MANUAL

Functional Safety

Voltage Repeater
KFD2-VR4-Ex1.26

SIL
IEC 61508/61511

ISO9001

CE

SIL 2

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"

2018-03

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.

2018-03

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.

2018-03

2 Product Description

2.1 Function

This isolated barrier is used for intrinsic safety applications.

It provides a floating output to power a vibration sensor (e. g. Bently Nevada) or an acceleration sensor in a hazardous area and transfers the voltage signal from that sensor to the non-hazardous area.

The device is designed to provide the power supply to the vibration sensors. Depending on connection the barrier provides 3.6 mA, 5.3 mA, or 8.9 mA supply current for 2-wire sensors, or 18 V at 20 mA for 3-wire sensors.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: input, output
- Non-safety relevant interfaces: power supply

Note!

For corresponding connections see datasheet.

2.3 Marking

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

KFD2-VR4-Ex1.26	Up to SIL 2

2.4 Standards and Directives for Functional Safety

Device-specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 2, edition 2000: 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.

2018-03

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- 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.
- 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 1×10^{-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 1×10^{-6} per hour, hence the maximum allowable PFH value would then be 1.5×10^{-7} per hour.
- Since the safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 60 % according to table 2 of IEC/EN 61508-2 for a SIL 2 (sub) system.
- Failure rate based on the Siemens standard SN29500.
- Any safe failures that occur (e. g. output in safe state) will be corrected within 8 hours (e. g. remove sensor fault).
- While the device is being repaired, measures must be taken to maintain the safety function (e. g. substitution by a replacement device).
- Propagation of failures is not relevant.
- There is no signalization of dangerous failures available at the output of the device. Therefore any fault detection by external safety devices is not assumed.

3.3 Safety Function and Safe State

Safety Function

The safety function of the device is fulfilled, as long as the output repeats the input voltage (0 V ... -20 V) with a tolerance of ±2 %.

Safe State

The safe state is defined, as the output being de-energized.

Reaction Time

The time that is needed to transfer a signal from the input of the device to the output according to the safety function.

Note!

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

Parameters	Characteristic values
Assessment type	FMEDA report
Device type	A (only hardware)
Mode of protection	Low demand mode or high demand mode
HFT	0
SIL (hardware)	2
$\lambda_{sd} + \lambda_{su}$ [1]	338 FIT
λ_{dd}	0 FIT
λ_{du}	103 FIT
$\lambda_{total\ (safety\ function)}$	477 FIT
$\lambda_{not\ part}$	35.1 FIT
SFF	76 %
PTC	100 %
MTBF [2]	239 years
PFH	1.03×10^{-7} 1/h
PFD_{avg} for T_1 = 1 year	4.52×10^{-4}
PFD_{avg} for T_1 = 3 years	9.03×10^{-3}
PFD_{avg} for T_1 = 5 years	2.26×10^{-3}
Reaction time [3]	12.5 µs

Table 3.1

1 Failures in components that are part of the safety function but do not influence the safety function are regarded as safe undetected.
2 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h.
3 The time that is needed to transfer a signal from the input of the device to the output according to the safety function.

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 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.

2018-03

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

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

2018-03

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

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 possible that the device is used under other circumstances than specified within the assumptions for the FMEDA assessment. The calculations for the safety loop can also reveal that the device can claim a different amount of the PFD value (standard is 15 %). Both effects can have an influence on the proof test interval.

The proof test detects dangerous undetected failures that can affect the safety function of the plant.

It is under the responsibility of the plant operator to define the type of proof test and the proof test interval. Do not exceed the proof test interval of a maximum of 3 years.

The following sections describe the steps of the proof test. The proof test reveals almost all 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.
- Apparatus suitable for generating the signals for test B.
- Load of 2.1 kΩ and 1.8 kΩ for the input, 10 kΩ for the output.

2018-03

Proof Test Procedure A

1. Prepare the test set-up, see next figure.
2. Connect an input load of 2.1 kΩ to terminals 4+ and 5-.
3. Connect an output load of 10 kΩ to terminals 7- and 8+.
4. Connect the power supply to terminals 11+ and 12- or via Power Rail.
5. Connect a voltage source to terminals 4 (common) and 2 (input).
6. Apply voltages of -5 V, -10 V. -20 V at the input.
7. Measure the output voltage.

   ↳ The output voltage must be within ± 200 mV.
8. Disconnect the ancillary equipment.
9. Set back the device to the original settings after the test.
10. Restore the safety loop.

Input voltage	Output voltage
-5 V	-5 V ± 200 mV
-10 V	-10 V ± 200 mV
-20 V	-20 V ± 200 mV

Table 5.1

Proof Test Procedure B

1. Prepare the test set-up, see next figure.
2. Connect an input load of 2.1 kΩ to terminals 4+ and 5-.
3. Connect an output load of 10 kΩ to terminals 7- and 8+.
4. Connect the power supply to terminals 11+ and 12- or via Power Rail.
5. Apply a voltage of -2 V DC + 1.414 V_{rms} sine wave at 20 kHz at the input.
6. Measure the amplitude of the sine wave at input and output.

   ↳ The output voltage amplitude must be at least 0.891 times the input voltage amplitude (i. e. the reduction in amplitude must not exceed 1 dB).
7. Disconnect the ancillary equipment.
8. Set back the device to the original settings after the test.
9. Restore the safety loop.

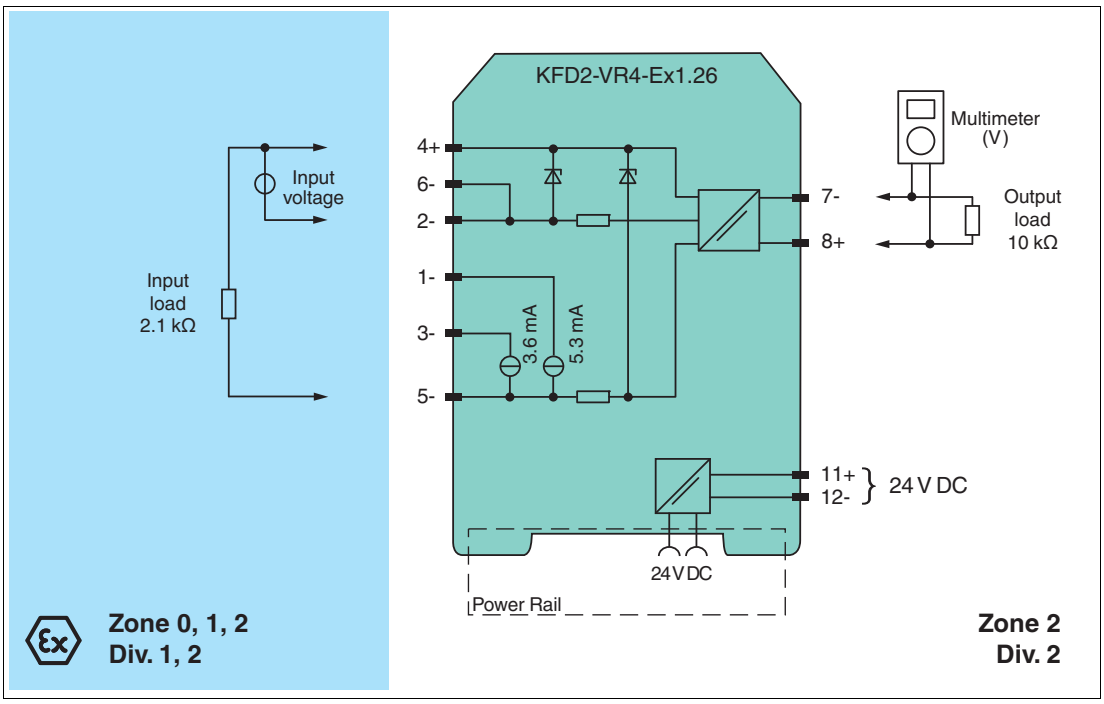


Figure 5.1 Set-up for proof tests A and B

2018-03

Proof Test Procedure C

1. Prepare the test set-up, see figure below.
2. Connect an input load of 1.8 kΩ to terminals 1- and 4+.
3. Measure the voltage load across the resistor and the current derived from it.
   ↳ The current value must be between 4.9 mA and 5.7 mA.
4. Disconnect the ancillary equipment.
5. Set back the device to the original settings after the test.
6. Restore the safety loop.

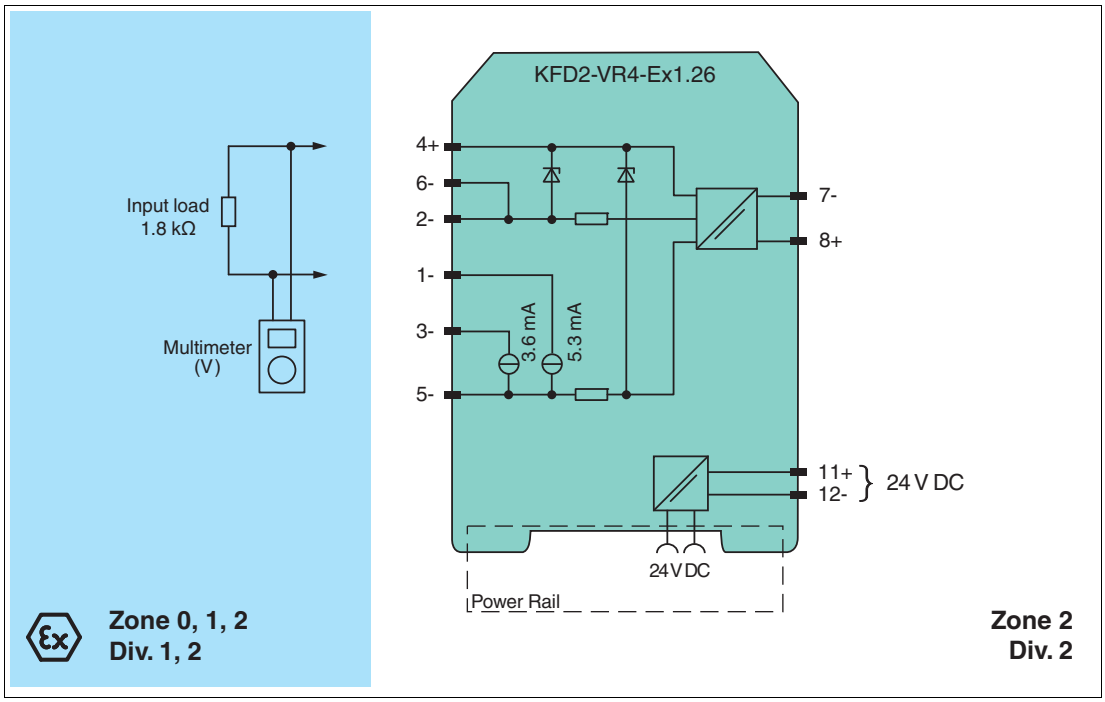


Figure 5.2 Set-up for proof test C

Proof Test Procedure D

1. Prepare the test set-up, see figure below.
2. Connect an input load of 1.8 kΩ to terminals 3- and 4+.
3. Measure the voltage load across the resistor and the current derived from it.
   ↳ The current value must be between 2.9 mA and 4.3 mA.
4. Disconnect the ancillary equipment.
5. Set back the device to the original settings after the test.
6. Restore the safety loop.

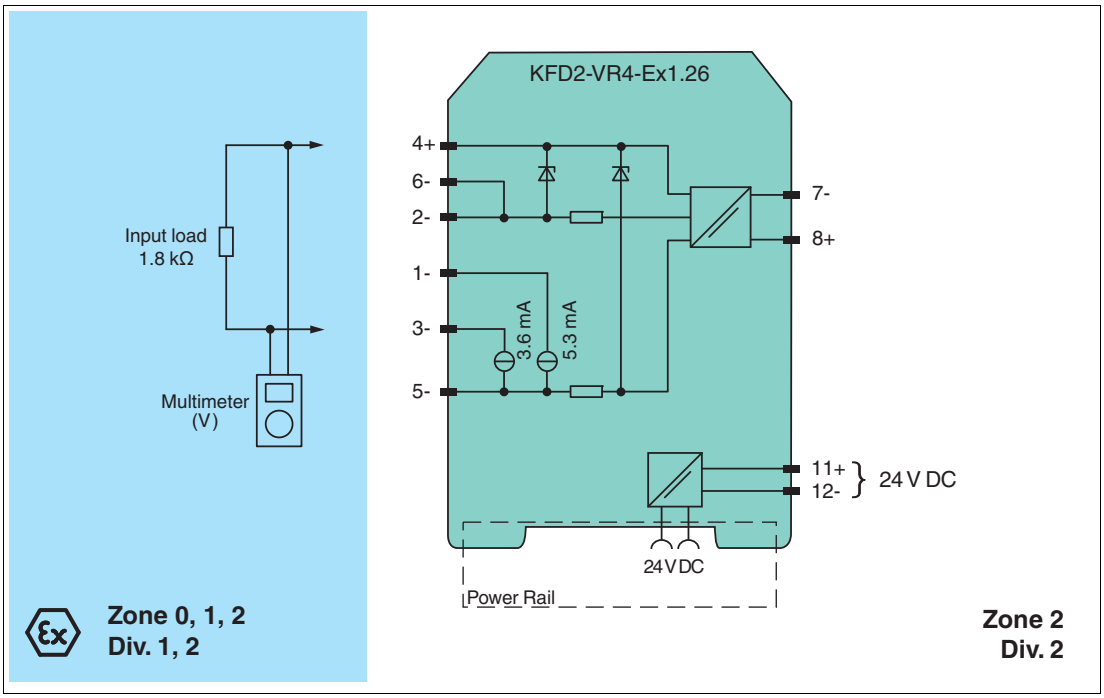


Figure 5.3 Set-up for proof test D

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.

2018-03

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
$\lambda_{total\ (safety\ function)}$	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
PLC	**P**rogrammable **L**ogic **C**ontroller
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
T_1	Proof Test Interval

2018-03

2018-03

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-2518B
03/2018

SCATTERGOOD & JOHNSON LTD
ELECTRICAL ENGINEERING & FLUID CONTROL DISTRIBUTORS
Est.1899

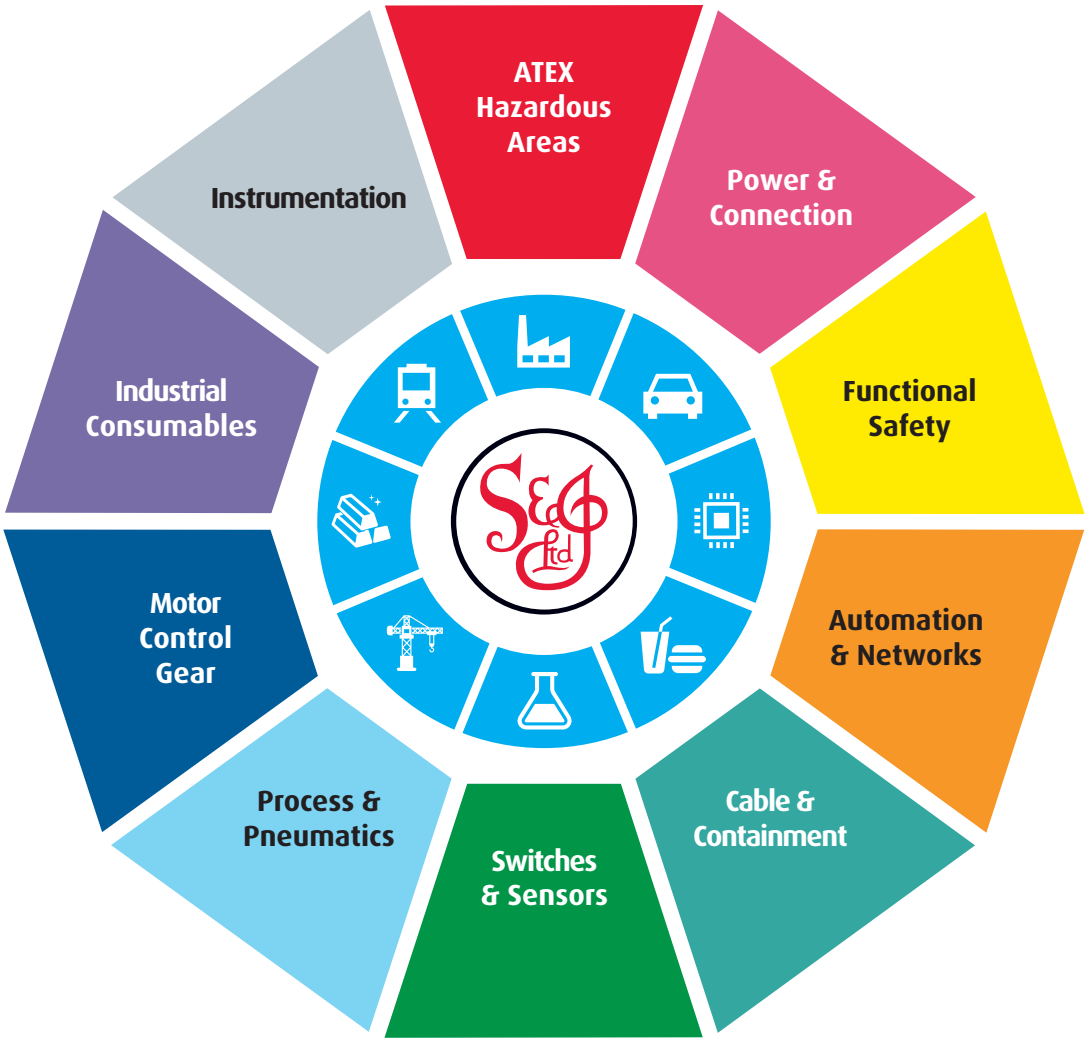
At Scattergood & Johnson Ltd, we pride ourselves on being a technical distributor to specialist industries.

Working with a range of quality product suppliers across a number of specialist markets, we are not your average 'box shifter' - we are your technical and supply chain partner.

We fully support every product we sell - for free! Our internal team and external sales engineers can answer any product or application question, no matter the complexity.

Backing up this technical ability is a range of 50,000+ products available from stock for nationwide next day delivery (same day if required!), or you can collect what you need from any of our trade counters around the UK.

Select your specialist interest below to learn more about how we can help.



Online, In Branch and On the Road - Scattergood & Johnson Ltd, there when you need us.

www.scatts.co.uk