculated for one safety function of a device.

[3] Time between fault detection and fault reaction.

Table 2.1

HiD2037, HiD2038(Y)

Parameters acc. to IEC 61508	Values
Assessment type and documentation	Full assessment
Device type	A
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL	2
Safety function	Signal transfer
λ_s [1]	301 FIT
λ_{dd}	0 FIT
λ_{du}	64.0 FIT
$\lambda_{no\ effect}$	148 FIT
$\lambda_{total\ (safety\ function)}$	365 FIT
$\lambda_{not\ part}$	86 FIT
SFF	82.48 %
MTBF [2]	312 years
PFH	6.40×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	2.80×10^{-4}
PFD_{avg} for T_{proof} = 2 years	5.61×10^{-4}
PFD_{avg} for T_{proof} = 5 years	1.40×10^{-4}
PTC	100 %
Reaction time [3]	< 100 ms

[1] Not considered failures are considered 50 % as dangerous undetected and 50 % as "No effect". "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[2] acc. to SN29500. This value is calculated for one safety function of a device.

[3] 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:
  - HiD2033, HiD2037: input I, output I
  - HiD2034, HiD2038(Y): input I, input II, output I, output II
- Non-safety relevant interfaces:
  - HiD2037, HiD2038(Y): power supply
  - HiD2037, HiD2038: fault output
  - 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 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 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.
  - Power supply set at nominal voltage of 24 V DC
  - Process calibrator with mA current source/sink feature (accuracy better than 20 µA)
- 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 (see figures).
- Test the devices by using the current values according to table below.
- Restore the safety loop. Any by-pass of the safety function must be removed.

Step No.	Set input value (mA)	Measurement point
		Output value (mA)
1	20.00	20.00 ± 0.4
2	12.00	12.00 ± 0.4
3	4.00	4.00 ± 0.4
4	23.00	23.00 ± 0.4
5	0	< 0.3

Table 4.1 Steps to be performed for the proof test

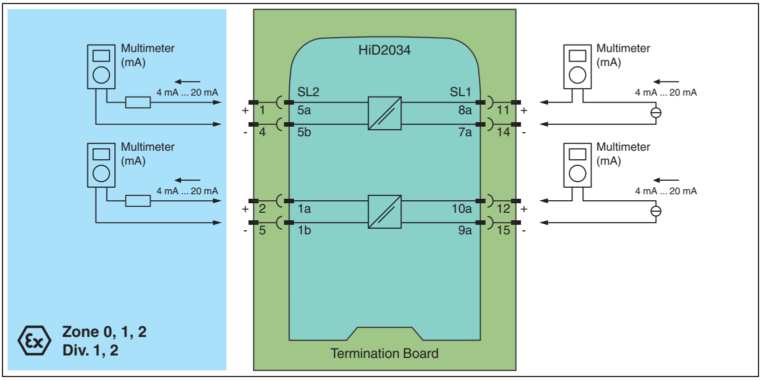

Figure 4.1 Proof test set-up for HiD2033, HiD2034

Channel 2 only for HiD2034.

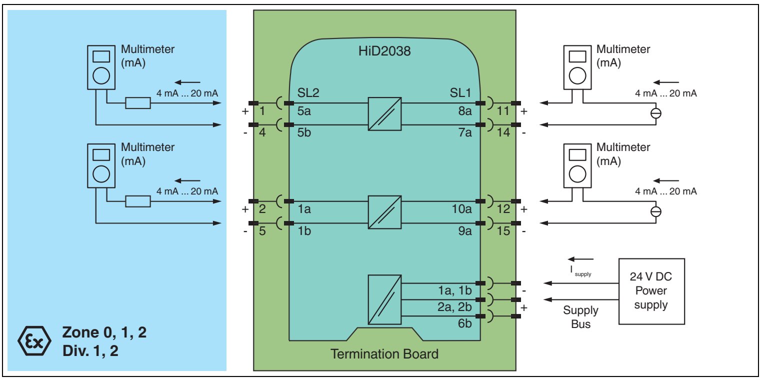

Figure 4.2 Proof test set-up for HiD2037, HiD2038(Y)

Channel 2 only for HiD2038(Y). The fault indication output is not available on HiD2038Y.

Tip

Normally the easiest way to test H-System modules is by using a stand-alone HiCTB08-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 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
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

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-3727
07/2014