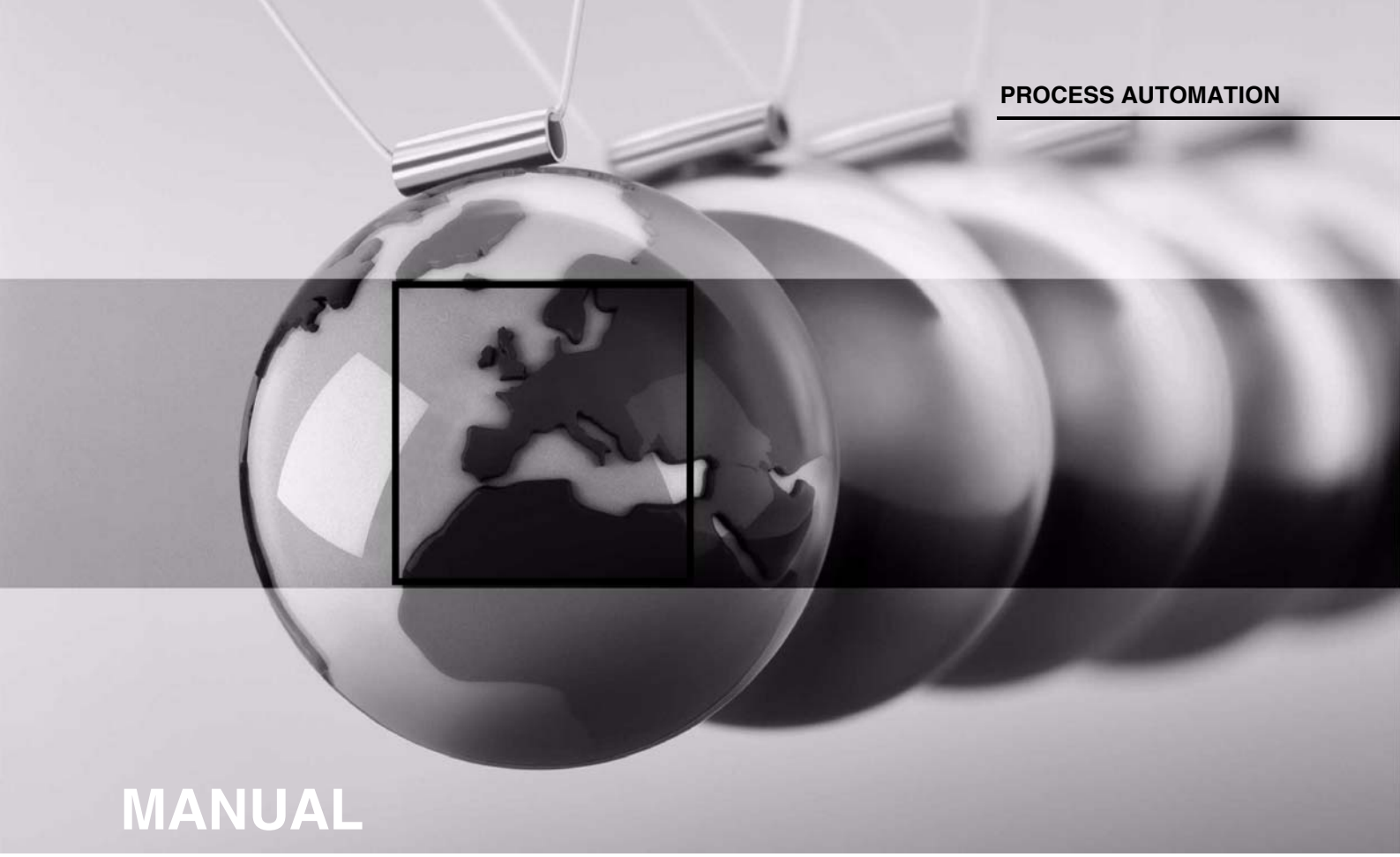

MANUAL

Functional Safety

SMART Transmitter Power Supply KCD2-STC-(Ex)1(.SP)(-Y1), HiC2025(Y1)

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"

1 Introduction 4
1.1 Content of this Document. 4
1.2 Safety Information 5
1.3 Symbols Used 6
2 Product Description. 7
2.1 Function 7
2.2 Interfaces 9
2.3 Marking 9
2.4 Standards and Directives for Functional Safety 9
3 Planning 10
3.1 System Structure. 10
3.2 Assumptions 11
3.3 Safety Function and Safe State 12
3.4 Characteristic Safety Values 13
3.5 Useful Lifetime 14
4 Mounting and Installation 15
4.1 Configuration 15
5 Operation 16
5.1 Proof Test Procedure 16
6 Maintenance and Repair 19
7 List of Abbreviations 20

2018-08

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.

2018-08

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.

2 Product Description

2.1 Function

KCD2-STC-1(.SP)

This signal conditioner provides the galvanic isolation between field circuits and control circuits.

The device supplies 2-wire transmitters in the field, and can also be used with current sources.

The device transfers the analog input signal to the control side as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

The output is selected as a current source, current sink, or voltage source via DIP switches.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

KCD2-STC-Ex1(.SP)

This isolated barrier is used for intrinsic safety applications.

The device supplies 2-wire transmitters in the hazardous area, and can also be used with current sources.

The device transfers the analog input signal to the non-hazardous area as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

The output is selected as a current source, current sink, or voltage source via DIP switches.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

SP version

The devices are available with screw terminals or spring terminals. The type code of the versions of the devices with spring terminals has the extension ".SP".

KCD2-STC-Ex1-Y1

This isolated barrier is used for intrinsic safety applications.

The device supplies 2-wire transmitters in the hazardous area.

The device transfers the analog input signal to the non-hazardous area as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

If the HART communication resistance in the loop is too low, the internal resistance can be used.

Test sockets for the connection of HART communicators are integrated into the terminals of the device.

The output is selected as a current source, current sink, or voltage source via DIP switches.

The device is mounted on a 35 mm DIN mounting rail according to EN 60715.

HiC2025

This isolated barrier is used for intrinsic safety applications.

The device supplies 2-wire transmitters in the hazardous area, and can also be used with current sources.

The device transfers the analog input signal to the non-hazardous area as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

The output is selected as a current source, current sink, or voltage source via DIP switches.

This device mounts on a HiC termination board.

HiC2025Y1

This isolated barrier is used for intrinsic safety applications.

The device supplies 2-wire transmitters in the hazardous area.

The device transfers the analog input signal to the non-hazardous area as an isolated current value.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

The output is selected as a current source, current sink, or voltage source via DIP switches.

This device mounts on a HiC termination board.

2018-08

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input I, output I
- Non-safety relevant interfaces: none
  The HART communication is not relevant for functional safety.

Note!

For corresponding connections see datasheet.

2.3 Marking

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

KCD2-STC-1(.SP)	Up to SIL 2
KCD2-STC-Ex1(.SP)(-Y1)	
HiC2025(Y1)	

2.4 Standards and Directives for Functional Safety

Device-specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 2, edition 2000: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1, 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.

2018-08

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rate based on the Siemens standard SN29500.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- The devices are not protected against power supply failures. It is within the responsibility of the user to ensure that low supply voltages are detected and adequate reaction on this fault is implemented.
- The safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- 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.
- The HART function is only used for configuration, calibration and diagnostics, not during operation.
- The indication of a dangerous failure (via fault bus) is detected within 1 hour by the programmable logic controller (PLC).

SIL 2 Application

- 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.

3.3 Safety Function and Safe State

Safety Function

The device transfers analog signals from the input to the output with a tolerance of 2 % related to the full signal range.

Use the following DIP switch settings for safety-relevant applications:

DIP Switch Settings KCD2-STC-(Ex)1(.SP)(-Y1)

Function	S1	S2	S3	S4
Current source 4 mA to 20 mA	II	II	I	II
Voltage source 1 V to 5 V	II	II	I	I
Current sink 4 mA to 20 mA	II	I	II	II

Table 3.1

DIP Switch Settings HiC2025(Y1)

Function	S1	S2	S3	S4
Current source 4 mA to 20 mA	OFF	OFF	ON	OFF
Voltage source 1 V to 5 V	OFF	OFF	ON	ON
Current sink 4 mA to 20 mA	OFF	ON	OFF	OFF

Table 3.2

Safe State

In the safe state, the following values must be reached at the output:

- < 3.6 mA or > 21.5 mA,
- < 0.9 V or > 5.375 V,

Reaction Time

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

Note!

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

Parameters	Characteristic values
Assessment type	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	122 FIT
λ_{dd}	172 FIT
λ_{du}	45 FIT
$\lambda_{no\ effect}$	122 FIT
$\lambda_{total\ (safety\ function)}$	338 FIT
$\lambda_{not\ part}$	72 FIT
SFF	86.8 %
MTBF [1]	278 years
PFH	4.45×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.95×10^{-4}
PFD_{avg} for T_{proof} = 2 years	3.90×10^{-4}
PFD_{avg} for T_{proof} = 5 years	9.74×10^{-4}
Reaction time [2]	< 20 ms

Table 3.3

1 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.
2 Time between fault detection and fault reaction

The characteristic safety values like PFD, SFF, HFT and T_1 are taken from the SIL report/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.

2018-08

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 Devices with DIP Switches on the Device Side

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.

Configuring the Devices with DIP Switches on the Front Side

The device is configured via DIP switches. The DIP switches for setting the safety functions are on the front of the device.

1. De-energize the device before configuring the device.
2. Open the cover.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Close the cover.
5. Secure the DIP switches to prevent unintentional adjustments.
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 instructions 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 8 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test Procedure

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.

Equipment required:

- Digital multimeter with an accuracy better than 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
- Process calibrator with current source and current sink function with an accuracy better than 20 µA

Proof Test Procedure

The proof test reveals almost all possible dangerous faults (diagnostic coverage > 90 %).

1. Put out of service the entire safety loop. Protect the application by means of other measures.
2. Prepare a test set-up, see figures below.
3. Test the devices. Verify the current values as given in table below.
4. Set back the device to the original settings for the application after the test.

Step No.	Input	Output		
	Input value (mA)	Output value (mA)	Output value for 2-wire Tx (V)	Output value for 4-wire Tx (V)
1	20.00	20.00 ± 0.4	15.2 ± 0.4	4.7 ± 0.5
2	12.00	12.00 ± 0.4	17.0 ± 0.4	4.7 ± 0.5
3	4.00	4.00 ± 0.4	18.9 ± 0.4	4.7 ± 0.5
4 [1]	23.00	23.00 ± 0.4	14.1 ± 0.4	4.7 ± 0.5
5 [1]	0	< 0.2	22.5 ± 0.5	n. a.
6	12.00			

Table 5.1 Steps to be performed for the proof test

[1] The output shall detect a fail high or fail low condition.

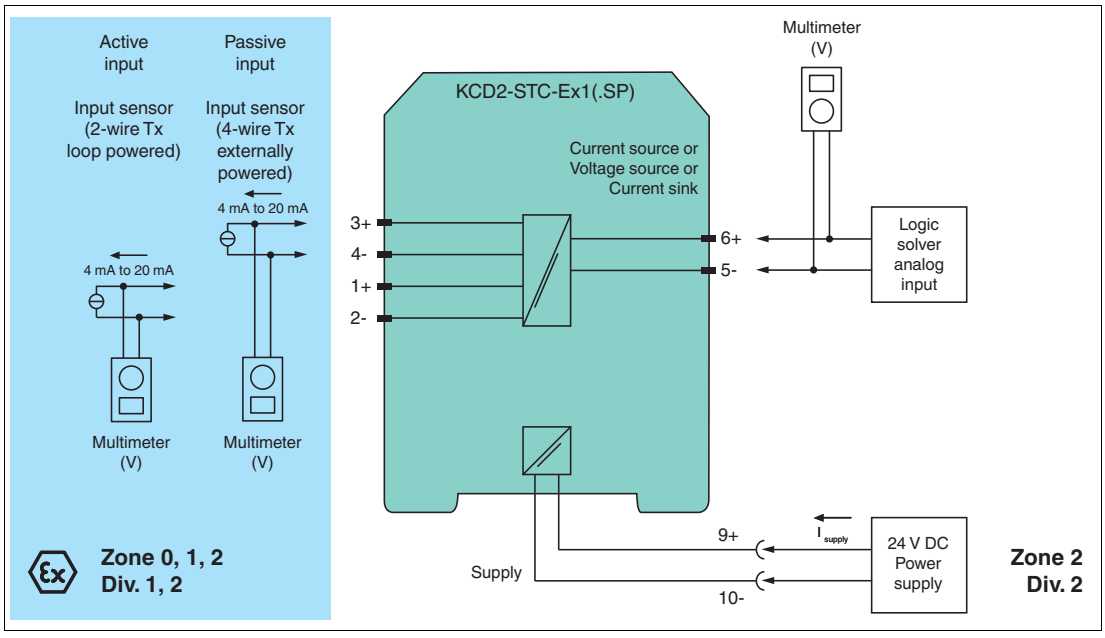

Figure 5.1 Proof test set-up for KCD2-STC-(Ex)1(.SP)(-Y1)

Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD2-STC-Ex1(.SP)(-Y1)
For Y1 version only connect the multimeter to terminals 1 and 2.

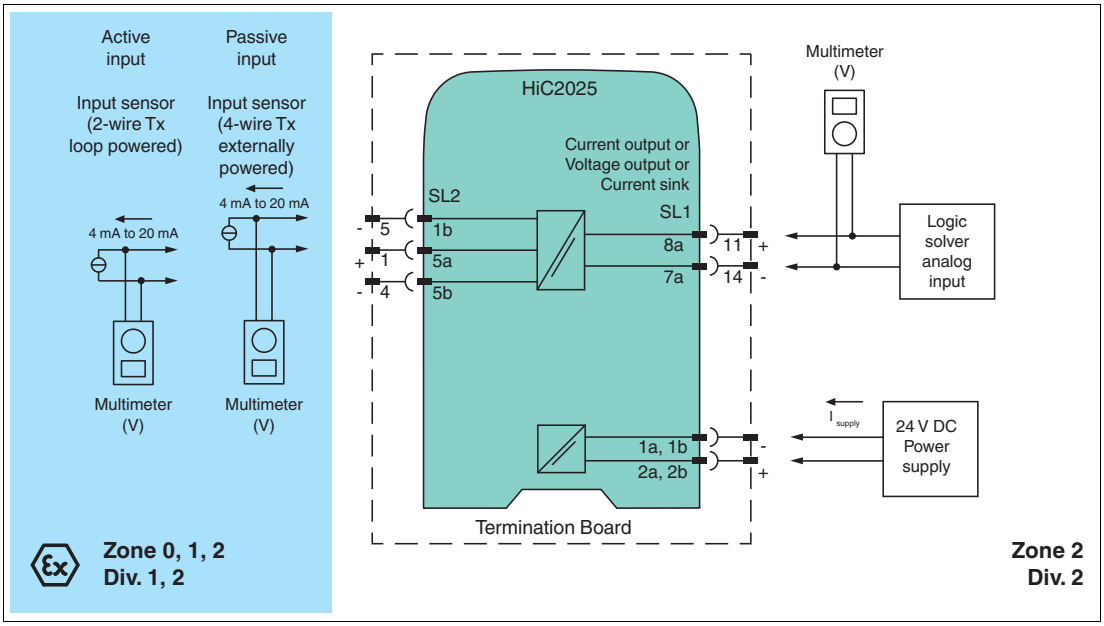

Figure 5.2 Proof test set-up for HiC2025(Y1)

For Y1 version only connect the multimeter to terminals 1 and 4.

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.

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
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIL (SC)	**S**afety **I**ntegrity **L**evel (**S**ystematic **C**apability)
SIS	**S**afety **I**nstrumented **S**ystem
T_1	Proof Test Interval

2018-08

2018-08

2018-08

2018-08

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-1596G
08/2018