Functional Safety

Switch Amplifier
KFU8-SR-1.3L.V

Manual

SIL

IEC 61508/61511

ISO9001

SIL 2

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.

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

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

This signal conditioner converts the state of 3-wire sensors (PNP or NPN) or sensors with push-pull output stages into two relay outputs.

It has one input and two form C changeover relay outputs.

The switch amplifier has an adjustable energized/de-energized delay for the relay outputs.

The start-up time of the device is as long as the time setting value + 500 ms.

During an error condition the outputs de-energize.

A fault is signalized by LEDs.

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

2.2 Interfaces

The device has the following interfaces:

- Safety-relevant interfaces: input, output I, output II
- Non-safety relevant interfaces: fault indication output

Note

For corresponding connections see datasheet.

2.3 Marking

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

KFU8-SR-1.3L.V	Up to SIL 2

2.4 Standards and Directives for Functional Safety

Device specific standards and directives

Functional safety	IEC/EN 61508, part 1 – 7, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC 61511-1:2016+COR1:2016+A1:2017 EN 61511-1:2017+A1:2017 Functional safety – Safety instrumented systems for the process industry sector (user)

DOCT-9020 2024-04

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 rates are constant, wear is not considered.
- Failure rate based on the Siemens standard SN 29500.
- The safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- External power supply failure rates are not included.
- Only one input and one output are part of the safety function (only for 2-channel version).
- Short circuit (SC) detection and lead breakage (LB) detection are enabled.
- 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 ºC may be assumed. For a higher average temperature of 60 ºC, 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.

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.
- 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 10^{-2}, hence the maximum allowable PFD_{avg} value would then be 10^{-3}.
- For a SIL 2 application operating in high demand mode the total PFH value of the SIF should be smaller than 10^{-6} per hour, hence the maximum allowable PFH value would then be 10^{-7} per hour.
- Since the 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.

3.3 Safety Function and Safe State

Safe State

In the safe state of the safety function the output is de-energized.

Safety Function

Configuration for the SIL applications

Switch	Function		Position
S1	Sensor type	Input: push-pull output, NO contact, NPN	I
		Input: PNP, NO contact	II
S2	Default time	Any position [1]	I or II
S3	Mode of operation	ON delay, minimum input pulse length	I
S4	Direction of effect	Output I activated if sensor closed	I
		Output I activated if sensor open	II
S5	Direction of effect	Output II activated if sensor closed	I
		Output II activated if sensor open	II
S6	Time setting	Any position [2]	0 to 7
S7	Time setting	Any position [2]	0 to 9

Table 3.1

[1] Position I: default time = 0.1 s x (time setting value of switches S6 and S7)
Position II: default time = 1 s x (time setting value of switches S6 and S7)

[2] The device changes the state from dangerous to safe state immediately.
Only the opposite change of state is influenced by the delay functionality.

Reaction Time

The fault reaction time is ≤ 50 ms.

Note

See corresponding datasheets for further information.

3.4 Characteristic Safety Values

1oo1 Structure

Parameters	Characteristic values	
Assessment type and documentation	Full assessment	
Device type	A	
Mode of operation	Low demand mode or high demand mode	
HFT	0	
SIL	2	
SC	3	
Safety function	1 output relay is de-energized when the input is in OFF state [1].	2 output relays are de-energized when the input is in OFF state [1].
λ_s	227 FIT	249 FIT
λ_{dd}	0 FIT	73 FIT
λ_{du}	72 FIT	37.1 FIT
$\lambda_{no\ effect}$	198 FIT	202 FIT
$\lambda_{total\ (safety\ function)}$	299 FIT	359 FIT
SFF [2]	76 %	90 %
MTBF [3]	190 years	171 years
PFH	7.16×10^{-8} 1/h	3.71×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year [4]	3.14×10^{-4}	1.63×10^{-4}
PFD_{avg} for T_1 = 2 years [4]	6.27×10^{-4}	3.25×10^{-4}
PFD_{avg} for T_1 = 3 years [4]	9.41×10^{-4}	8.13×10^{-4}
PTC	100 %	
Fault reaction time [5]	≤ 50 ms	

Table 3.2

1 Sensor type: 3-wire sensor for SIL 2 safety loop, PNP/NPN or push-pull output
2 **No effect failures** are not influencing the safety function and are therefore not included in SFF and in the failure rates of the safety function.
3 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.
4 8760 h/year
5 Time between fault detection and fault reaction

The characteristic safety values like PFD, SFF, HFT and T_1 are taken from the SIL report/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. Observe that the useful lifetime can be reduced if the device is exposed to the following conditions:

- highly stressful environmental conditions such as constantly high temperatures
- temperature cycles with high temperature differences
- permanent repeated mechanical stress (vibration)

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

Please note 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.

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

The device is configured via DIP switches. The DIP switches are on the front of the device.

1. De-energize the device before configuring the device.
2. Open the cover.
3. Configure the device for the required safety function via the DIP switches, see chapter 3.3.
4. Close the cover.
5. Secure the DIP switches to prevent unintentional adjustments.
6. Connect the device again.

Note

See corresponding datasheets for further information.

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.

Check the settings after the configuration by suitable tests.

5.1.1 Procedure for Manual Proof Test

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
- 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).

Proof Test Procedure

1. Put out of service the entire safety loop. Protect the application by means of other measures.
2. Prepare a test set-up, see figures below.
3. Simulate the sensor state by connecting a potentiometer, a resistor for short circuit detection or by a resistor for lead breakage detection.
   Test each input channel individually.
4. Connect a potentiometer of 4.7 kΩ (threshold for normal operation) to the input.
   ↳ The threshold must be between 1.4 mA and 1.9 mA, the hysteresis must be between 170 µA and 250 µA.
   - If the input current is above the threshold the relay must be activated for normal mode of operation. The yellow LED lights up.
   - If the input current is below the threshold the relay must be activated for inverted mode of operation. The yellow LED lights up.
5. 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.
6. Test all relay outputs with a specific current, e. g. 100 mA. To avoid electric shock, use a test voltage of 24 V DC. Check that the relay contacts are open.
   ↳ The relays must be de-activated. The relay contacts must **definitely open**.
7. After the test, reset the device to the original settings.
8. Check the correct behavior of the safety loop. Is the configuration correct?
9. Secure the DIP switches to prevent unintentional adjustments.

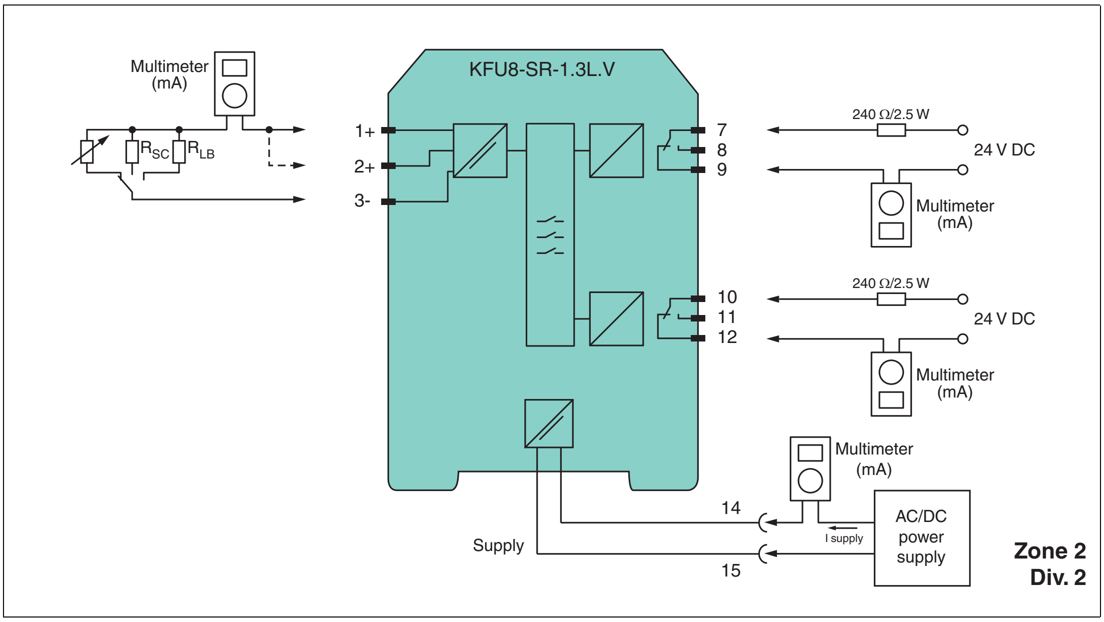

Figure 5.1 Proof test set-up

2024-04
DOCT-9020

PEPPERL+FUCHS

5.1.2 Procedure for In-Loop Proof Test

If you check the safety function within an application, 90 % of the dangerous undetected failures are revealed.

You can also use documented switching actions for verification within the framework of regular proof test intervals. The calculated values correspond to the values in the **Characteristic Safety Values** table, see chapter 3.4.

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 List of Abbreviations

DC	**D**iagnostic **C**overage of dangerous faults
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
MTTF$_D$	**M**ean **T**ime **T**o dangerous **F**ailure
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
PL	**P**erformance **L**evel
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

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-9020 2024-04