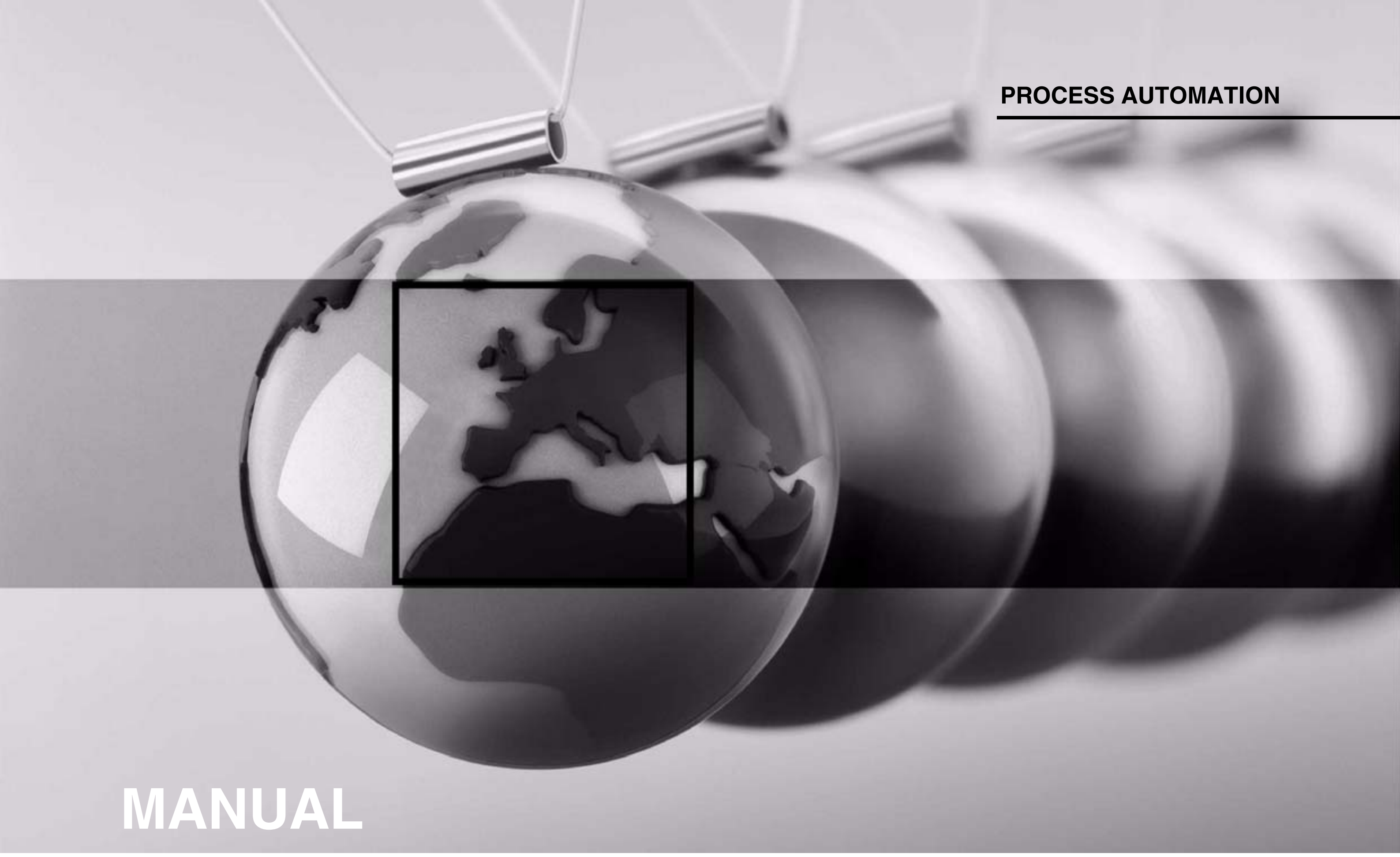

Functional Safety

M-LB-(Ex-)5000-System
Surge Protection Barriers

SIL
IEC 61508/61511

ISO9001

CE

SIL 3

Ex

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

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.

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

PEPPERL+FUCHS

2 Product Description

2.1 Function

This manual describes solely the safety function and safe state of the surge protection barrier as part of the surge protection system. The surge protection barrier consists of a protection module and a base module.

Danger!

Danger to life from wrong usage of the device

The protection of the safety loop against overvoltage is **not the safety function** of the surge protection barrier.

The surge protection barrier protects applications and equipment against voltage surges caused by lightning or switching operations.
The statement concerning the safety function of the surge protection barrier solely describes the effect on safety loops in which the barrier is installed. The barrier acts in the safety loops as a simple pass through element.

Surge Protection Barrier without Status Indication

The surge protection barrier without status indication consists of a M-LB-(Ex-)51** protection module and a M-LB-(Ex-)50**(.SP) base module.

The protection module limits induced transients of different causes, e. g. lightning or switching operations. The limitation is achieved by diverting the current to earth and limiting the signal circuit voltage during the duration of the overvoltage pulse.

The device is inserted onto the base module and forms the surge protection barrier together with the base module.

The device can be replaced without tools by a locking lever.

Surge Protection Barrier with Status Indication

The surge protection barrier with status indication consists of a M-LB-(Ex-)52** protection module and a M-LB-(Ex-)50**(.SP) base module.

The protection module limits induced transients of different causes, e. g. lightning or switching operations. The limitation is achieved by diverting the current to earth and limiting the signal circuit voltage during the duration of the overvoltage pulse.

The device has LEDs for the status indication. If required, this status is transferred to the corresponding function module via a status indication output.

This status indication is non-safety-relevant.

The device is inserted onto the base module and forms the surge protection barrier together with the base module.

The device can be replaced without tools by a locking lever.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces: protected signal lines
- Non-safety relevant interfaces: fault indication output

Note!

For corresponding connections see datasheet.

2.3 Marking

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

Protection modules M-LB-(Ex-)51**, M-LB-(Ex-)52** Base modules M-LB-(Ex-)50**(.SP)	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 1 – 7, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1 – 3, edition 2003: Functional safety – Safety instrumented systems for the process industry sector (user)

3 Planning

3.1 System Structure

3.1.1 Low Demand Mode of Operation

If there are two control loops, one for the standard operation and another one for the functional safety, then usually the demand rate for the safety loop is assumed to be less than once per year.

The relevant safety parameters to be verified are:

- the PFD_{avg} value (average **P**robability of dangerous **F**ailure on **D**emand) and the T_1 value (proof test interval that has a direct impact on the PFD_{avg} value)
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.2 High Demand or Continuous Mode of Operation

If there is only one safety loop, which combines the standard operation and safety-related operation, then usually the demand rate for this safety loop is assumed to be higher than once per year.

The relevant safety parameters to be verified are:

- the PFH value (**P**robability of dangerous **F**ailure per **H**our)
- Fault reaction time of the safety system
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.3 Safe Failure Fraction

The safe failure fraction describes the ratio of all safe failures and dangerous detected failures to the total failure rate.

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

A safe failure fraction as defined in IEC/EN 61508 is only relevant for elements or (sub)systems in a complete safety loop. The device under consideration is always part of a safety loop but is not regarded as a complete element or subsystem.

For calculating the SIL of a safety loop it is necessary to evaluate the safe failure fraction of elements, subsystems and the complete system, but not of a single device.

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

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 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.
- The control loop is considered to be either isolated from ground (except i. e. components within the protection module), or one of the protected lines is directly connected to ground. In both cases, a failure mode leads to a safe reaction or has no effect, so the worst case is assumed to be a no effect failure.
- Failure rate based on the Siemens standard SN29500.
- Failure rates are constant, wear is not considered.
- The control loop has a hardware fault tolerance of **0** and it is a type **A** device. A SFF value for this device is not given, since this value has to be calculated in conjunction with the connected field device, as described in the following section.
- The devices M-LB-(Ex-)5*13 and M-LB-(Ex-)5*14 do not withstand conducted RF immunity tests (10 V according to IEC/EN 61000-4-6).
  The devices M-LB-(Ex-)5*13, M-LB-(Ex-)5*14, M-LB-(Ex-)5*43, and M-LB-(Ex-)5*44 do not withstand immunity tests against conducted common mode disturbances at spot frequencies (100 V according to IEC/EN 61000-4-16).

  Cause is that the limit values of the protective elements for the application are lower than the test limits required by the standards. The user has to decide whether the devices are suitable for the application or whether the devices with higher voltage limits must be used.

Application

The surge protection barrier and the connected device (field device, 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}	10^{-2}	10^{-7}	10^{-3}
Actuator (40 %)	4×10^{-7}	4×10^{-3}	4×10^{-8}	4×10^{-4}
Transmitter (25 %)	2.5×10^{-7}	2.5×10^{-3}	2.5×10^{-8}	2.5×10^{-4}
Isolator (10 %)	10^{-7}	10^{-3}	10^{-8}	10^{-4}

Table 3.1 Overview PFD_{avg}/PFH budget

3.3 Safety Function and Safe State

The safety function of the surge protection barriers depends on the signal loop to which it is attached. The interference on safety relevant signals (e. g. 4 mA to 20 mA analog signal) that pass through the devices was evaluated.

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.

The surge protection barriers limit induced transients of different causes, e. g. lightning or switching operations. This protection function itself is not the safety function of the device.

Safe State

The safe state depends on the application. There are 6 different applications:

- Digital input (NAMUR signal)
  Lead breakage and short circuit are out of range and counted as safe failures.
- Digital output (de-energized to safe – DTS)
  Lead breakage and short circuit interrupt the energy transfer to the field and are counted as safe failures.
- Analog input (4 mA ... 20 mA)
  Lead breakage and short circuit are out of range and counted as safe failures.
- Analog output (4 mA ... 20 mA)
  Lead breakage and short circuit interrupt the energy transfer to the field and are counted as safe failures.
- Resistance thermometer (RTD)
  Measurement current = 200 µA (i. e. KFD2-UT2-1)
  - R ≤ 3137 Ω (Pt1000 at 600 °C)
  - R ≥ 60 Ω (Pt100 at -100 °C)
  Wire resistance = 35 Ω (1000 m total and 0.5 mm^2 Cu)

  Lead breakage and short circuit are out of range and counted as safe failures.
- Thermocouple (TC)
  - U ≤ 80 mV (type E at 1000 K)
  - U ≥ -10 mV (type E at -270 K)
  Lead breakage and short circuit lead to plausible temperature readings and were rated dangerous undetected. Special values apply, see Table 3.2. If you are using a signal converter with line fault detection, the values for standard 2-wire applications apply.

For the evaluation, all deviations from the input signal were rated as dangerous undetected, if the deviations are

- greater than the specified leakage current or
- greater than the 0.5 Ω line resistance.

The user must observe the valid range for the signals in the application and react accordingly if this range is left.

The values given in the following table are calculated for 2-wire, 3-wire or 4-wire applications as field devices are usually connected by more than one wire. For the calculation, add the numbers from the respective column to the numbers given for the safety loop. They are already summarized for the respective application.

Safety Function

The safety function of the surge protection barrier is to behave like a piece of copper wire, passing through the process signal without being altered.

Reaction Time

The reaction time is < 1 ms.

Note!
The fault indication output is not safety relevant.

Note!
See corresponding datasheets for further information.

3.4 Characteristic Safety Values

1oo1 Structure

Parameters	Characteristic values			
Assessment type	Full assessment			
Device type	A			
Mode of operation	Low demand mode or high demand mode			
Safety function [1]	Pass through the signal			
HFT	0			
SIL [2]	3			
Devices	M-LB-(Ex-)51**, M-LB-(Ex-)52**, M-LB-(Ex-)50**(.SP)			
	2-wire	2-wire (TC)	3-wire	4-wire
λ_s	16.8 FIT	0 FIT	14.9 FIT	19.8 FIT
λ_{du}	1.1 FIT	17.8 FIT	8.4 FIT	15.2 FIT
λ_{dd}	0 FIT	0 FIT	0 FIT	0 FIT
$\lambda_{no\ effect}$	17.3 FIT	17.3 FIT	46 FIT	57.3 FIT
$\lambda_{total\ (safety\ function)}$	17.8 FIT	17.8 FIT	23.3 FIT	35 FIT
MTBF [3]	3247 years	3252 years	1646 years	1236 years
PFH	1.05×10^{-9} 1/h	1.78×10^{-8} 1/h	8.44×10^{-9} 1/h	1.52×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	4.60×10^{-6} 1/h	1.69×10^{-4} 1/h	9.35×10^{-5} 1/h	1.44×10^{-4} 1/h
PFD_{avg} for T_1 = 2 years	9.20×10^{-6} 1/h	3.38×10^{-4} 1/h	1.87×10^{-4} 1/h	2.89×10^{-4} 1/h
PFD_{avg} for T_1 = 5 years	2.30×10^{-5} 1/h	8.46×10^{-4} 1/h	4.68×10^{-4} 1/h	7.22×10^{-4} 1/h
PFD_{avg} for T_1 = 10 years	4.60×10^{-5} 1/h	1.69×10^{-3} 1/h	9.35×10^{-4} 1/h	1.44×10^{-3} 1/h
PTC	100 %	87 %	83 %	87 %
Reaction time [4]	< 1 ms			

Table 3.2

1 The safe state of the surge protection barrier depend on the application.
2 The maximum safety integrity level of the safety loop in which the device might be used depends on the performance values of the whole safety loop or the elements of the safety loop. See chapter 7.
3 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 24 h.
4 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, 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.

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.

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 instruction 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 24 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test

According to IEC/EN 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous failures that are not detected otherwise.

Check the function of the subsystem at periodic intervals depending on the applied PFD_{avg} in accordance with the characteristic safety values. See chapter 3.4.

It is under the responsibility of the plant operator to define the type of proof test and the interval time period.

Equipment required:

- 2 digital multimeter with an accuracy of 0.1 %
- Variable power supply 0 V DC to 50 V DC and current limitation

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. Test the devices for the application they are used for.
4. Set back the device to the original settings for the application after the test.

Leakage Current Measurement

Device	Step no.	Measurement	Expected result
M-LB-(Ex-)5*42	1	30 V between terminals 3 and 4	Leakage current below 3 µA
M-LB-(Ex-)5*44	1 2 3	30 V between terminals 3 and 4 30 V between terminal 3 and ground 30 V between terminal 4 and ground	Leakage current below 6 µA
M-LB-(Ex-)5*12	1	1 V between terminals 3 and 4	Leakage current below 5 µA
M-LB-(Ex-)5*14	1 2 3	1 V between terminals 3 and 4 1 V between terminal 3 and ground 1 V between terminal 4 and ground	Leakage current below 5 µA
M-LB-(Ex-)5*41	1	15 V between terminals 3 and 4	Leakage current below 3 µA
M-LB-(Ex-)5*43	1 2	15 V between terminals 3 and 4 15 V between terminal 3 and ground	Leakage current below 6 µA
M-LB-(Ex-)5*11	1	1 V between terminals 3(+) and 4(-)	Leakage current below 5 µA
M-LB-(Ex-)5*13	1 2	1 V between terminals 3(+) and 4(-) 1 V between terminal 3(+) and ground(-)	Leakage current below 5 µA

Table 5.1

Resistance Measurement

Device	Step no.	Measurement	Expected result
M-LB-(Ex-)5**1 M-LB-(Ex-)5**2	1	Resistance between terminals 1 and 4	Resistance below 0.5 Ω
M-LB-(Ex-)5**3 M-LB-(Ex-)5**4	1 2	Resistance between terminals 1 and 4 Resistance between terminals 2 and 3	Resistance below 0.5 Ω

Table 5.2

6 Maintenance and Repair

Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.

Maintaining, Repairing or Replacing the Device

In case of maintenance, repair or replacement of the device, proceed as follows:

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

7 Application Examples

This chapter shows how to integrate a surge protection barrier into a safety loop.

Integration of a Surge Protection Barrier into a Safety Loop

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

1. the signal characteristic of the safety loop: analog or digital,
2. the signal direction of the safety loop as seen from the perspective of the safety-rated programmable logic controller (SPLC): input or output,
3. the safe state of the field device allocated to the surge protection barrier,
4. the mode of operation: low demand mode, high demand mode or continuous mode
5. the required SIL level of the safety loop.

After the safety loop is defined, assign a surge protection barrier to the field device.
Create a basic overview as shown below.

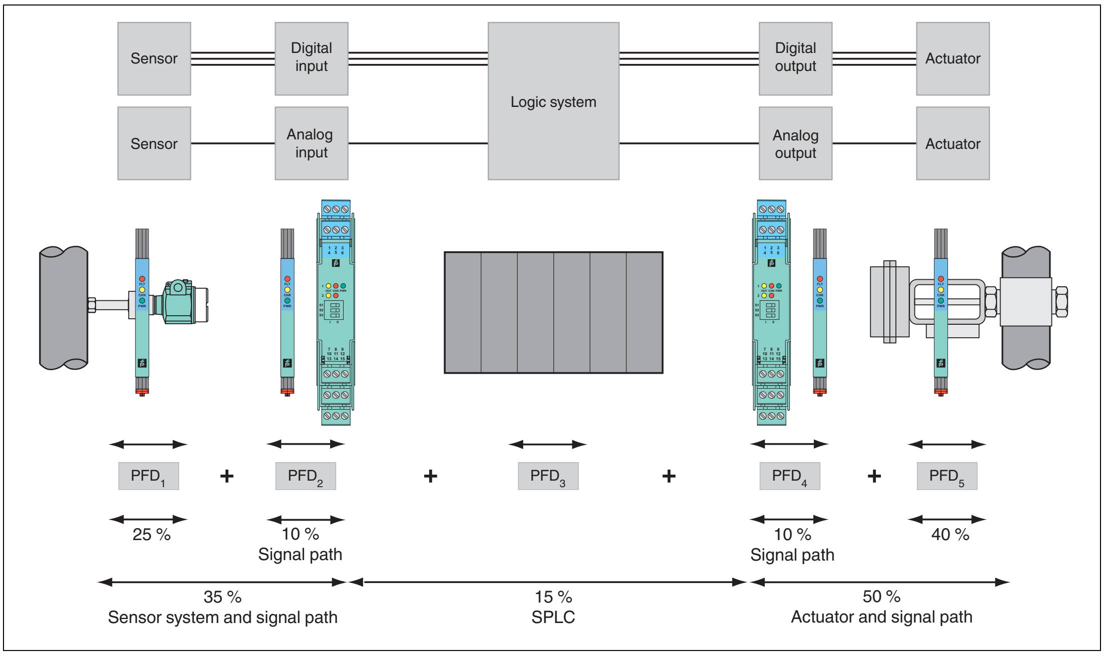

Figure 7.1 Example of a complete safety loop with assigned surge protection barriers

In principle, the performance values of the surge protection barriers have to be added to the performance values of the field device or the safety-rated programmable logic controller (SPLC). By doing so, it is assumed that the surge protection barrier is a part of this device. Verify with these new values if the necessary SIL level can be achieved.

You find examples of the various applications in the following section.

Example 1 - Digital Input - NAMUR NE 22 Signals

When using a standard isolated barrier from Pepperl+Fuchs, it is possible to implement low demand safety loops with SIL 2 with a standard NAMUR NE 22 digital input signal.
A sample configuration would be the isolated barrier KCD2-SR-Ex1.LB with surge protection barrier M-LB -Ex-5***.

Basic parameters:

1. Signal characteristic of the safety loop: 2-wire application
2. Signal direction of the safety loop as seen from the perspective of the safety-rated programmable logic controller (SPLC): input
3. Safe state of the field device allocated to the surge protection barrier: de-energized
4. Required SIL level of the safety loop: SIL 2

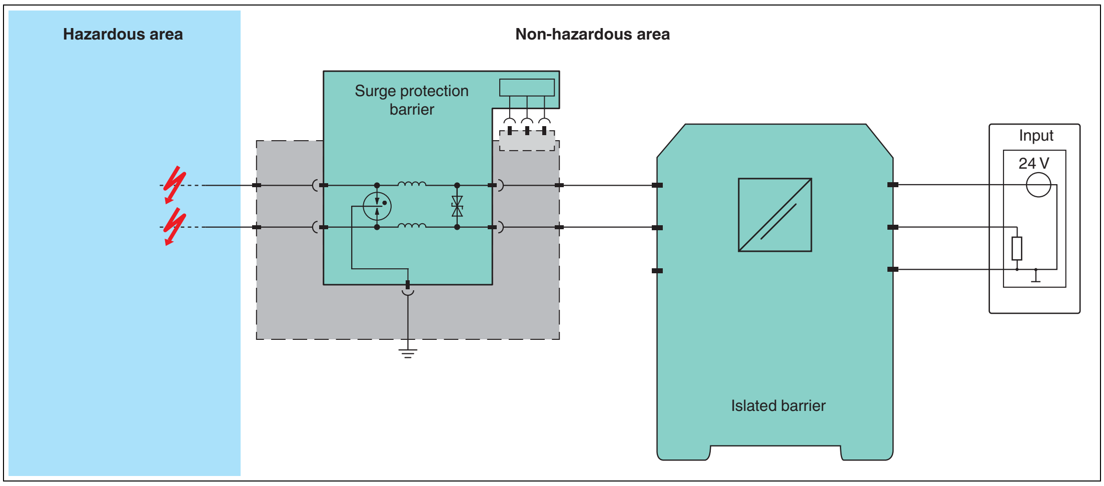

Figure 7.2 Sample configuration consisting of a surge protection barrier and an isolated barrier

SIL level calculation of the safety loop

- SFF value of the safety loop is as demanded for type A components > 60 %.
- As an optimum, the combination of surge protection barrier and isolated barrier claims 10 % of the overall PFD_{avg} maximum 1×10^{-2} and therefore has a $PFD_{avg} <1 \times 10^{-3}$

The isolated barrier KCD2-SR-Ex1.LB has the following performance values:

λ_{total}	254 FIT
PFD_{avg} for T_1 = 1 year	2.05×10^{-4}
SFF	81.5 %

Table 7.1

Use for calculation of λ_{du} of the isolated barrier the PFD_{avg} formula given in IEC 61508:

- $PFD_{avg} = 1/2 \times \lambda_{du} \times T_1$
- $\lambda_{du} = 2 \times PFD_{avg} / T_1 = 2 \times 2.05 \times 10^{-4} / 8760\ [h] = 47$ FIT

2018-03

PEPPERL+FUCHS

The corresponding surge protection barrier M-LB-Ex-5*** has the following performance values:

λ_{total}	17.8 FIT
λ_{du}	1.1 FIT

Table 7.2

The next step is to allocate the surge protection barrier to the isolated barrier by adding the total failure rates of both components.

- $\sum \lambda_{total} = \lambda_{isolated\ barrier} + to + \lambda_{surge\ protection\ barrier}$
- $\sum \lambda_{total}$ = 254 FIT + 17.8 FIT ≈ 272 FIT

The same has to be done for the dangerous undetected failure rates of both devices.

- $\sum \lambda_{du} = \lambda_{du/isolated\ barrier} + to + \lambda_{du/surge\ protection\ barrier}$
- $\sum \lambda_{du}$ = 47 FIT + 1.1 FIT ≈ 48 FIT

Use these values for calculating the SFF and PFD_{avg} for the combination of both devices.

- SFF = 1 – (λ_{du} / λ_{total})
- SFF = 1 – (48 FIT / 272 FIT) = 82 %
- PFD_{avg_1y} = 1/2 x λ_{du} x 8760 [h] (5)
- PFD_{avg_1y} = 1/2 x 48 FIT x 8760 [h] = 2.10 x 10^{-4}

The following table summarizes the results of the calculations:

λ_{total}	272 FIT
λ_{du}	48 FIT
PFD_{avg} for T_1 = 1 year	2.10 x 10^{-4}
SFF	82 %

Table 7.3

The requirements for a SIL 2 safety loop are still fulfilled for this specific combination.

Example 2 - Digital Output – Solenoid Drivers

The Pepperl+Fuchs digital output devices can be categorized into two groups – loop powered devices and bus powered devices.

The calculation for both groups is identical except that values of the solenoid driver may be different. The method for calculation is identical to the method in the previous example.

Basic parameters:

1. Signal characteristic of the safety loop: 2-wire application
2. Signal direction of the safety loop as seen from the perspective of the safety-rated programmable logic controller (SPLC): output
3. Safe state of the field device allocated to the surge protection barrier: de-energized
4. Required SIL level of the safety loop: SIL 2

The isolated barrier has the following performance values:

λ_{total}	714 FIT
λ_{du}	10.3 FIT
PFD_{avg} for T_1 = 1 year	4.51×10^{-5}
SFF	98.5 %

Table 7.4

The corresponding surge protection barrier M-LB-Ex-5*** has the following performance values:

λ_{total}	17.8 FIT
λ_{du}	1.1 FIT

Table 7.5

Use these values for calculating the SFF and PFD_{avg} for the combination of both devices. Use for calculation the PFD_{avg} formula given in IEC 61508, see above.

The following table summarizes the results of the calculations:

λ_{total}	732 FIT
λ_{du}	11.4 FIT
PFD_{avg} for T_1 = 1 year	4.99×10^{-5}
SFF	98.6 %

Table 7.6

The requirements for a SIL 2 safety loop are still fulfilled for this specific combination.

Example 3 - Analog Inputs – 4 mA to 20 mA Signals

Basic parameters:

1. Signal characteristic of the safety loop: analog 2-wire application
2. Signal direction of the safety loop as seen from the perspective of the safety-rated programmable logic controller (SPLC): input
3. Safe state of the field device allocated to the surge protection barrier: output signal < 4 mA or > 20 mA
4. Required SIL level of the safety loop: SIL 3

The isolated barrier KCD2-STC-Ex1 has the following performance values:

λ_{total}	348 FIT
λ_{du}	67 FIT
PFD_{avg} for T_1 = 1 year	2.93×10^{-4}
SFF	80.8 %

Table 7.7

The corresponding surge protection barrier M-LB-Ex-5*** has the following performance values:

λ_{total}	17.8 FIT
λ_{du}	1.1 FIT

Table 7.8

Use these values for calculating the SFF and PFD_{avg} for the combination of both devices. Use for calculation the PFD_{avg} formula given in IEC 61508, see above.

The following table summarizes the results of the calculations:

λ_{total}	366 FIT
λ_{du}	68 FIT
PFD_{avg} for T_1 = 1 year	2.98×10^{-4}
SFF	81.4 %

Table 7.9

The requirements for a SIL 3 safety loop are still fulfilled for this specific combination.

8 List of Abbreviations

PCS	**P**rocess **C**ontrol **S**ystem
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_d	Probability of dangerous failure
$\lambda_{no\ effect}$	Probability of failures of elements in the safety control 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 elements that are not in the safety control loop
$\lambda_{total\ (safety\ function)}$	Safety function
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**ailures
MTTR	**M**ean **T**ime **T**o **R**estoration
PFD$_{avg}$	Average **P**robability of **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
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

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-5661A
03/2018