SAFETY MANUAL SIL

SMART Transmitter Power Supply

KFD2-STC4-(Ex)*,
KFD2-STV4-(Ex)*,
KFD2-CR4-(Ex)*

SIL
IEC 61508/61511

ISO9001

CE

SIL2
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"

2014-09

1 Introduction

1.1 General Information

This manual contains information on using the device in control circuits that are related to functional safety.

The corresponding data sheets, the operating instructions, the system description, the declaration of conformity, the EC-Type Examination Certificate, and the applicable certificates (see data sheet) are an integral part of this document.

The stated documents are available at **www.pepperl-fuchs.com** or from 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.

In the event of a device fault, the devices must be taken out of operation and measures must be taken to protect them against unintentional startup. Devices may be repaired only by the manufacturer. Deactivating or bypassing safety functions, or failing to observe the instructions in this manual (which lead to faults or affect the safety functions), can damage property and the environment or cause personal injury, for which Pepperl+Fuchs GmbH accepts no liability.

The devices have been developed, manufactured, and tested according to the applicable safety standards. The devices may be used only for the applications described in the instructions under the specified ambient conditions and exclusively in connection with the approved peripherals.

1.2 Intended Use

The isolated barriers and signal conditioners KFD2-CR4-(Ex)* and KFD2-STC4-(Ex)* provide power for 2-wire transmitters in a hazardous area. The versions without the designation "Ex" are for safe areas only. The devices transfer their analog signals to the safe area as isolated current sources. The one channel versions KFD2-CR4-(Ex)1* and KFD2-STC4-(Ex)1* can also be used with 3-wire transmitters and 2-wire current sources as inputs.

The isolated barriers and signal conditioners KFD2-STC4-(Ex)*-3 and KFD2-STC4-(Ex)*-Y* provide a current sink output while other KFD2-STC4-(Ex)* devices provide a current source output.

The isolated barriers and signal conditioners KFD2-STV4-(Ex)* provide power for 2-wire transmitters in a hazardous area. The versions without the designation "Ex" are for safe areas only. The devices transfer the analog signals to the safe area as isolated voltage sources. The one channel versions KFD2-STV4-(Ex)1* can also be used with 3-wire transmitters and 2-wire current sources as inputs.

Digital signals may be superimposed on the analog values (SMART signals) and are transferred bidirectionally (only KFD2-STC4-(Ex)* and KFD2-STV4-(Ex)*).

The devices are single devices for DIN rail mounting.

2014-09

1.3 Manufacturer Information

Pepperl+Fuchs GmbH

Lilienthalstrasse 200, 68307 Mannheim, Germany

Up to SIL2	■ KFD2-CR4-(Ex)* ■ KFD2-STC4-(Ex)* ■ KFD2-STV4-(Ex)*
Up to SIL3	■ KFD2-CR4-(Ex)1.2O* ■ KFD2-STC4-(Ex)1.2O* ■ KFD2-STV4-(Ex)1.2O*

The stars replace a combination of characters, depending on the product.

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 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.

2014-09

2.2 Assumptions

The following assumptions have been made during the FMEDA analysis:

- Only one input and one output are part of the considered safety function (only 2-channel version).
- 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 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** components with a Hardware Fault Tolerance of **0**.
- 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 °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.
- It is assumed that any safe failures that occur (e.g., output in safe condition) will be corrected within eight hours (e.g., correction of a sensor fault).
- While the device is being repaired, measures must be taken to maintain the safety function (e.g., by using a replacement device).
- The HART protocol is only used for setup, calibration, and diagnostic purposes, not during operation.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.

SIL3 application

SIL3 can be reached if the two outputs of a KFD2-***-(Ex)1.2O* device are connected to the same DCS/ESD device and evaluated if the deviation remains below 2 %.

- 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.

SIL2 application

- 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.
- 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.

2.3 Safety Function and Safe State

Safety Function

The safety function of the devices is the transfer of the analog signals from the input to the output with a tolerance of 2 %.

Device type	Input signals	Output signals
KFD2-CR4-(Ex)* and KFD2-STC4-(Ex)*	0/4 mA … 20 mA	0/4 mA ... 20 mA
KFD2-STV4-(Ex)*-1	0/4 mA … 20 mA	0/1 V … 5 V
KFD2-STV4-(Ex)*-2	0/4 mA … 20 mA	0/2 V … 10 V

Table 2.1

Safe State

The user must ensure that the ESD system reacts adequately when the outputs are:

- < 4 mA or > 20 mA for the KFD2-CR4-(Ex)* and KFD2-STC4-(Ex)*
- < 1 V or > 5 V for the KFD2-STV4-(Ex)*-1
- < 2 V or > 10 V for the KFD2-STV4-(Ex)*-2

Reaction Time

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

2014-09

Functional Safety Wiring Configuration for KFD2-***-(Ex)1.2O* Devices

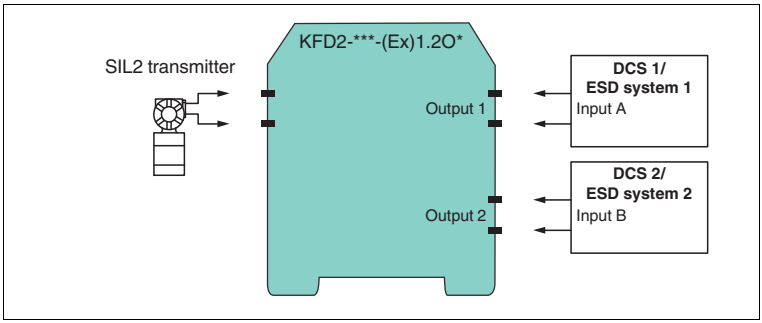

Figure 2.1 SIL2 application for KFD2-***-(Ex)1.2O* devices

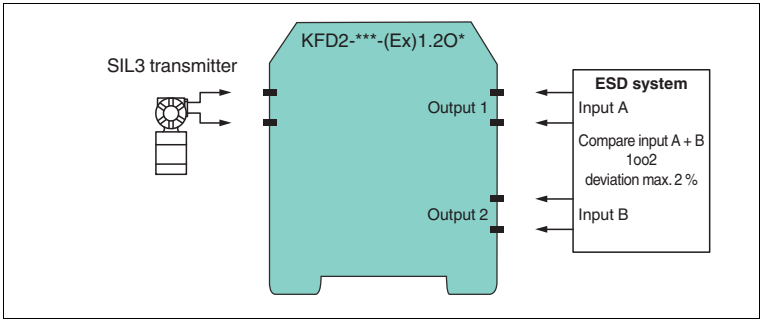

Figure 2.2 SIL3 application for KFD2-***-(Ex)1.2O* devices

2.4 Characteristic Safety Values

KFD2-CR4-(Ex)1, KFD2-STC4-(Ex)1, KFD2-STC4-(Ex)1-3, KFD2-STC4-(Ex)1-Y*, KFD2-STV4-(Ex)1-1, KFD2-STV4-(Ex)1-2

Parameters acc. to IEC 61508	Values
Assessment type	FMEDA report
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function [2]	Transfer of analog values
HFT	0
SIL	2
λ_s	192 FIT
λ_{dd} [1]	118 FIT
λ_{du}	36 FIT
$\lambda_{no\ effect}$ [2]	192 FIT
$\lambda_{not\ part}$	212 FIT
$\lambda_{total\ (safety\ function)}$	346 FIT
SFF	89 %
MTBF [3]	204 years
PFH	3.60×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.58×10^{-4}
PFD_{avg} for T_{proof} = 2 years	3.15×10^{-4}
PFD_{avg} for T_{proof} = 5 years	7.88×10^{-4}

[1] "Fail high" and "Fail low" failures are considered as dangerous detected failures λ_{dd}.

[2] "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[3] acc. to SN29500. This value includes failures which are not part of the safety function.

Table 2.2

KFD2-CR4-(Ex)1.2O, KFD2-STC4-(Ex)1.2O, KFD2-STC4-(Ex)1.2O-3, KFD2-STC4-(Ex)1.2O-Y*, KFD2-STV4-(Ex)1.2O-1, KFD2-STV4-(Ex)1.2O-2

Parameters acc. to IEC 61508	**Values**			
Assessment type	FMEDA report			
Device type	A			
Demand mode	Low Demand Mode or High Demand Mode			
Safety function [2]	Transfer of analog values			
HFT	0			
SIL			2	3
Input and output function	Input	Output	Single output used in safety function	Both outputs used in safety function
λ_s	120 FIT	144 FIT	264 FIT	670.2 FIT
λ_{dd} [1]	71.6 FIT	95.3 FIT	166.9 FIT	85.4 FIT
λ_{du}	14.4 FIT	43.8 FIT	57.2 FIT	16.6 FIT
$\lambda_{no\ effect}$ [2]	120 FIT	144.1 FIT	264 FIT	408 FIT
$\lambda_{not\ part}$	107 FIT	205 FIT	312 FIT	517 FIT
$\lambda_{total\ (safety\ function)}$	206 FIT	284 FIT	490 FIT	774 FIT
SFF			88 %	97 %
MTBF [3]			142 years	147 years
PFH [4]			5.72×10^{-8} 1/h	1.66×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year			2.50×10^{-4}	7.26×10^{-5}
PFD_{avg} for T_{proof} = 2 years			5.01×10^{-4}	1.45×10^{-4}
PFD_{avg} for T_{proof} = 5 years			1.25×10^{-3}	3.63×10^{-4}

[1] "Fail high" and "Fail low" failures are considered as dangerous detected failures λ_{dd}.

[2] "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[3] acc. to SN29500. This value includes failures which are not part of the safety function.

[4] The safety characteristic values were calculated considering a common cause factor of 5 % for the safety relevant output part. For the application with both outputs in the safety function, the ESD system needs to evaluate if the outputs differ by more than 2 %.

Table 2.3

KFD2-CR4-(Ex)2, KFD2-STC4-(Ex)2, KFD2-STC4-(Ex)2-3, KFD2-STC4-(Ex)2-Y*, KFD2-STV4-(Ex)2-1, KFD2-STV4-(Ex)2-2

Parameters acc. to IEC 61508	Values
Assessment type	FMEDA report
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety function [2]	Transfer of analog values
HFT	0
SIL	2
λ_s	165 FIT
λ_{dd} [1]	111 FIT
λ_{du}	36 FIT
$\lambda_{no\ effect}$ [2]	165 FIT
$\lambda_{not\ part}$	111 FIT
$\lambda_{total\ (safety\ function)}$	312 FIT
SFF	88 %
MTBF [3]	269 years
PFH	3.60×10^{-8} 1/h
PFD_{avg} for T_{proof} = 1 year	1.58×10^{-4}
PFD_{avg} for T_{proof} = 2 years	3.15×10^{-4}
PFD_{avg} for T_{proof} = 5 years	7.88×10^{-4}

[1] "Fail high" and "Fail low" failures are considered as dangerous detected failures λ_{dd}.

[2] "No effect" failures are not influencing the safety functions and are therefore added to the λ_s.

[3] acc. to SN29500. This value includes failures which are not part of the safety function.

Table 2.4

The characteristic safety values like PFD, PFH, 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	KFD2-CR4-(Ex)1, KFD2-STC4-(Ex)1, KFD2-STC4-(Ex)1-3, KFD2-STC4-(Ex)1-Y*, KFD2-STV4-(Ex)1-1, KFD2-STV4-(Ex)1-2
Input I, output I, output II	KFD2-CR4-(Ex)1.2O, KFD2-STC4-(Ex)1.2O, KFD2-STC4-(Ex)1.2O-3, KFD2-STC4-(Ex)1.2O-Y*, KFD2-STV4-(Ex)1.2O-1, KFD2-STV4-(Ex)1.2O-2
Input I, input II, output I, output II	KFD2-CR4-(Ex)2, KFD2-STC4-(Ex)2, KFD2-STC4-(Ex)2-3, KFD2-STC4-(Ex)2-Y*, KFD2-STV4-(Ex)2-1, KFD2-STV4-(Ex)2-2

- Non-safety relevant interfaces: none
  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 (view Figures). 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.

Proof Test for all Channels

Step No.	Set input value (mA)	Measurement point		
		Output value (mA) for STC4 and CR4 devices	Output value (V) for STV4 devices, -1 version	Output value (V) for STV4 devices, -2 version
1	20.0	20.0 ± 0.4	5.0 ± 0.1	10.0 ± 0.2
2	12.0	12.0 ± 0.4	3.0 ± 0.1	6.0 ± 0.2
3	4.0	4.0 ± 0.4	1.0 ± 0.1	2.0 ± 0.2
4	23.0	23.0 ± 0.4	5.75 ± 0.1	11.5 ± 0.2
5	0	< 0.2	< 0.1	< 0.1

Table 4.1

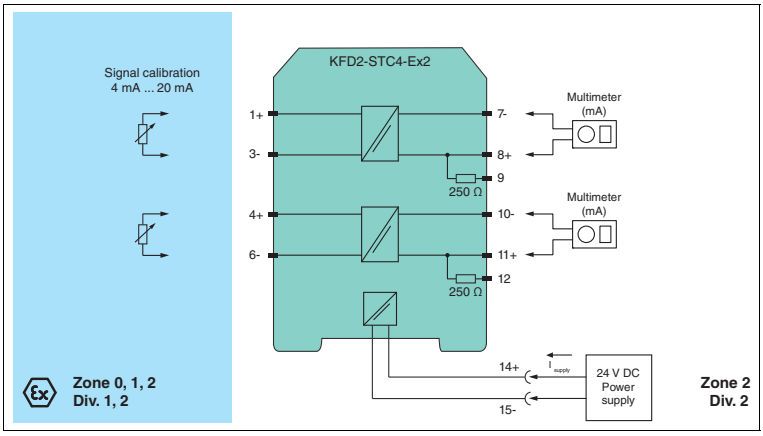

Figure 4.1 Proof test set-up for KFD2-CR4-(Ex)* and KFD2-STC4-(Ex)*

Usage in Zone 0, 1, 2/Div. 1, 2 only for Ex versions
For KCD2-CR4-(Ex)1 and KFD2-STC4-(Ex)1 do not regard the second channel.

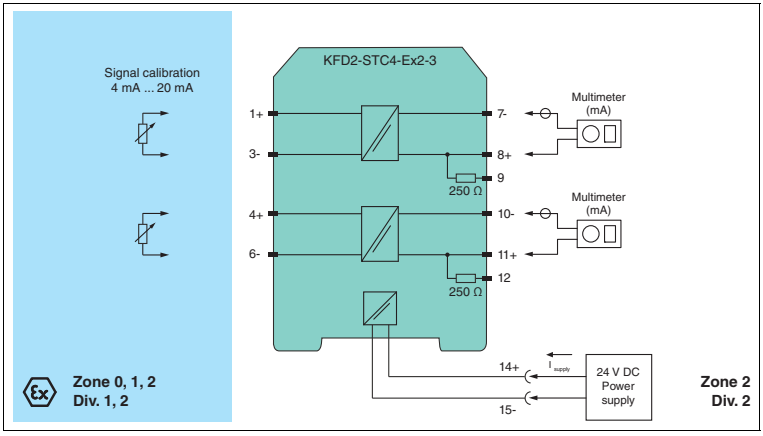

Figure 4.2 Proof test set-up for KFD2-STC4-(Ex)*-3 and KFD2-STC4-(Ex)*-Y*

Usage in Zone 0, 1, 2/Div. 1, 2 only for Ex versions
For KFD2-STC4-(Ex)1-3 and KFD2-STC4-(Ex)1-Y* do not regard the second channel.

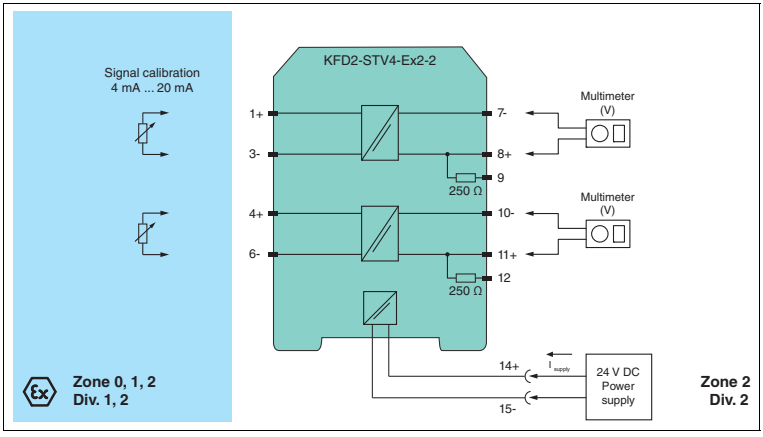

Figure 4.3 Proof test set-up for KFD2-STV4-(Ex)*-1 and KFD2-STV4-(Ex)*-2

Usage in Zone 0, 1, 2/Div. 1, 2 only for Ex versions
For KFD2-STV4-(Ex)1-1 and KFD2-STV4-(Ex)1-2 do not regard the second channel.

Proof Test for Versions with Splitter Functionality (1.2O)

Step No.	Set input value (mA)	Measurement point		
		Values for Outputs I and II (mA) for STC4 and CR4 devices	Values for Outputs I and II (V) for STV4 devices, -1 version	Values for Outputs I and II (V) for STV4 devices, -2 version
1	20.0	20.0 ± 0.4	5.0 ± 0.1	10.0 ± 0.2
2	12.0	12.0 ± 0.4	3.0 ± 0.1	6.0 ± 0.2
3	4.0	4.0 ± 0.4	1.0 ± 0.1	2.0 ± 0.2
4	23.0	23.0 ± 0.4	5.75 ± 0.1	11.5 ± 0.2
5	0	< 0.2	< 0.1	< 0.1

Table 4.2

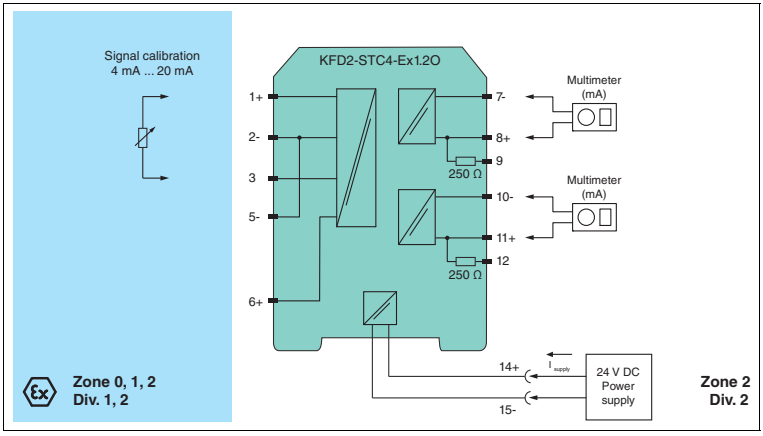

Figure 4.4 Proof test set-up for KFD2-CR4-(Ex)1.2O and KFD2-STC4-(Ex)1.2O

Usage in Zone 0, 1, 2/Div. 1, 2 only for Ex versions

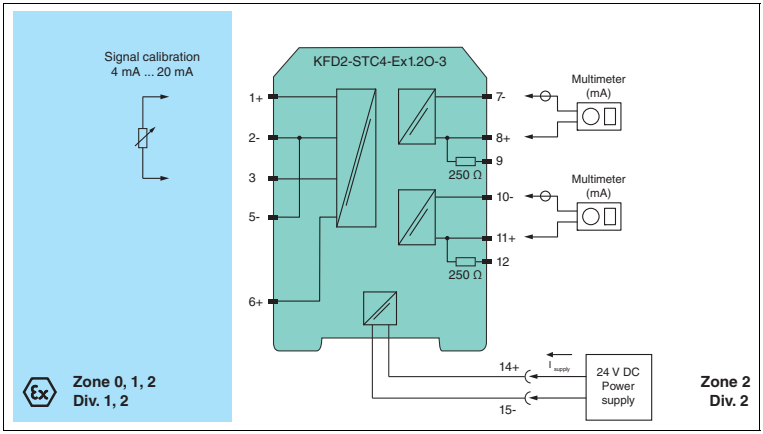

Figure 4.5 Proof test set-up for KFD2-STC4-(Ex)1.2O-3 and KFD2-STC4-(Ex)1.2O-Y*

Usage in Zone 0, 1, 2/Div. 1, 2 only for Ex versions

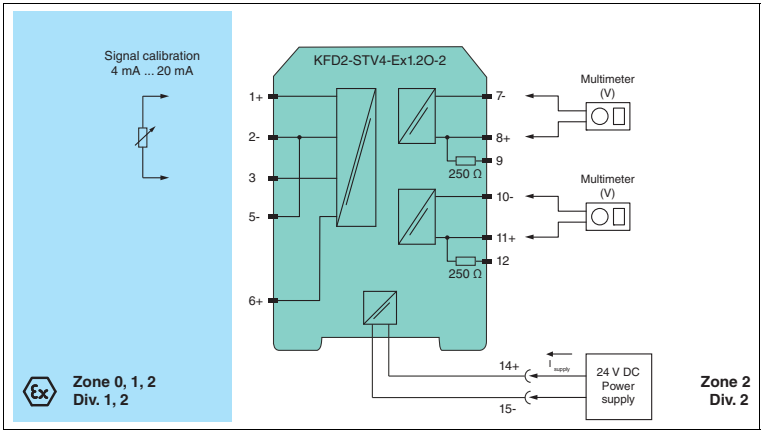

Figure 4.6 Proof test set-up for KFD2-STV4-(Ex)1.2O-1 and KFD2-STV4-(Ex)1.2O-2

Usage in Zone 0, 1, 2/Div. 1, 2 only for Ex versions

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

2014-09

2014-09

2014-09

2014-09

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-1895B
09/2014