Functional Safety

Multifunction Terminal MFT-***.****(.L)

Manual

SIL

IEC 61508/61511

ISO9001

CE SIL 3

Your automation, our passion.

PEPPERL+FUCHS

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

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.

Note

For specific device information such as the year of construction, scan the QR code on the device. As an alternative, enter the serial number in the serial number search 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.

DOCT-6782A 2024-04

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

Danger!

Danger to life from wrong usage of the device

The protection of the safety loop is **not the safety function** of the device.

The statement concerning the safety function of the device solely describes the effect on safety loops in which the device is installed. The device acts in the safety loops as a simple pass through element.

The device provides the galvanic isolation between field side and control side.

The device consists of a base module and a plug-in module. The base module is mounted on a DIN mounting rail. The plug-in module is connected to the base module.

The plug-in module is available in different versions that differ in their function.

Note

See corresponding datasheets for further information.

Typical applications for the multifunction terminal are:

- Fusing Ex d valves, signal lamps, acoustic sensors
- Diode decoupling of supply circuits
- Simple OR gate for Zone 1 mounting
- Visible disconnect of field devices
- Relay switch for power circuits
- Current limitation using resistors
- Optocoupler applications

2.2 Interfaces

The device has the following safety relevant interfaces.

- Field side terminals
- Control side terminals

Note

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs Group Lilienthalstraße 200, 68307 Mannheim, Germany
Internet: www.pepperl-fuchs.com

Multifunction Terminal MFT-R.****, MFT-2R.****, MFT-D****(.L), MFT-2D.****, MFT-F.****(.L), MFT-2F.****, MFT-2L.****, MFT-FT.****, MFT-RNO.****, MFT-RNC.****, MFT-BASE.*P	Up to SIL 3

The *-marked letters of the type code are placeholders for versions of the device.

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 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.

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 control loop has a hardware fault tolerance of **0** and it is a type **A** device.
- 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.

Application

The multifunction terminal and the connected device (transmitter, isolator or actuator) have to be considered in combination. The PFD_{avg}/PFH budget of the device categories in the entire safety loop is:

- Actuator (valve) 40 %
- Transmitter (sensor) 25 %
- Isolator 10 %

As an overview for the SIL2 or SIL3 safety loop this means:

Device category	SIL2		SIL3	
	PFH	PFD_{avg}	PFH	PFD_{avg}
Total	10^{-6} 1/h	10^{-2}	10^{-7} 1/h	10^{-3}
Actuator (40 %)	4 x 10^{-7} 1/h	4 x 10^{-3}	4 x 10^{-8} 1/h	4 x 10^{-4}
Transmitter (25 %)	2.5 x 10^{-7} 1/h	2.5 x 10^{-3}	2.5 x 10^{-8} 1/h	2.5 x 10^{-4}
Isolator (10 %)	10^{-7} 1/h	10^{-3}	10^{-8} 1/h	10^{-4}

Table 3.1 Overview PFD_{avg}/PFH budget

3.3 Safety Function and Safe State

The device transfers signals from the field side to the control side or vice versa.
The transferred signals are evaluated as:

- analog input (AI)
- analog output (AO)
- digital input (DI)
- digital output (DO)

The digital communication is checked for any corruption of the bit-by-bit communication.

Observe the PFH/PFD_{avg} values in the functional safety manual and the specified calculation rules. The devices fulfil the requirements for SIL 3 and can be used to pass safety relevant signals through in applications up to SIL 3.

Safe State

Signal type	Safe state
Analog signal (AI, AO)	The safe state is defined as the device interrupting the signal (output current < 4 mA). The probability is zero that the signal suddenly rises above what the input provides.
Digital signal (DI, DO)	The safe state is defined as the device interrupting the signal (output current = 0 mA, output voltage = 0 V).

Table 3.2

Safety Function

For evaluating safety values, the assumption was made that the device transfers signals from one terminal to the other terminal.

In automation, signals are generally evaluated as digital and analog inputs and outputs (DI, DO, AI, AO). In one case, digital communication was evaluated separately for any corruption of the bit-by-bit communication. It is assumed that the safety function ensures correct bus communication and that there is no dangerous deviation in the communication signal.

Reaction Time

The reaction time is < 10 ms.

The reaction time depends on the application. Where in doubt, measure the reaction time in the safety loop.

Note

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

1oo1 Structure

Parameters	Characteristic values			
Assessment type and documentation	FMEDA report			
Device type	A			
Mode of operation	Low demand mode or high demand mode			
Safety function	Pass through the signal			
HFT	0			
SIL	3			
Signal type	Analog signal (AI, AO) or digital signal (DI, DO)			
Device version	MFT-R.****	MFT-2R.****	MFT-D.1000	MFT-D.1000.L
λ_s	0.97 FIT	1.94 FIT	1.15 FIT	2.00 FIT
λ_{dd}	0 FIT	0 FIT	0 FIT	0 FIT
λ_{du}	0.06 FIT	0.12 FIT	0.50 FIT	0.50 FIT
$\lambda_{no\ effect}$	0.02 FIT	0.04 FIT	0.20 FIT	0.20 FIT
$\lambda_{total\ (safety\ function)}$	1.03 FIT	2.06 FIT	1.65 FIT	2.50 FIT
MTBF [1]	90599 years	45300 years	55415 years	36588 years
PFH	6.00×10^{-11} 1/h	1.20×10^{-10} 1/h	5.00×10^{-10} 1/h	5.00×10^{-10} 1/h
PFD_{avg} for T_1 = 1 year	2.63×10^{-7}	5.26×10^{-7}	2.19×10^{-6}	2.19×10^{-6}
PFD_{avg} for T_1 = 2 years	5.26×10^{-7}	1.05×10^{-6}	4.38×10^{-6}	4.38×10^{-6}
PFD_{avg} for T_1 = 5 years	1.31×10^{-6}	2.63×10^{-6}	1.10×10^{-5}	1.10×10^{-5}
Reaction time [2]	< 10 ms			

Table 3.3

1 acc. to SN 29500. This value includes failures which are not part of the safety function/MTTR = 8 h.
2 Time between fault detection and fault reaction

DOCT-6782A 2024-04

Parameters	Characteristic values			
Assessment type and documentation	FMEDA report			
Device type	A			
Mode of operation	Low demand mode or high demand mode			
Safety function	Pass through the signal			
HFT	0			
SIL	3			
Signal type	Analog signal (AI, AO) or digital signal (DI, DO)			
Device version	MFT-2D.0500	MFT-F.****	MFT-F.****.L	MFT-2F.****
λ_s	2.30 FIT	3.35 FIT	4.60 FIT	6.70 FIT
λ_{dd}	0 FIT	0 FIT	0 FIT	0 FIT
λ_{du}	1.00 FIT	0 FIT	0 FIT	0 FIT
$\lambda_{no\ effect}$	0.40 FIT	22.5 FIT	22.6 FIT	45.0 FIT
$\lambda_{total\ (safety\ function)}$	3.30 FIT	3.35 FIT	4.60 FIT	6.70 FIT
MTBF [1]	27708 years	4380 years	4133 years	2190 years
PFH	1.00×10^{-9} 1/h	0 1/h	0 1/h	0 1/h
PFD_{avg} for T_1 = 1 year	4.38×10^{-6}	0	0	0
PFD_{avg} for T_1 = 2 years	8.76×10^{-6}	0	0	0
PFD_{avg} for T_1 = 5 years	2.19×10^{-5}	0	0	0
Reaction time [2]	< 10 ms			

Table 3.4

1 acc. to SN 29500. This value includes failures which are not part of the safety function/MTTR = 8 h.
2 Time between fault detection and fault reaction

Parameters	Characteristic values			
Assessment type and documentation	FMEDA report			
Device type	A			
Mode of operation	Low demand mode or high demand mode			
Safety function	Pass through the signal			
HFT	0			
SIL	3			
Signal type	Analog signal (AI, AO) or digital signal (DI, DO)			
Device version	MFT-2L.****	MFT-RNC-0006	MFT-RNO-0006	MFT-FT.0001
λ_s	2.50 FIT	41.2 FIT	42.8 FIT	2.34 FIT
λ_{dd}	0 FIT	0 FIT	0 FIT	0 FIT
λ_{du}	0 FIT	57 FIT	55 FIT	0.60 FIT
$\lambda_{\text{no effect}}$	0.20 FIT	1.78 FIT	1.78 FIT	0.36 FIT
$\lambda_{\text{total (safety function)}}$	2.50 FIT	98 FIT	98 FIT	2.94 FIT
MTBF [1]	36588 years	1035 years	1035 years	30687 years
PFH	0 1/h	5.67×10^{-8} 1/h	5.51×10^{-8} 1/h	6.00×10^{-10} 1/h
PFD_{avg} for T_1 = 1 year	0	2.48×10^{-4}	2.41×10^{-4}	2.63×10^{-6}
PFD_{avg} for T_1 = 2 years	0	4.97×10^{-4}	4.83×10^{-4}	5.26×10^{-6}
PFD_{avg} for T_1 = 5 years	0	1.24×10^{-3}	1.21×10^{-3}	1.31×10^{-5}
Reaction time [2]	< 10 ms			

Table 3.5

1 acc. to SN 29500. This value includes failures which are not part of the safety function/MTTR = 8 h.
2 Time between fault detection and fault reaction

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.

The standard EN/ISO 13849-1:2015 proposes a useful lifetime T_M of 20 years for devices used within industrial environments. As the devices do not contain any critical components, this useful lifetime may be assumed under the following conditions:

- no high temperatures resp. no temperature changes
- no permanently high humidity
- no strong and continuous vibrations

For devices containing relays, observe the maximum switching cycles specified in the datasheets. For safety applications, reduce the number of switching cycles to up to 2/3 of the maximum value.

A useful lifetime of 15 years is assumed for devices containing optical isolators, as the brightness of the LEDs decreases during their useful lifetime.

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

Observe that the useful lifetime refers to the (constant) failure rate of the device. The effective life time can deviate from this.

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.

DOCT-6782A 2024-04

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 Mounting

Mounting and Grounding the Device

1. Mount the device on a 35 mm x 7.5 mm DIN mounting rail according to EN 60715.
2. Ground the device via the DIN mounting rail.

4.2 Configuration

A configuration of the device is not necessary and not possible.

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

Many backplanes have DIP switches that can be used to bypass the output shutdown. If the output shutdown is put out of service, the safety function is no longer guaranteed.

Prevent the access to the DIP switches and the manipulation of the output shutdown during operation. Use the Pepperl+Fuchs switch protection cover as described in the documentation.

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

A proof test is not defined. If a proof test is required for the application, the simplicity of the device makes it easy for the user to define a proof test.

DOCT-6782A 2024-04

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.

Reporting Device Failure

If you use the device in a safety loop according to IEC/EN 61508, it is required to inform the device manufacturer about possible systematic failures.

Report all failures in the safety function that are due to functional limitations or a loss of device function – especially in the case of possible dangerous failures.

In these cases, contact your local sales partner or the Pepperl+Fuchs technical sales support (service line).

It is not necessary to report failures in the safety function that are due to external influences or damage.

7 Application Examples

This chapter shows how to integrate a multifunction terminal into a safety loop.

Integration of a Multifunction Terminal into a Safety Loop

To define and calculate the safety relevant values for a safety loop, you have to determine the following basic parameters first:

1. Signal characteristic of the safety loop: analog or digital,
2. Signal direction of the safety loop as seen from the perspective of the safety-related programmable logic controller (SPLC): input or output,
3. Safe state of the field device allocated to the multifunction terminal,
4. Mode of operation: low demand mode, high demand mode or continuous mode
5. Required SIL level of the safety loop.

After the safety loop is defined, assign a multifunction terminal to the field device. Create a basic overview as shown below.

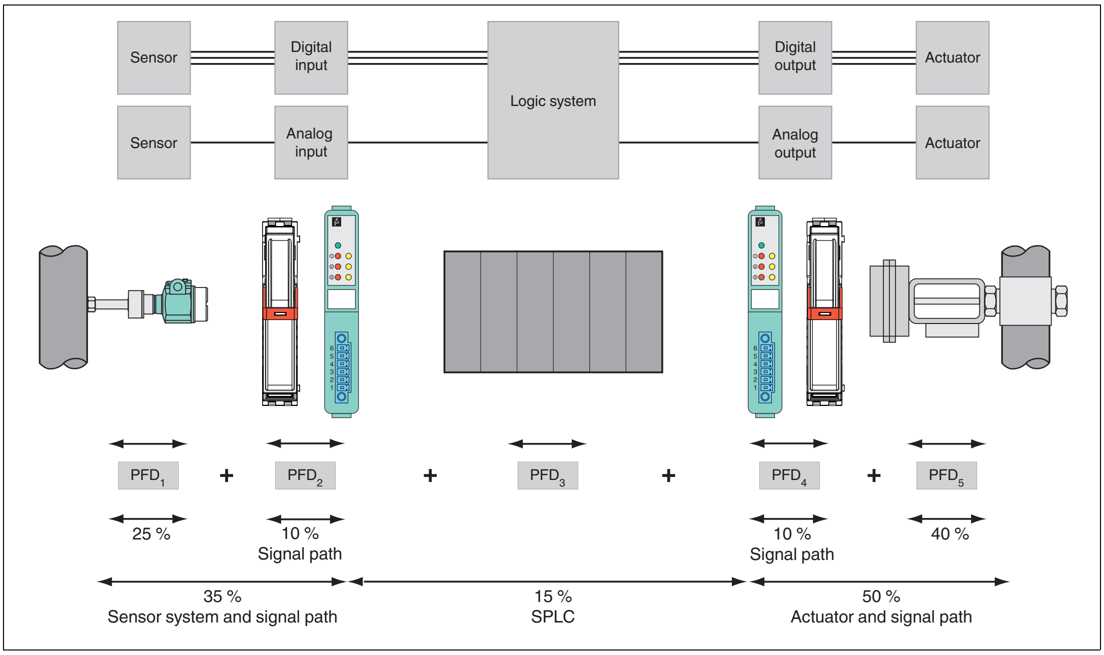

Figure 7.1 Example of a complete safety loop with assigned multifunction terminals

In principle, the failure rates of the multifunction terminals have to be added to the failure rates of the field device or the safety-related programmable logic controller (SPLC). By doing so, it is assumed that the multifunction terminal is a part of this device. Verify with these new values if the necessary SIL level can be achieved.

DOCT-6782A 2024-04

8 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.
$\lambda_{not\ part}$	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	**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
PFD_{avg}	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure per hour
PLC	**P**rogrammable **L**ogic **C**ontroller
PTC	**P**roof **T**est **C**overage
SC	**S**ystematic **C**apability
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIS	**S**afety **I**nstrumented **S**ystem
T_1	Proof Test Interval
FLT	Fault
LB	**L**ead **B**reakage
LFD	**L**ine **F**ault **D**etection
SC	**S**hort **C**ircuit
$T_{service}$	Time from start of operation to putting the device out of service

DOCT-6782A 2024-04

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

PEPPERL+FUCHS

www.pepperl-fuchs.com

DOCT-6782A / 2024-04