PROCESS AUTOMATION

SAFETY MANUAL SIL

SMART Transmitter Power Supply

KCD2-STC-(Ex)1.HC(.SP), HiC2025HC

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 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

The devices are available as safe area version (KCD2-STC-1.HC(.SP)) where they can be used as a signal conditioner providing isolation for non-intrinsically safe applications. Also the devices are available as hazardous area version (KCD2-STC-Ex1.HC(.SP), HiC2025HC) allowing use as isolated barriers for intrinsic safety applications.

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

It transfers the analog input signal to the safe 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.

In the KCD2-STC-(Ex)1.HC(.SP) test sockets for the connection of HART communicators are integrated into the terminals of the device.

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".

The KCD2-STC-(Ex)1.HC(.SP) is a single device for DIN rail mounting while the HiC2025HC is a plug-in device to be inserted into a specific Termination Board.

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

KCD2-STC-1.HC(.SP)
KCD2-STC-Ex1.HC(.SP)
HiC2025HC

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.

PEPPERL+FUCHS

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}.
- 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 ºC. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 ºC, 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.
- During normal operation any change of the operating function (DIP switch modification) must be prevented.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be 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 HART protocol is only used for setup, calibration, and diagnostic purposes, not during normal operation.
- The application program in the logic solver must be 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 (4 mA ... 20 mA) with a tolerance of 2 %.

Therefore the DIP switch settings used in safety relevant applications are:

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

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

Table 2.1

DIP Switch Settings HiC2025HC

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

Table 2.2

Safe State

The safe state is defined as the output reaching values < 3.6 mA/0.9 V or > 20.5 mA/5.125 V.

Reaction Time

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

2.4 Characteristic Safety Values

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	126.3 FIT
λ_{dd}	0 FIT
λ_{du}	50.3 FIT
$\lambda_{no\ effect}$	228.3 FIT
$\lambda_{total\ (safety\ function)}$	405 FIT
$\lambda_{not\ part}$	32.2 FIT
SFF	87.58 %
MTBF [1]	261 years
PFH	5.03×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	2.20×10^{-4}
PFD_{avg} for T_{proof} = 2 years	4.41×10^{-4}
PFD_{avg} for T_{proof} = 5 years	1.10×10^{-3}
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 2.3

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: input I, output I
- Non-safety relevant interfaces: none
  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 KCD2 devices provide a suitable cover to protect against accidental changes while on the HiC 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.

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. The effective life time can be higher.

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 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 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
  - 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 KCD2-STC-(Ex)1.HC(.SP) device (→ see Figure 4.1 on page 13) or for testing the HiC2025HC device (→ see Figure 4.2 on page 13). 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)	Measurement point		
		Output value (mA)	Across 2-wire Tx (V)	Across 4-wire Tx (V)
1	20.00	20.00 ± 0.4	15.1 ± 0.4	2.2 ± 1.1
2	12.00	12.00 ± 0.4	16.1 ± 0.4	2.2 ± 1.1
3	4.00	4.00 ± 0.4	17.1 ± 0.4	2.2 ± 1.1
4*	23.00	23.00 ± 0.4	14.5 ± 0.5	2.2 ± 1.1
5*	0	< 0.2	19.0 ± 1.0	n.a.
6	12.00			

* The output value shall detect a Fail High, Fail Low condition.

Table 4.1 Steps to be performed for the proof test

2012-07

PEPPERL+FUCHS

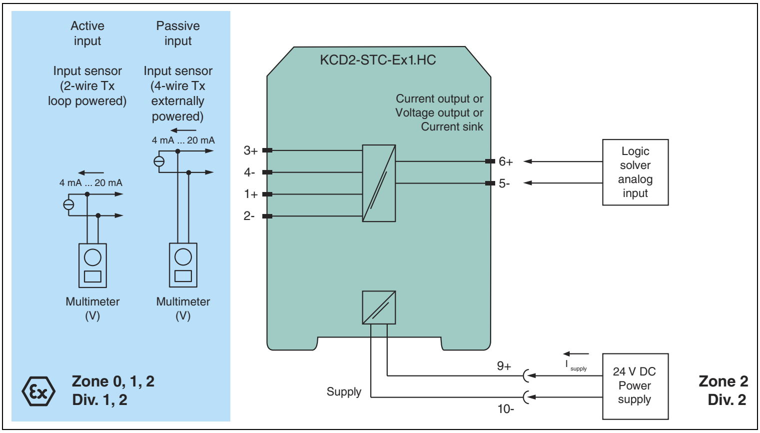

Figure 4.1 Proof test set-up KCD2-STC-(Ex)1.HC(.SP)

Usage in Zone 0, 1, 2/Div. 1, 2 only for KCD2-STC-Ex1.HC(.SP)

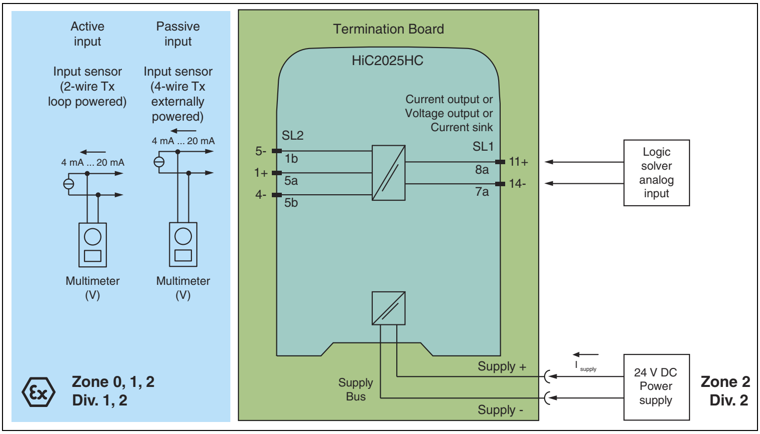

Figure 4.2 Proof test set-up for HiC2025HC

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
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
$\lambda_{\text{no effect}}$	Probability of failures of components in the safety path that have no effect on the safety function
$\lambda_{\text{not part}}$	Probability of failure of components that are not in the safety path
$\lambda_{\text{total (safety function)}}$	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

TDOCT-2750_ENG
07/2012