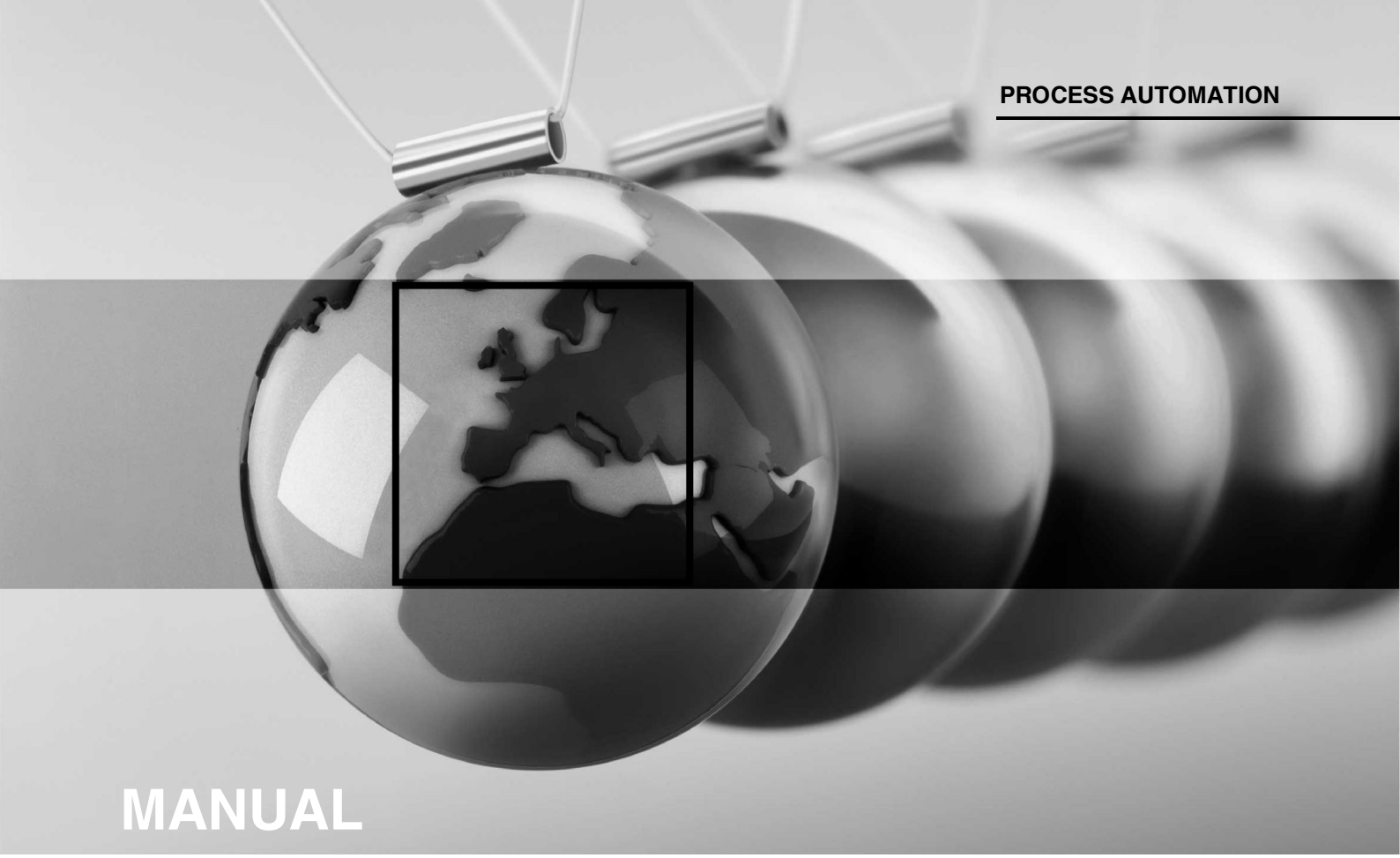

MANUAL

Functional Safety

Solenoid Driver
HiD2872, HiC2873(Y1), HiD2876, HiC2877

SIL
IEC 61508/61511

ISO9001

CE

SIL 2
SIL 3

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"

2019-07

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

Note!

This document does not substitute the instruction manual.

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:

- 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.

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.

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.

2019-07

2 Product Description

2.1 Function

General

This isolated barrier is used for intrinsic safety applications.

The device supplies power to solenoids, LEDs and audible alarms located in a hazardous area.

The output signal has a resistive characteristic. As a result the output voltage and current are dependent on the load.

Line fault detection of the field circuit is indicated by a red LED and an output on the fault bus.

HiD2872

This device is a 2-channel device.

The device is loop powered or bus powered.

It is controlled with a loop powered control signal, switch contact, transistor, or logic signal.

At full load, 12 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

An alternative low current output is available for driving a single LED without installing an external current limiting resistor.

This device mounts on a HiD Termination Board.

HiC2873

This device is a 1-channel device.

The device is loop powered or bus powered.

It is controlled with a loop powered control signal, switch contact, transistor, or logic signal.

At full load, 12 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

This device mounts on a HiC termination board.

HiC2873Y1

This device is a 1-channel device.

The device is bus powered.

The device is controlled with a switch contact, transistor, or logic signal.

At full load, 12 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

This device mounts on a HiC termination board.

HiD2876

This device is a 2-channel device.

The device is loop powered or bus powered.

It is controlled with a loop powered control signal, switch contact, transistor, or logic signal.

At full load, 11.2 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

An alternative low current output is available for driving a single LED without installing an external current limiting resistor.

This device mounts on a HiD Termination Board.

HiC2877

This device is a 1-channel device.

The device is loop powered or bus powered.

It is controlled with a loop powered control signal, switch contact, transistor, or logic signal.

At full load, 11.2 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

This device mounts on a HiC termination board.

2019-07

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces:
  - HiC2873(Y1), HiC2877: input I, output I
  - HiD2872, HiD2876: input I, input II, output I, output II
- Non-safety relevant interfaces: power supply, fault output

Note!

For corresponding connections see datasheet.

2.3 Marking

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

HiD2872 HiC2873 HiD2876 HiC2877	Up to SIL 2 (bus powered) Up to SIL 3 (loop powered)

HiC2873Y1	Up to SIL 2 (bus powered)

2.4 Standards and Directives for Functional Safety

Device-specific standards and directives

Functional safety	IEC/EN 61508, part 2, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1 – 3, edition 2003: Functional safety – Safety instrumented systems for the process industry sector (user)

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 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.

2019-07

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rate based on the Siemens standard SN 29500.
- 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 °C may be assumed. For a higher average temperature of 60 °C, 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.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- Since the outputs of the device use common components, these outputs must not be used in the same safety function.

SIL 2 application (bus powered)

- A SIL 2 application can also be implemented in bus powered mode.
  For corresponding connections see datasheet.
- The device shall claim less than 10 % of the total failure budget for a SIL 2 safety 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 safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 60 % according to table 2 of IEC/EN 61508-2 for a SIL 2 (sub) system.

SIL 3 application (loop powered)

- SIL 3 is not available for HiC2873Y1.
- A SIL 3 application can only be implemented using the loop powered mode.
  For corresponding connections see datasheet.
- The device shall claim less than 10 % of the total failure rate for a SIL 3 safety loop.
- For a SIL 3 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^{-3}, hence the maximum allowable PFD_{avg} value would then be 10^{-4}.
- For a SIL 3 application operating in high demand mode the total PFH value of the SIF should be smaller than 10^{-7} per hour, hence the maximum allowable PFH value would then be 10^{-8} per hour.
- Since the safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 90 % according to table 2 of IEC/EN 61508-2 for a SIL 3 (sub) system.

3.3 Safety Function and Safe State

Safe State

The safe state of the output is the de-energized state. The output current is less than 0.4 mA.

Safety Function

The output is de-energized if the input is in low state. The low state is reached when the input voltage is 5 V or below or the contact is open.

DIP switch settings

The device is configured by DIP switches.

The filter (switch S6) and the line fault detection (switch S5) are not safety relevant. However, use of the line fault detection feature is recommended for safety applications. Consider the consequences if the device remains in the safe state.

Reaction Time

The combined fault detection and fault reaction time is the time in which the device reacts to an occurred fault.

The reaction time (switch off delay) for the safety function is < 100 ms.

Note!

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

SIL 3 Application (Loop Powered)

Parameters	Characteristic values
Assessment type	FMEDA report
Device type	A
Mode of operation	Low demand mode, high demand mode or continuous mode
Safety function	De-energized if the input is in low condition
HFT	0
SIL	3
SC	3
λ_s	127 FIT
λ_{dd}	0 FIT
λ_{du}	0 FIT
$\lambda_{total\ (safety\ function)}$	127 FIT
$\lambda_{no\ effect}$	131 FIT
SFF	100 %
MTBF [1]	293 years
PFH [2]	0 1/h
PFD_{avg} for T_1 = 1 year [2]	0
T_1 max. [2]	Defined in "Proof Test" chapter but not necessary to validate the safety values, see chapter 5.1.
PTC	100 %
Reaction time [3]	< 100 ms

Table 3.1

1 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h.
The value is calculated for one safety function of the device.

2 As the λ_d failure rate is 0 FIT, a PFD calculation yields a PFD of zero, independent from the proof test interval.

3 Time between fault occurence and fault reaction

SIL 2 Application (Bus Powered)

Parameters	Characteristic values
Assessment type	FMEDA report
Device type	A
Mode of operation	Low demand mode, high demand mode or continuous mode
Safety function	De-energized if the input is in low condition
HFT	0
SIL	2
SC	3
λ_s	97 FIT
λ_{dd}	0 FIT
λ_{du}	30 FIT
$\lambda_{total\ (safety\ function)}$	127 FIT
$\lambda_{no\ effect}$	131 FIT
SFF	76 %
MTBF [1]	293 years
PFH	2.96×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	1.41×10^{-4}
PFD_{avg} for T_1 = 2 years	2.70×10^{-4}
PFD_{avg} for T_1 = 5 years	6.55×10^{-4}
PTC	99 %
Reaction time [2]	< 100 ms

Table 3.2

1 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h. The value is calculated for one safety function of the device.

2 Time between fault occurence and fault reaction

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).

3.5 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, 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 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 60 °C.

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

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.

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 instruction 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 24 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.

When the device is used in loop powered mode no dangerous failures can occur.
A proof test is not necessary. Nevertheless, we recommend a regular functional test of the device, e. g. in combination with the proof test of the final element.

Equipment required:

- Digital multimeter with an accuracy of 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
- Load resistor according to table

Check the settings after the configuration by suitable tests.

Proof Test Procedure

1. Connect load and supply as shown in the figures on the following pages.
2. Measure the output voltage via multimeter. Compare the value to the nominal value specified in the table below.
3. Short circuit the load resistor and measure the short circuit current via multimeter. Compare the resulting value to the nominal value specified in the table below.
4. Set the input voltage to 5 V.

   ↳ The output current must stay below 0.4 mA. This is the safety function: when the input is in low condition the output must definitely be de-energized.
5. If applicable, repeat the test procedure for output II by connecting the power supply between the appropriate terminals. Repeat the output voltage and short circuit test.
6. Restore the safety loop. Remove any by-passes from the safety loop.

Device	Output resistor (Ω)	Output voltage (V)	Short circuit current (mA)
HiD2872, HiC2873, HiC2873Y1	300	> 12	$50 < I_{sc} < 60$
HiD2876, HiC2877	280	> 11.2	$50 < I_{sc} < 60$

Table 5.1 Expected test results for the proof test

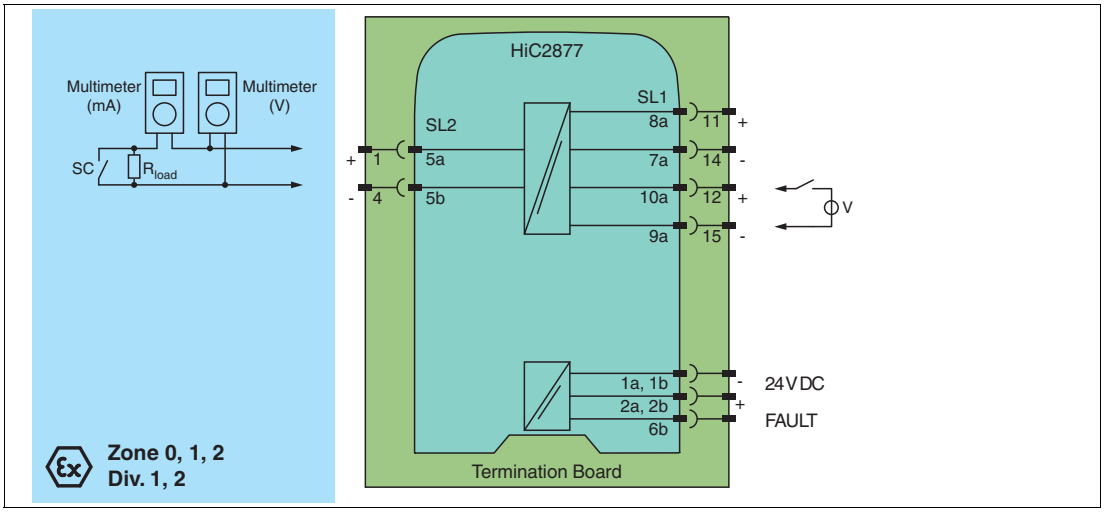

Figure 5.1 Proof test set-up for 1-channel devices (example HiC2877)

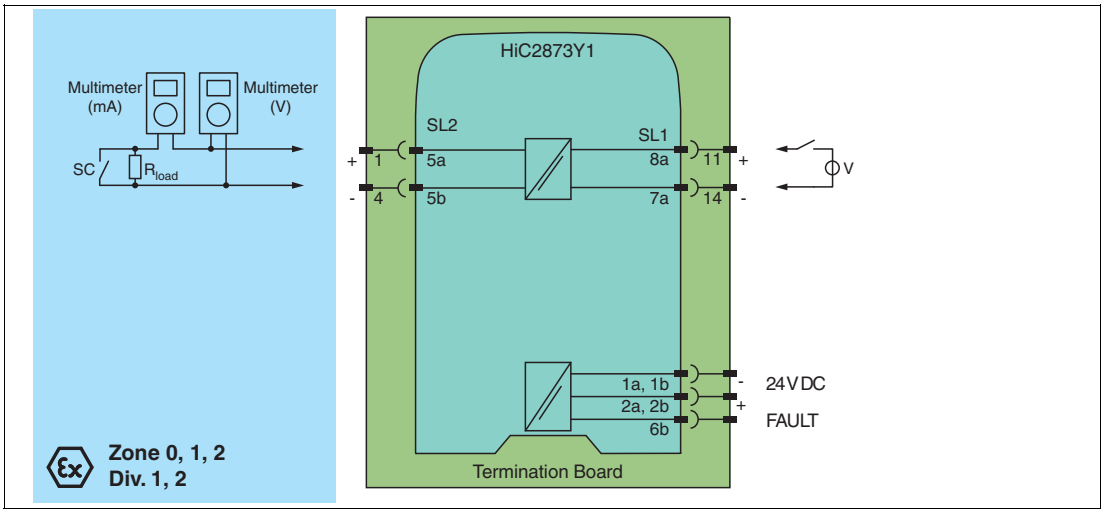

Figure 5.2 Proof test set-up for 1-channel device HiC2873Y1

Tip

The easiest way to test HiC devices is by using a stand-alone HiCTB**-SCT-***-**-** termination board. In this test, it is not necessary to disconnect the wiring of the existing application. Faults in a subsequent wiring can be avoided.

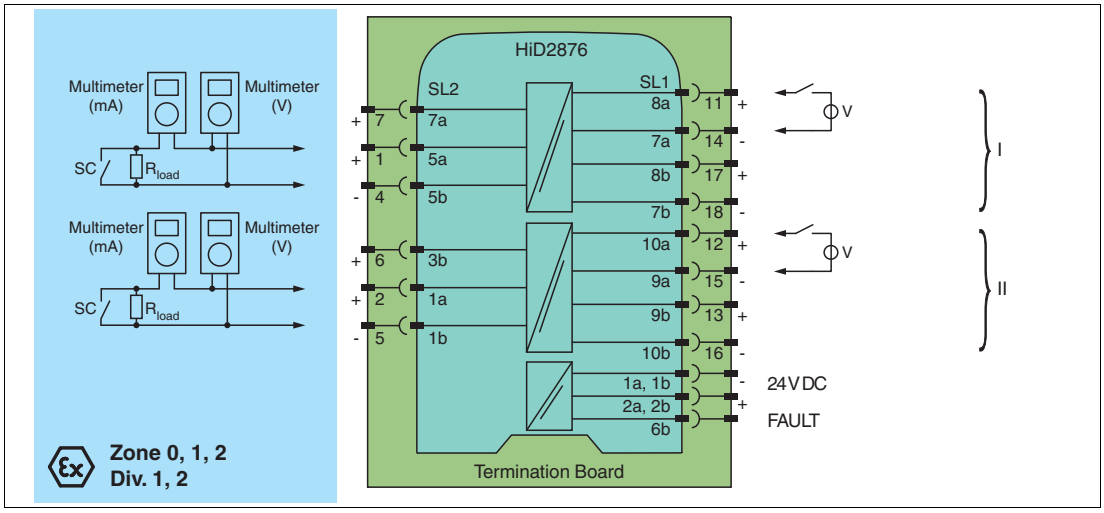

Figure 5.3 Proof test set-up for 2-channel devices (example HiD2876)

Tip

The easiest way to test HiD devices by using a stand-alone HiDTB**-SCT-***-**-** termination board. In this test, it is not necessary to disconnect the wiring of the existing application. Faults in a subsequent wiring can be avoided.

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.

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
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 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 components that are not in the safety loop
$\lambda_{total\ (safety\ function)}$	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_{avg}	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
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
T_1	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

2019-07

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-3721C
07/2019