

Functional Safety

**Transmitter Power Supply
KF**-CRG2-(Ex)1.D**

Manual

SIL

IEC 61508/61511



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"

Worldwide

Pepperl+Fuchs Group
Lilienthalstr. 200
68307 Mannheim
Germany
Phone: +49 621 776 - 0
E-mail: info@de.pepperl-fuchs.com

North American Headquarters

Pepperl+Fuchs Inc.
1600 Enterprise Parkway
Twinsburg, Ohio 44087
USA
Phone: +1 330 425-3555
E-mail: sales@us.pepperl-fuchs.com

Asia Headquarters

Pepperl+Fuchs Pte. Ltd.
P+F Building
18 Ayer Rajah Crescent
Singapore 139942
Phone: +65 6779-9091
E-mail: sales@sg.pepperl-fuchs.com
<https://www.pepperl-fuchs.com>

1	Introduction	5
1.1	Content of this Document	5
1.2	Safety Information	6
1.3	Symbols Used	7
2	Product Description	8
2.1	Function	8
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	17
5.1	Proof Test	17
6	Maintenance and Repair	20
7	List of Abbreviations	21

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.

1.2 Safety Information

Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismantling lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismantling 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 supplies 2-wire and 3-wire transmitters, and can also be used with current sources.

Two relays and an active 0/4 mA to 20 mA current source are available as outputs. The relay contacts and the current output can be integrated in safety-relevant circuits. The current output is easily scaled.

On the display the measured value can be indicated in various physical units.

The device is easily configured by the use of keypad or with the PACTware configuration software.

The input has a line fault detection.

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

KFD2-CRG2-1.D

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

The device is supplied by a voltage of 20 V DC to 30 V DC via Power Rail or terminals.

A fault is signaled by LEDs and a separate collective error message output.

KFD2-CRG2-Ex1.D

This isolated barrier is used for intrinsic safety applications.

The device is supplied by a voltage of 20 V DC to 30 V DC via Power Rail or terminals.

A fault is signaled by LEDs and a separate collective error message output.

KFU8-CRG2-1.D

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

The device is supplied by a voltage of 20 V DC to 90 V DC or 48 V AC to 253 V AC via terminals.

A fault is signaled by LEDs.

KFU8-CRG2-Ex1.D

This isolated barrier is used for intrinsic safety applications.

The device is supplied by a voltage of 20 V DC to 90 V DC or 48 V AC to 253 V AC via terminals.

A fault is signaled by LEDs.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input and output
- Non-safety relevant interfaces: collective error message output (only KFD2-CRG2-(Ex)1.D)



Note

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs Group Lilienthalstraße 200, 68307 Mannheim, Germany
--

Internet: www.pepperl-fuchs.com
--

KFD2-CRG2-1.D, KFD2-CRG2-Ex1.D, KFU8-CRG2-1.D, KFU8-CRG2-Ex1.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 2016: 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 T₁ 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.

$$\text{SFF} = (\lambda_s + \lambda_{dd}) / (\lambda_s + \lambda_{dd} + \lambda_{du})$$

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 the elements and subsystems, but not of a single device.

Nevertheless the SFF of the device is given in this document for reference.

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rate based on the Siemens standard SN 29500.
- Failure rates are constant, wear is not considered.
- External power supply failure rates are not included.
- The collective error message output is not safety relevant.
- The indication of a dangerous failure is detected within 1 hour by the programmable logic controller (PLC).
- The safety-related device is considered to be of type **B** 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.
- Since the outputs of the device use common components, these outputs must not be used in the same safety function.
- Features that extend the reaction time of the output are not considered within the specified reaction time. It is the user's responsibility to consider this time within the safety calculation.
- Observe the useful lifetime limitations of the output relays according to the datasheet.
- The device must be configured for the required safety function before the commissioning. During the operation any change of the configuration is not allowed. See chapter 4.1.1.
- The device configuration is protected by a password against changing.

Analog Output

- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.

SIL 2 Application

- To build a SIL safety loop for the defined SIL, it is assumed as an example that this device uses 10 % of the available budget for PFD_{avg}/PFH .
- The device can be used in SIL 2 applications with low demand mode according to IEC/EN 61511 table 6 with $HFT = 0$.

A prior use approach according to IEC/EN 61511 section 11.4.3 can be supported because the operating and ambient conditions of the devices are known and the devices are parameterized and not programmed.

The fact that IEC/EN 61508 requires higher SFF values for type B devices can be neglected based on the prior use approach.

3.3 Safety Function and Safe State

Safe State

Relay contact output

The safe state is present when the output is de-energized.

Current output

The safe state depends on the limit value in the respective application.

Safety Function

Relay contact output

Input values that show a peripheral fault are given as λ_{LF} . In this case the relay is set to the safe state and the failures can be counted as safe undetected.

If the current output or the collective error message output are used to detect faults, the failures may be counted as dangerous detected failures, because the state of the relay contact is triggered by a fault in the periphery or in the device.

Current output

The device transfers a current value with 5 % accuracy related to the full scale of the output.

Values below 4 mA or above 20 mA indicate a fault in the periphery or within the device and a dangerous detected failure.

Reaction Time

The combined fault detection and fault reaction time is the time in which the device reacts to an occurred fault.

The reaction time for all safety functions is < 1 s.

Note

See corresponding datasheets for further information.



3.4 Characteristic Safety Values

Parameters	Characteristic values			
	Relay contact output		Current output	
	KFD2-CRG2-(Ex)1.D	KFU8-CRG2-(Ex)1.D	KFD2-CRG2-(Ex)1.D	KFU8-CRG2-(Ex)1.D
Assessment type	FMEDA report with proven in use/prior use assessment ¹			
Device type	B			
Mode of operation	Low demand mode or high demand mode			
HFT	0			
SIL	2			
SC	2			
Safety function	Digital output		Analog output	
λ_{su}	165 FIT	213 FIT	137 FIT	177 FIT
λ_{dd}	–	–	74 FIT	83 FIT
λ_{LF}^2	70 FIT	79 FIT		
λ_{du}	114 FIT	108 FIT	90 FIT	81 FIT
$\lambda_{no\ effect}$	164 FIT	194 FIT	151 FIT	178 FIT
$\lambda_{no\ part}$	35.8 FIT	34.4 FIT	35.0 FIT	34.8 FIT
λ_{total} (safety function)	348 FIT	399 FIT	300 FIT	341 FIT
λ_{total} (signal path)	548 FIT	628 FIT	486 FIT	554 FIT
SFF ³	67 %	72 %	70 %	76 %
MTBF ⁴	207 years	181 years	234 years	206 years
PFH ¹	1.13×10^{-7} 1/h ⁵	1.08×10^{-7} 1/h ⁴	9.00×10^{-8} 1/h	8.10×10^{-8} 1/h
PFD _{avg} for T ₁ = 1 year	4.96×10^{-4} 1/h	4.75×10^{-4} 1/h	3.94×10^{-4} 1/h	3.56×10^{-4} 1/h
PFD _{avg} for T ₁ = 2 years	9.92×10^{-4} 1/h	9.50×10^{-4} 1/h	7.88×10^{-4} 1/h	7.12×10^{-4} 1/h
PFD _{avg} for T ₁ = 5 years	2.48×10^{-3} 1/h ⁴	2.37×10^{-3} 1/h ⁴	1.97×10^{-3} 1/h ³	1.78×10^{-3} 1/h ³
PTC	99 %			
Reaction time ⁶	< 1 s			

Table 3.1

- ¹ For the proven in use/prior use demonstration, sales figures, customer returns and questionnaires filled out by customers were used which show that no unknown systematic faults are expected. The device is based on a former device that was evaluated for a proven-in-use statement by exida.com GmbH.
- ² These failures can be counted as dangerous detected failures or as safe failures depending on the application, see chapter 3.3.
- ³ For the calculation of the values acc. to IEC/EN 61508:2010, the "no effect" values are excluded from the SFF calculation.
- ⁴ acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.
- ⁵ For using this proof test interval for the safety application, the usage of more than 10 % of the failure rate for the safety loop is necessary.
- ⁶ Time between fault occurrence and fault reaction



Note

The characteristic values apply to all modes of operation that can be set on the device.

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, 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.

The estimated useful lifetime is greater than the warranty period prescribed by law or the manufacturer's guarantee period. However, this does not result in an extension of the warranty or guarantee services. Failure to reach the estimated useful lifetime is not a material defect.

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.

For requirements regarding the connected output load, refer to the documentation of the connected peripheral devices.

Note

See corresponding datasheets for further information.



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 Device via Keypad

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 4.1.1.
3. Activate the password protection in the device to prevent unauthorized or accidental changes to the configuration.
4. Leave the parameterization mode to prevent unintentional adjustments.
5. Close the cover.
6. Check the device to ensure that the expected safety function is guaranteed.
7. Document any changes to the device configuration.



Configuring the Device via PACTware Operating Software

The device can also be configured via the PACTware operating software. The interface for connecting a personal computer for configuring is on the front of the device.

1. Open the cover.
2. Connect a personal computer via the K-ADP-USB adapter to the device.
3. Configure the device for the required safety function via the PACTware operating software, see chapter 4.1.1.
4. Protect the device configuration by a password against changing.
5. Leave the parameterization mode to prevent unintentional adjustments.
6. Disconnect the personal computer from the device.
7. Close the cover.
8. Check the device to ensure that the expected safety function is guaranteed.
9. Document any changes to the device configuration.



Note

For more information see the manual.

4.1.1 Configuration for Use in Safety Function



Configuring the Device for Use in Safety Function

1. Configure the device for the required safety function via the keypad or the operating software.
2. Enable the short circuit (SC) detection and lead breakage (LB) detection.
3. If using the current output:
 - Set the characteristic of the current output to the **4 mA to 20 mA NE 43** mode.
 - Set the parameter **Fault current** to **Up/Down, Up or Down**. Ensure that the PLC reacts adequately on a detected line fault.
 - The parameter **Smoothing** can delay the safe reaction. Choose the appropriate setting for your application.
4. If using the relay contact output:
 - Set the parameter **Mode** (operating behavior) to **Passive**.
If inverted reaction is necessary, use the normally closed contact. Ensure in this case
 - that the normally closed contact is properly connected and
 - that all precautions have been taken which are necessary for an energized-to-safe function.
 - The parameter **Delay** delays the safe reaction. Choose the appropriate setting for your application.
5. Activate the password protection in the device to prevent unauthorized or accidental changes to the 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.



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

This section describes a possible proof test procedure. The user is not obliged to use this proposal. The user may consider different concepts with an individual determination of the respective effectiveness, e. g. concepts according to NA106:2018.

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.
- Power supply set to nominal voltage
- Load resistor i. e. 220 Ω , 150 mW
- Simulate the sensor state by a NAMUR sensor simulator for 4 mA to 20 mA signals. This simulator must also be capable to signal faults (i. e. with 0.3 mA or 22.5 mA).



Proof Test Procedure

1. Connect a digital multimeter and the load defined by the application to terminals 7- and 8+.
2. Set the input current to 4 mA, 12 mA, and 20 mA, depending on the used configuration. Measure the output current and the relay function.
 - ↳ The proof test for the current output is passed if the measured output values are:
 - for 4 mA application: 3.9 mA to 4.1 mA
 - for 12 mA application: 11.9 mA to 12.1 mA
 - for 20 mA application: 19.9 mA to 20.1 mA
3. Set the input current to 20 mA. Measure the input voltage on terminals 1+ and 3-.
 - ↳ The proof test for the current output is passed if the measured input voltage is ≥ 15 V. The proof test for the relay contact output is given for the normally closed contact.
4. If the line fault detection is activated, remove the current source on terminals 1+ and 3-.
 - ↳ The red LED flashes. The relay is in the high-impedance state.
5. Test the circuit diagnosis by simulating 2.0 mA on the input if a Max alarm is configured and 21.5 mA if a Min alarm is configured.
 - ↳ The red LED is off. The relay is in the low impedance state. The output current is between 3.7 mA and 3.9 mA or between 20.4 mA and 20.6 mA depending on the selected operating behavior.
6. Test the circuit diagnosis by simulating 0.15 mA on the input if a Max alarm is configured and 22.5 mA if a Min alarm is configured.
 - ↳ The red LED flashes. The relay is in the high impedance state. The output current is between 1.9 mA and 2.1 mA or between 21.4 mA and 21.6 mA depending on the selected operating behavior.
7. Set back the device to the original settings for the current application after the test.

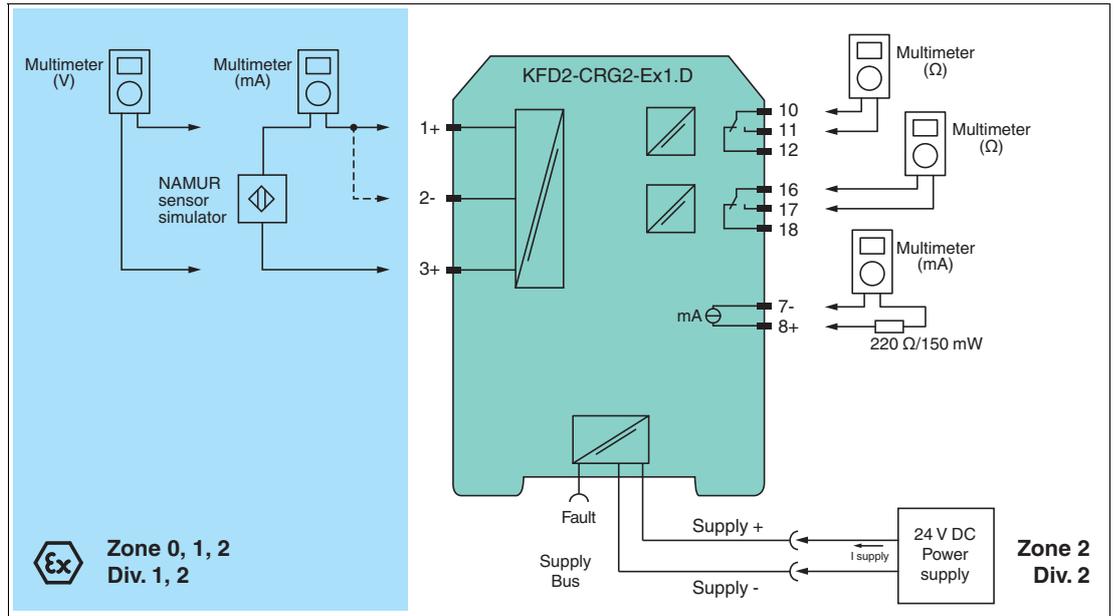


Figure 5.1 Proof test set-up for KF**-CRG2-(Ex)1.D

Usage in Zone 0, 1, 2/Div. 1, 2 only for KFD2-CRG2-Ex1.D or KFU8-CRG2-Ex1.D

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	Emergency Shutdown
FIT	Failure In Time in 10^{-9} 1/h
FMEDA	Failure Mode, Effects, and Diagnostics Analysis
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.
$\lambda_{not\ part}$	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	Hardware Fault Tolerance
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restoration
PCS	Process Control System
PFD_{avg}	Average Probability of dangerous Failure on Demand
PFH	Average frequency of dangerous failure per hour
PLC	Programmable Logic Controller
PTC	Proof Test Coverage
SC	Systematic Capability
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
T₁	Proof Test Interval

Your automation, our passion.

Explosion Protection

- Intrinsic Safety Barriers
- Signal Conditioners
- FieldConnex® Fieldbus
- Remote I/O Systems
- Electrical Ex Equipment
- Purge and Pressurization
- Industrial HMI
- Mobile Computing and Communications
- HART Interface Solutions
- Surge Protection
- Wireless Solutions
- Level Measurement

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

Pepperl+Fuchs Quality

Download our latest policy here:

www.pepperl-fuchs.com/quality

