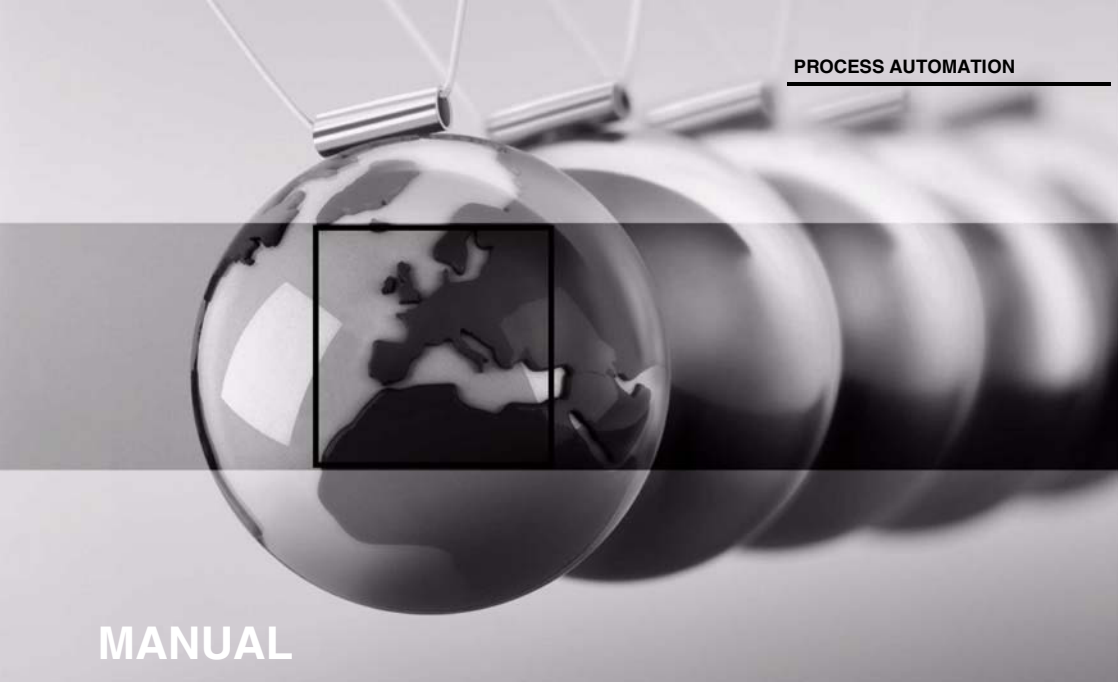

MANUAL

Functional Safety
Overspeed/Underspeed Monitor
KF**-DWB-(Ex)1.D

SIL
IEC 61508/61511

ISO9001

CE

SIL 2

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"

2016-04

1 Introduction

1.1 Contents

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:

- EC-type of examination
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- FMEDA report
- Assessment report
- Additional documents

For more information about functional safety products from Pepperl+Fuchs 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.

2 Product Description

2.1 Function

General

The device monitors an overspeed condition or an underspeed condition of the binary signal of a NAMUR sensor or mechanical contact.

The input frequency is compared to the user-defined reference frequency. The input frequency is 1 mHz to 5 kHz.

The overspeed condition or the underspeed condition is signaled via the relay contact outputs.

A fault is signalized by LEDs acc. to NAMUR NE44.

The start-up override feature sets the relay contact outputs to default conditions defined by the user for up to 1000 seconds.

The device is easily configured by the use of keypad.

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

KFA5-DWB-Ex1.D

This isolated barrier is used for intrinsic safety applications.

The input is designed for use with 2-wire sensors.

The device is supplied by a power supply of 115 V AC.

KFA6-DWB-Ex1.D

This isolated barrier is used for intrinsic safety applications.

The input is designed for use with 2-wire sensors.

The device is supplied by a power supply of 230 V AC.

KFD2-DWB-1.D

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

The input is designed for use with 2- or 3-wire sensors.

The device is supplied by a power supply of 24 V DC.

If the device is operated via Power Rail, additionally a collective error message is available.

KFD2-DWB-Ex1.D

This isolated barrier is used for intrinsic safety applications.

The input is designed for use with 2-wire sensors.

The device is supplied by a power supply of 24 V DC.

If the device is operated via Power Rail, additionally a collective error message is available.

KFU8-DWB-1.D

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

The input is designed for use with 2- or 3-wire sensors.

The device can be supplied by a power supply from 20 V DC to 90 V DC or from 48 V AC to 253 V AC.

2.2 Interfaces

The device has the following interfaces:

- Safety relevant interfaces: input, output I, output II
- Non-safety relevant interfaces:
  - Start-up override input
  - Fault indication output
  - KFD2-DWB-(Ex)1.D: collective error message output

Note!

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs GmbH Lilienthalstraße 200, 68307 Mannheim, Germany

KFA5-DWB-Ex1.D, KFA6-DWB-Ex1.D, KFD2-DWB-1.D, KFD2-DWB-Ex1.D, KFU8-DWB-1.D	Up to SIL 2

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.

2016-04

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 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/EN 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. The humidity level is within manufacturer's rating. 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 fault indication output which signals if the field circuits are broken or shorted is not considered in the FMEDA and the calculations.
- The indication of a dangerous failure (via fault bus) is detected within 1 hour by the programmable logic controller (PLC).
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures. These failures have been classified as **dangerous detected** failures.
- If you are using the device in high demand mode, observe also the useful lifetime limitations of the output relays according to the datasheet.
- The display function and the displayed values are not part of the safety function.
- The IEC/EN 61511-1 section 11.4.4 allows devices to be used in applications one SIL higher than given by table 3 of IEC/EN 61508-2, if the device is proven in use. The assessment and proven in use demonstration lead to the result that the device may be used in applications up to SIL 2. However, it is the responsibility of the end-user to decide on applying proven in use devices.

SIL 2 Application

- The device shall claim less than 15 % 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 1.5×10^{-2}, hence the maximum allowable PFD_{avg} value would then be 1.5×10^{-3}.
- For a SIL 2 application operating in high demand mode the total PFH value of the SIF should be smaller than 1.5×10^{-6} per hour, hence the maximum allowable PFH value would then be 1.5×10^{-7} per hour.
- The safety-related device is considered to be of type **B** device with a hardware fault tolerance of **0**.

2016-04

3.3 Safety Function and Safe State

Safe State

The safe state of output I and output II is the de-energized state (high impedance).

Safety Function

The safe state is achieved, when the measured frequency leaves the permissible range for the application.

Device Settings via Keypad

Function	Mode	Menu
Password protection	enabled	Service
Short circuit detection	enabled	Error
Lead breakage detection	enabled	Error

Table 3.1

Note!

For more information see the manual.

Line Fault Detection

For use in a safety function enable the line fault detection.

The input loop of all versions is supervised. The related safety function is that the outputs go to fault state (safe state) if a line fault is detected.

Note!

The collective error message output is not safety relevant.

3.4 Characteristic Safety Values

KFU8-DWB-1.D

Parameters acc. to IEC 61508	Characteristic values	
Assessment type and documentation	FMEDA and proven in use assessment	
Device type	B	
Mode of operation [1]	Low demand mode or high demand mode	Low demand mode
HFT	0	
SIL (SC)	2	
Safety function	De-energized to safe	
Fault reaction time [2]	1 s	5 min
λ_s [3]	237 FIT	236 FIT
λ_{dd}	29.6 FIT	61 FIT
λ_{du}	132 FIT	101 FIT
$\lambda_{total\ (safety\ function)}$ [3]	398 FIT	398 FIT
$\lambda_{not\ part}$	31.6 FIT	31.6 FIT
SFF [3]	66 %	74 %
MTBF [4]	177 years	178 years
PFH	1.32×10^{-7} 1/h	1.01×10^{-7} 1/h
PFD_{avg} for T_1 = 1 year	5.78×10^{-4}	4.42×10^{-4}
PFD_{avg} for T_1 = 2 years	1.16×10^{-3}	8.85×10^{-4}
PFD_{avg} for T_1 = 5 years	2.89×10^{-3}	2.21×10^{-3}
PTC	99 %	99 %
Reaction time [5]	1 s + 1/f	

Table 3.2

1 The values for a fault reaction time of 5 min benefit from internal software diagnostic functions and are therefore deemed suitable only for low demand application.

2 The fault reaction time is the delay time after discovering an internal fault by diagnostics in the device. The sampling rate is not relevant.

3 "No effect failures" are not influencing the safety function and are therefore not included in the SFF and the failure rates.

4 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h. The value is calculated for one safety function of the device.

5 For the reaction time, the delay time of the electronic circuit and the delay resulting from sampling the signals (1/f) are added.

KFD2-DWB-1.D, KFD2-DWB-Ex1.D

Parameters acc. to IEC 61508	Characteristic values	
Assessment type and documentation	FMEDA and proven in use assessment	
Device type	B	
Mode of operation [1]	Low demand mode or high demand mode	Low demand mode
HFT	0	
SIL (SC)	2	
Safety function	De-energized to safe	
Fault reaction time [2]	1 s	5 min
λ_s [3]	189 FIT	188 FIT
λ_{dd}	20.9 FIT	52 FIT
λ_{du}	138 FIT	107 FIT
$\lambda_{total\ (safety\ function)}$ [3]	347 FIT	347 FIT
$\lambda_{not\ part}$	33.0 FIT	33.0 FIT
SFF [3]	60 %	69 %
MTBF [4]	202 years	202 years
PFH	1.38×10^{-7} 1/h	1.07×10^{-7} 1/h
PFD_{avg} for T_1 = 1 year	6.04×10^{-4}	4.69×10^{-4}
PFD_{avg} for T_1 = 2 years	1.21×10^{-3}	9.37×10^{-4}
PFD_{avg} for T_1 = 5 years	3.02×10^{-3}	2.34×10^{-3}
PTC	99 %	99 %
Reaction time [5]	1 s + 1/f	

Table 3.3

[1] The values for a fault reaction time of 5 min benefit from internal software diagnostic functions and are therefore deemed suitable only for low demand application.

[2] The fault reaction time is the delay time after discovering an internal fault by diagnostics in the device. The sampling rate is not relevant.

[3] "No effect failures" are not influencing the safety function and are therefore not included in the SFF and the failure rates.

[4] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h. The value is calculated for one safety function of the device.

[5] For the reaction time, the delay time of the electronic circuit and the delay resulting from sampling the signals (1/f) are added.

KFA5-DWB-Ex1.D, KFA6-DWB-Ex1.D

Parameters acc. to IEC 61508	Characteristic values
Assessment type and documentation	FMEDA and proven in use assessment
Device type	B
Mode of operation [1]	Low demand mode
HFT	0
SIL (SC)	2
Safety function	De-energized to safe
Fault reaction time [2]	5 min
λ_s [3]	144 FIT
λ_{dd}	51 FIT
λ_{du}	123 FIT
$\lambda_{total\ (safety\ function)}$ [3]	319 FIT
$\lambda_{not\ part}$	20.4 FIT
SFF [3]	61.5 %
MTBF [4]	243 years
PFH	1.23×10^{-7} 1/h
PFD_{avg} for T_1 = 1 year	5.39×10^{-4}
PFD_{avg} for T_1 = 2 years	1.08×10^{-3}
PFD_{avg} for T_1 = 5 years	2.69×10^{-3}
PTC	99 %
Reaction time [5]	1 s + 1/f

Table 3.4

[1] The values for a fault reaction time of 5 min benefit from internal software diagnostic functions and are therefore deemed suitable only for low demand application.

[2] The fault reaction time is the delay time after discovering an internal fault by diagnostics in the device. The sampling rate is not relevant.

[3] "No effect failures" are not influencing the safety function and are therefore not included in the SFF and the failure rates.

[4] acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h. The value is calculated for one safety function of the device.

[5] For the reaction time, the delay time of the electronic circuit and the delay resulting from sampling the signals (1/f) are added.

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 ... 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 there are no components with reduced life time in the safety loop (for example electrolytic capacitors, relays, flash memories, optocoupler) which can produce dangerous undetected failures and
- 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.

Derating

For the safety application, reduce the number of switching cycles or the maximum current. A derating to 2/3 of the maximum value is adequate.

Maximum Switching Power of Output Contacts

The useful lifetime is limited by the maximum switching cycles of the relays under load conditions.

Note!

For more information see the corresponding datasheets.

4 Mounting and Installation

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 keypad. The keypad for setting the safety functions is on the front of the device.

1. Open the cover.
2. Configure the device for the required safety function via the keypad, see chapter 3.3.
3. Secure the device configuration by a password against changing.
4. Leave the parameterization mode to prevent unintentional adjustments.
5. Close the cover.
6. Check the device configuration to ensure the expected output behavior.
7. Document any changes to the device configuration.

Note!

For more information see the manual.

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.

Danger!
Danger to life from missing safety function

With enabled start-up override, dangerous faults can remain undetected. The safety function is no longer guaranteed.

Observe that the safety function is not carried out correctly while the start–up override is active. Ensure that the input of the start-up override is not accidentally brigded.

Danger!
Danger to life from missing safety function

The outputs of the device use common components. If you use these outputs in safety functions, the outputs can fail all at the same time. You cannot establish redundancy this way.

When planning a safety function, observe that these outputs can fail simultaneously due to a failure in the same component.

Danger!
Danger to life from missing safety function

If the outputs of the device are not tested regularly, the safety function is no longer guaranteed.

If you use the device in low demand mode applications, test the outputs once a year.

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

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 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.
- Frequency generator configured to deliver NAMUR signals with an accuracy of 1 %
- Power supply set to nominal voltage
- Load resistor i. e. 240 Ω, 2.5 W
- Simulate the sensor state by a potentiometer of 4.7 kΩ (threshold for normal operation), by a resistor of 220 Ω (short circuit detection) and by a resistor of 150 kΩ (lead breakage detection).

Check the settings after the configuration by suitable tests.

Proof Test Procedure for the Switching Threshold

1. Test in the proof test with the same configuration which is used in the application. Substitute the sensors by sensor simulators or calibrators.
2. If the start-up override is enabled, disable the start-up override. That means, do not bridge the input of the start-up override.
3. Test the input channel. The threshold must be between 1.4 mA and 1.9 mA. The hysteresis must be between 170 µA and 250 µA.

   ↳ For normal mode of operation the corresponding yellow LED must have lit, if the input current is above the threshold.
4. Connect a resistor R_{SC} (220 Ω) or a resistor R_{LB} (150 kΩ) to the input.

   ↳ The device must detect an external fault. This state is indicated by red LED and the relay of the corresponding output must be de-activated.
5. Attach a load and supply defined by the application's current and voltage.
6. Set back the device to the original settings for the current application after the test.
7. Leave the parameterization mode to prevent unintentional adjustments.

2016-04

Proof Test Procedure for the Relay Contact Output

1. Connect the frequency generator to terminals 1+ and 3-.
2. Set the frequency on the frequency generator 1 % below and 1 % above the defined threshold for the considered output.
   Check the hysteresis behavior and adjust the trip point accordingly.
3. Connect a digital multimeter to the output. Attach a load and supply defined by the application's current and voltage.
4. Measure the output behavior. Compare the output behavior with the intended behavior.

   ↳ If you use the pulse divider functionality, the output frequency must have a value corresponding to the configured divider ratio.

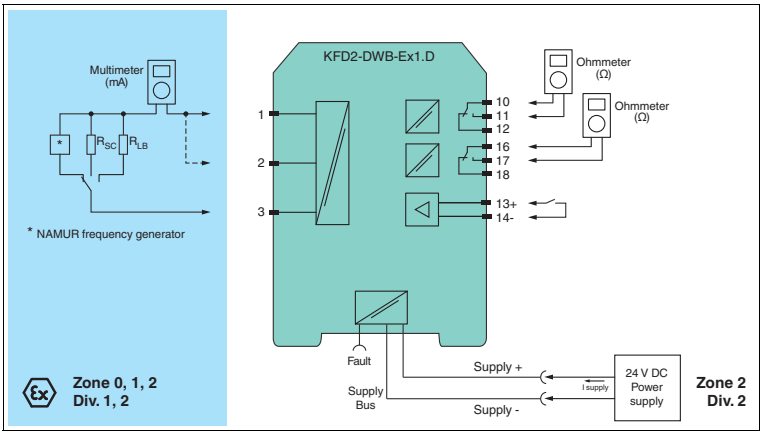

Figure 5.1 Proof test set-up for KF**-DWB-(Ex)1.D

Usage in Zone 0, 1, 2/Div. 1, 2 only for KFA5-DWB-Ex1.D, KFA6-DWB-Ex1.D, and KFD2-DWB-Ex1.D

6 Maintenance and Repair

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.

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. Ensure the proper function of the safety loop, while the device is maintained, repaired or replaced.
   If the safety loop does not work without the device, shut down the application.
   Do not restart the application without taking proper precautions.
   Secure the application against accidental restart.
3. Do not repair a defective device. A defective device must only be repaired by the manufacturer.
4. Replace a defective device only by a device of the same type.

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
$\lambda_{total\ (safety\ function)}$	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**estoration
PCS	**P**rocess **C**ontrol **S**ystem
$\mathbf{PFD}_{avg}$	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
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
$\mathbf{T}_1$	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit

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-5138
04/2016