SAFETY MANUAL SIL

SMART Transmitter Power Supply

KCD2-STC-Ex1.ES(.SP)
KFD2-STC4-Ex1.ES
HiC2025ES
HiD2025ES

SIL
IEC 61508/61511

ISO9001

CE

SIL3

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

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 dismounting of the device may only be carried out by appropriate trained and 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.

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

1.2 Intended Use

These isolated barriers are used for intrinsic safety applications. They provide 2-wire SMART transmitters with power in hazardous areas and transfer the analog values to the safe area. They are also used with 2-wire SMART current sources.

Digital signals may be superimposed on the analog values in the hazardous or safe area and are transferred bi-directionally.

The output may be configured by means of DIP switches to act as a voltage source, current source or current sink.

A separate fault output is signalled if the input signal is outside the range of 3 mA … 22 mA.

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

2015-06

The KCD2-STC-Ex1.ES(.SP) and KFD2-STC4-Ex1.ES are single channel devices for DIN rail mounting. The HiC2025ES and HiD2025ES are plug-in devices to be inserted respectively into a HiC or HiD Termination Board.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

KCD2-STC-Ex1.ES(.SP)
KFD2-STC4-Ex1.ES
HiC2025ES
HiD2025ES

Up to SIL3

1.4 Relevant Standards and Directives

Device specific standards and directives

- Functional safety IEC 61508 part 1 ... 7, edition 2010:
  Standard of functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer)
- Electromagnetic compatibility:
  - EN 61326-1:2013 (industrial locations)
  - EN 61326-3-2:2008 (specified environment)
  - 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_1 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:

- 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 °C over a long period. A moisture level within the manufacturer's specifications is assumed. For a higher average temperature of 60 °C, 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.
- The device shall claim less than 10 % of the total failure budget for a SIL3 safety loop.
- For a SIL3 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 SIL3 application operating in High Demand Mode of operation 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 loop has a Hardware Fault Tolerance of **0** and it is a type **A** component, the SFF must be > 90 % according to table 2 of IEC 61508-2 for a SIL3 (sub)system.
- Failure rates are constant, wear out mechanisms are not included.
- External power supply failure rates are not included.
- Failure rate based on the Siemens SN29500 data base.
- Any safe failures that occur (e. g. output in safe state) will be corrected within 8 hours (e. g. remove sensor fault).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (e. g. substitution by an equivalent device).
- The HART protocol is not part of the safety function. It does not transmit safety-relevant messages.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.

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 (in the range 3.6 mA ... 20.5 mA) with a tolerance of ±2 %.

Safe State

The safe state is defined, as the output being

- < 3.6 mA or > 20.5 mA (current output)
- < 0.9 V or > 5.125 V (voltage output)

Safety Response Time

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

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)	3
SC	3
$\lambda_{sd} + \lambda_{su}$	0 FIT
λ_{dd}	220 FIT
λ_{du}	9.9 FIT
$\lambda_{total\ (safety\ function)}$	531 FIT
$\lambda_{total\ (whole\ device)}$	598 FIT
$\lambda_{no\ effect}$	301.7 FIT
$\lambda_{not\ part}$	66.6 FIT
SFF	95.7 %
PTC [1]	99 %
MTBF [2]	191 years
PFH (= λ_{du})	0.99×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	0.95×10^{-4}
PFD_{avg} for T_1 = 2 years	1.32×10^{-4}
PFD_{avg} for T_1 = 5 years	2.45×10^{-4}

[1] Proof test coverage

[2] 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 (proof test interval) are taken from the FMEDA. Please note, 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 Recommendation

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, fault bus output
  The HART communication is not relevant for functional safety.

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 functionality any change of the operating function (DIP switch modification) can invalidate the safety function behavior and must be avoided.

The K-System devices provide a suitable cover to protect against accidental changes while on the H-System devices the access to the DIP switch 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.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime.

2015-06

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 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 and with the same DIP switch configuration.

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:
  - 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) or a
  - Field transmitter that has already been verified that doesn't contain any dangerous undetected fault.
- 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 KCD2-STC-Ex1.ES(.SP) device (see Figure 4.1), the KFD2-STC4-Ex1.ES device (see Figure 4.2), the HiC2025ES device (see Figure 4.3) or the HiD2025ES device (see Figure 4.4). Choose the proper input terminals (passive input or active input) in accordance with the specific application and follow the steps indicated in the table below.
- Restore the safety loop. Any by-pass of the safety function must be removed.

Step No.	Set input value (mA)	Mandatory measurement points (safety relevant)			Optional test (non-safety relevant)	
		Output value (mA)	Across 2-wire Tx (V)	Across 4-wire Tx (V)	LED indication	Fault bus output
1	20.00	20.00 ± 0.04	15.2 ± 0.4	5.0 ± 0.8	Green = ON Red = OFF	No fault
2	12.00	12.00 ± 0.04	17.0 ± 0.4	5.0 ± 0.8	Green = ON Red = OFF	No fault
3	4.00	4.00 ± 0.04	18.9 ± 0.4	5.0 ± 0.8	Green = ON Red = OFF	No fault
4	23.00	23.00 ± 0.05	14.4 ± 0.5	5.0 ± 0.8	Green = ON Red = ON	Fault
5	0	< 0.2	23 ± 1.0	n.a.	Green = ON Red = ON	Fault
6	12.00	Restored as step 2				

Table 4.1 Steps to be performed for the proof test

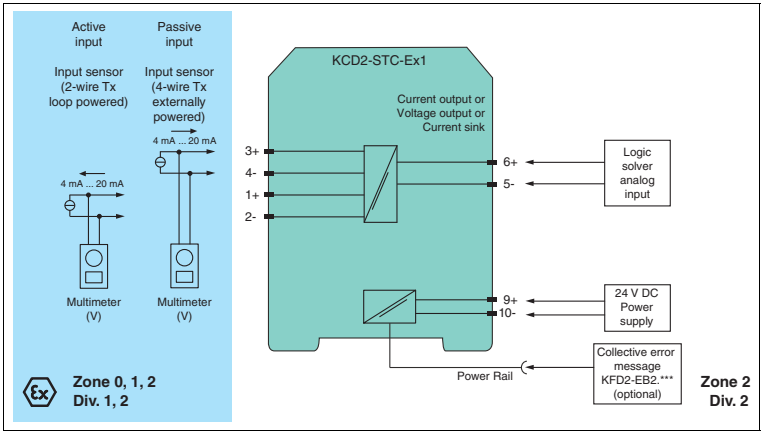

Figure 4.1 Proof test set-up for KCD2-STC-Ex1.ES(.SP)

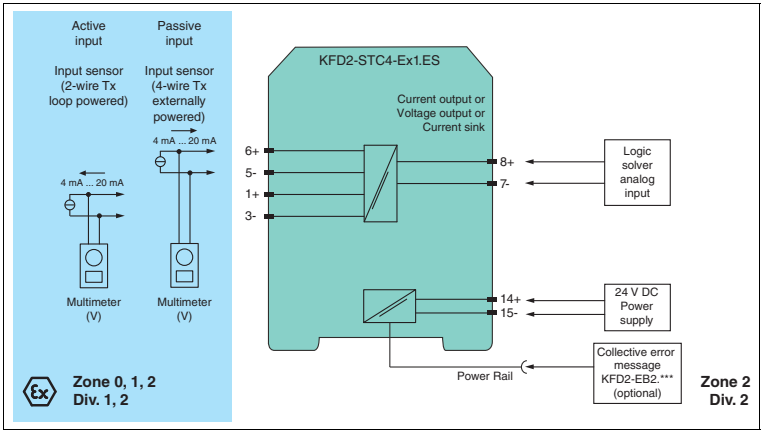

Figure 4.2 Proof test set-up for KFD2-STC4-Ex1.ES

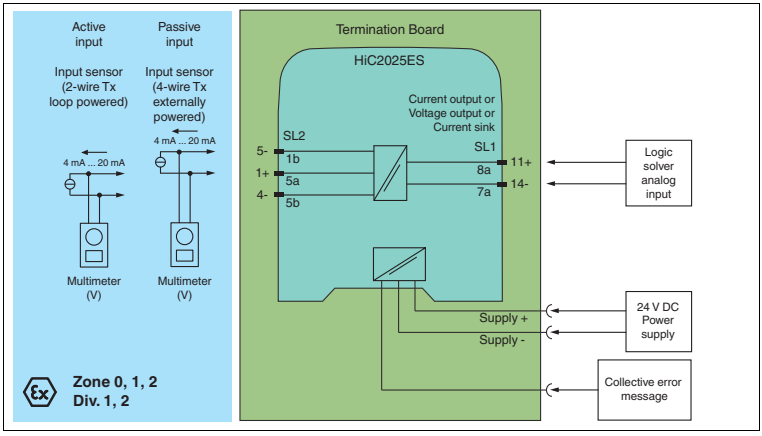

Figure 4.3 Proof test set-up for HiC2025ES

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.

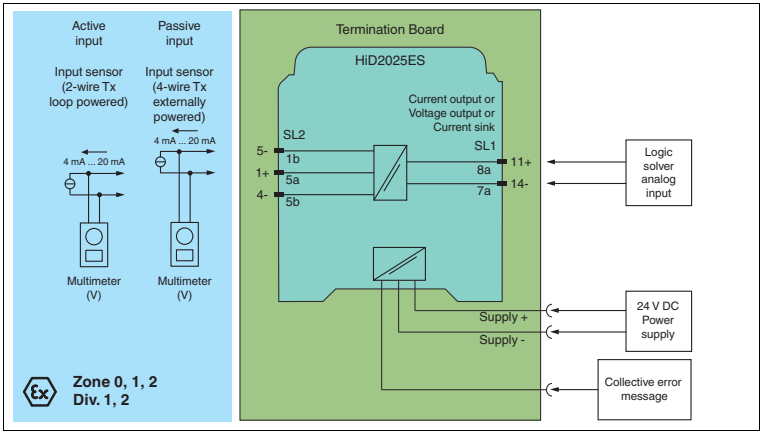

Figure 4.4 Proof test set-up for HiD2025ES

Tip

Normally the easiest way to test HiD modules is by using a stand-alone HiDTB**-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 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 When calculating the SFF this failure mode is not taken into account.
$\lambda_{not\ part}$	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
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

2015-06

2015-06

2015-06

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-2375C
06/2015