Functional Safety in practice

Whitepaper

Endress+Hauser

People for Process Automation

Register

1	**Introduction**	**3**
2	**End user project management**	**3**
2.1	Risk assessment and risk reduction	3
2.2	From potential hazards to safety	4
2.3	Types of errors in safety systems	5
2.4	Functional Safety Management	6
2.5	Limitation of figures – probabilistic vs. systematic	7
2.6	Technical requirements	8
2.7	Qualification of personnel	8
2.8	Requirements for a legally sound implementation	8
3	**Design and planning of safety instrumented systems**	**9**
3.1	General Requirements	9
3.2	Component selection	9
3.2.1	Operability	9
3.2.2	Proof of suitability	9
3.2.3	Required information	10
3.3	The Functional Safety Manual	10
4	**Safety loop calculation**	**11**
4.1	Preliminary remarks	11
4.2	Calulation formulas	12
4.3	Sample calculations	13
4.3.1	Single-channel protective system	13
4.3.2	Multichannel protective system	14
5	**Life cycle of Safety Instrumented Systems**	**20**
5.1	Commissioning	20
5.2	Safe parameterization	20
5.3	Device behavior during normal operation and during failures	21
5.4	Proof test	22
5.4.1	General	22
5.4.2	Effect of the proof test interval on PFD_{avg}	22
5.4.3	Ideal proof test	23
5.4.4	Proof Test Coverage	24
5.5	Repair	27
5.6	Modification	27
5.7	Useful lifetime	27
6	**Appendix**	**28**
6.1	References	28
6.1.1	Standards	28
6.1.2	Relevant NAMUR recommendations	28
6.1.3	Selected Internet Resources	29
6.2	Calculations according to IEC 61508:2010	29
6.3	Overview calculation tools	31
7	**Glossary**	**32**

1 Introduction

Functional safety is still an intensively discussed topic in the process industry.

This document is a supplement to the Endress+Hauser publication CP01008Z "Functional safety - SIL" and presumes the knowledge about Functional Safety gained there. It provides additional information for more advanced practitioners without using the standard language too much. For more detailed information, a study of relevant literature and the relevant standards is recommended.

The information in this publication is provided to the best of our knowledge. However we cannot accept any liability from misunderstanding that may occur.

2 End user project management

2.1 Risk assessment and risk reduction

To assess the risk reduction in functional safety the relevant safety figures are a useful tool. The target safety integrity level (SIL) characterizes the measure of the achievable risk reduction. The assessment of risk and risk reduction are tasks of the system operator.

Based on best practice (e.g. risk graph, HAZOP, LOPA), the operator determines the risk of a plant and the required risk reduction. For this purpose, he defines the safe state and uses appropriate measures to ensure that the required safety functions can be performed.

Note that despite all safety measures, a residual risk remains. Failures, that are not recognized and therefore do not lead to a safe state, remain a residual risk in the system. The operator must ensure that the residual risk is less than the tolerable risk.

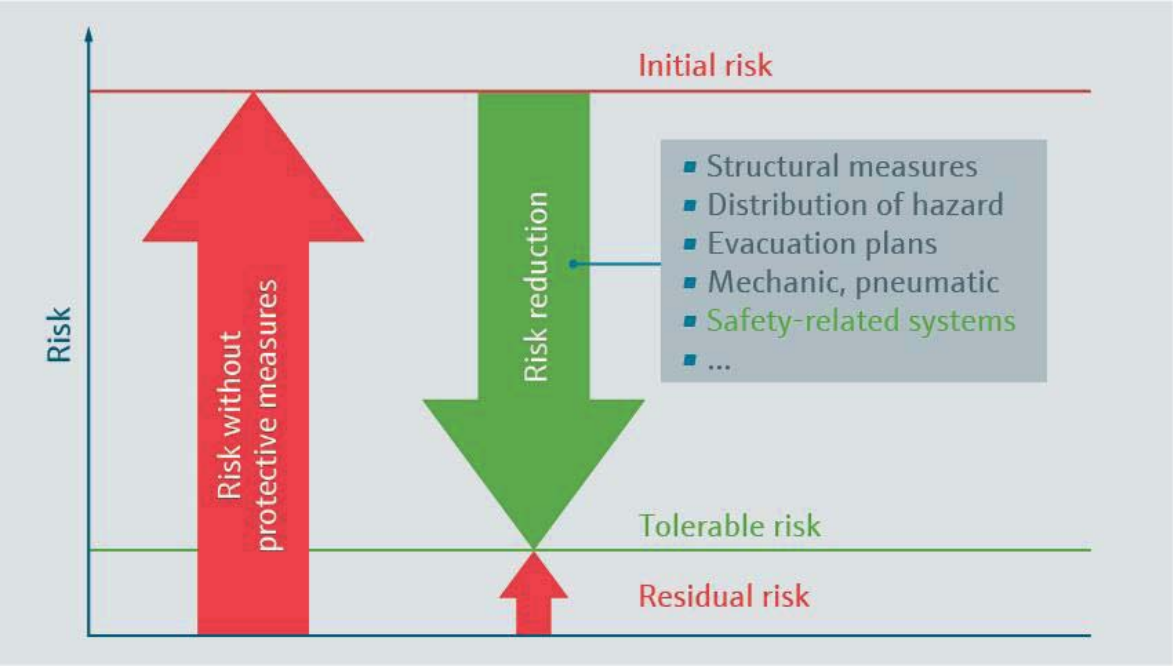


Figure 1: Risk reduction measures in facilities

There are various risk reduction measures (see Figure 1). In this document, only the risk-minimizing measures by safety instrumented systems (SIS) are described.

2.2 From potential hazards to safety

The operators of safety systems must take appropriate measures for risk assessment and risk reduction during the entire lifecycle.

For this purpose, IEC 61508 defines certain steps:

- Risk definition and assessment according to detailed failure probabilities for the entire safety loop from the sensor to the controller to the actuator over the entire safety lifecycle.
- Definition and implementation of measures (Functional Safety Management).
- Use of suitable (qualified) devices.

IEC 61511 defines this for safety systems as follows:

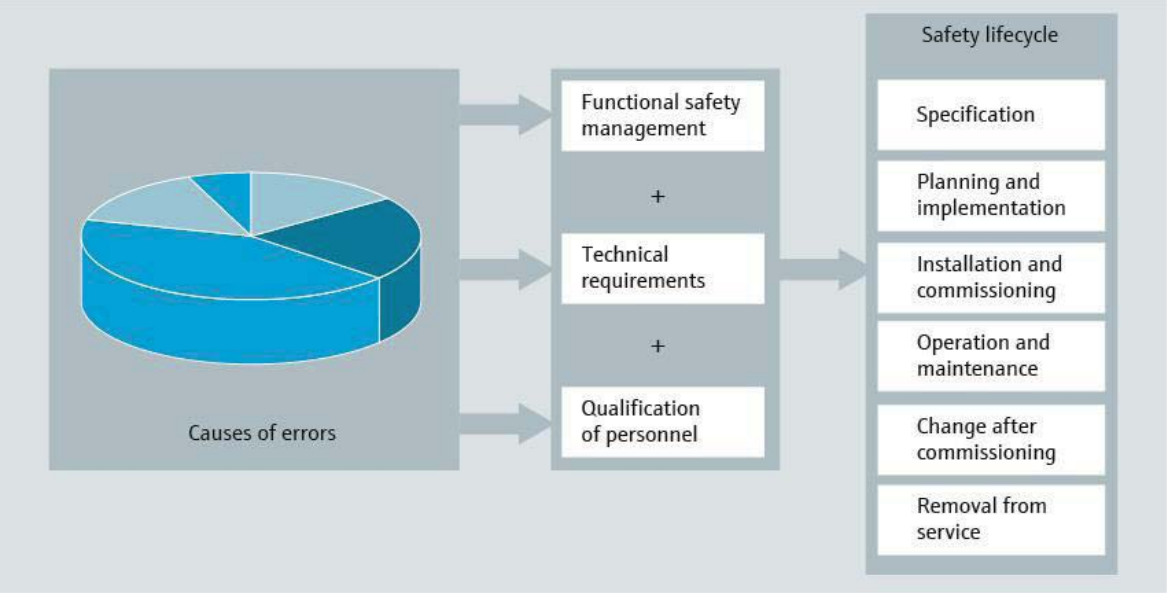


Figure 2: From potential hazards to safety

2.3 Types of errors in safety systems

In safety systems, the following types of errors can occur:

- Systematic faults
- Random faults (random failures)

According to VDI / VDE 2180 Part 5, faults in the use of devices in safety systems can be controlled as follows:

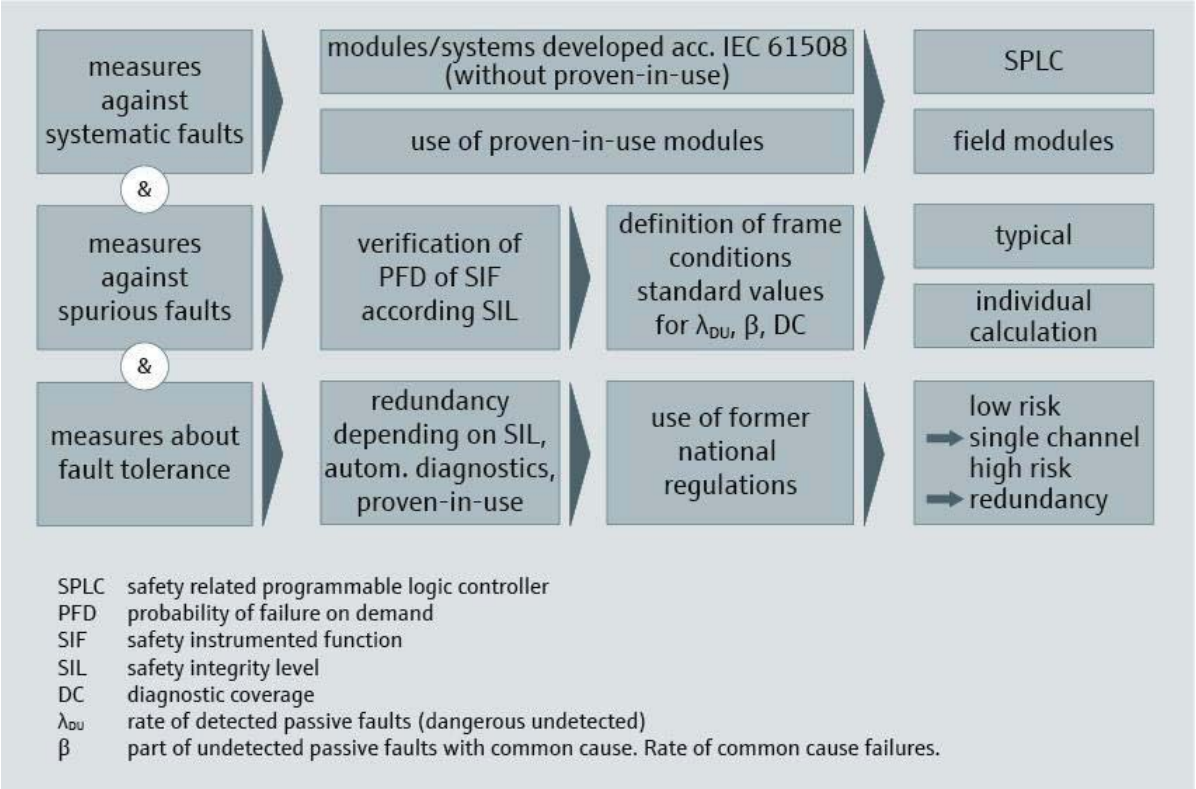


Figure 3: Measures to be taken when using devices in safety systems (Source: VDI/VDE 2180 Part 5)

2.4 Functional Safety Management

Every operator of a safety-related system should implement a functional safety management system. Below, an example of a Functional Safety Management System at an operator's facility is given (table of contents).

Table of contents	
1	Objective / purpose
	Terms and abbreviations
3	Scope
4	Organization in the safety lifecycle
4.1	Safety plan
4.2	Delegation of responsibility
4.2.1	Planning team
4.2.2	Assessment team
4.3	Risk consideration
4.3.1	Consideration of the risks within the HAZOP
4.3.2	Allocation of the scope of the relevant standard
4.3.3	Classification of the safety systems (SIS)
4.4	Preparation of system specification
4.5	Preparation of requirement specifications
4.6	Software Implementation
4.7	Verification of software
4.8	Installation and commissioning
4.9	Validation
4.10	Operation and maintenance
4.11	Decommissioning
5	Change management
6	Tests in safety lifecycle
6.1	Purpose
6.2	Tests to be carried out
6.2.1	Test of system specifications
6.2.2	Test of requirement specifications
6.2.3	Verification of software
6.2.4	Verification of correct application of assembly and commissioning
6.2.5	Validation
7	Audit (check of operational quality features)
7.1	Purpose
7.2	Planning and execution (minimum requirements)
7.2.1	Delegation of responsibility
7.2.2	Definition of scope
7.2.3	Specification of frequency
7.2.4	Execution of the audit
7.2.5	Documentation and evaluation of results
8	Applicable Documents
9	Modification service
10	Requirement index

Figure 4: Example of the structure of a Functional Safety Management System

2.5 Limitation of figures – probabilistic vs. systematic

For the assessment of the residual risk not only the results from the random hardware failures are relevant, but also systematic faults have an impact. These are caused by non-compliance with boundary conditions in the application area. Operators and system designers must consider the conditions and restrictions published by the device manufacturer in the safety documentation. Non-compliance can have impact on proper execution of the safety function. For example, exceeding the permissible ambient temperature can downgrade the measurement accuracy.

To reduce systematic faults, functional safety management systems of both the manufacturer and the operator are important for safe and reliable operation.

Random failures are evaluated using probabilistic methods. These failures are detected by device-internal diagnostic measures which set the device to a safe state.

For the assessment of the residual risk in a plant, the consideration of both safety-related figures and the avoidance of systematic faults are absolutely necessary.

	Systematic faults	**Random failures**
Plants	Incorrect design	None
	Incorrect assembly	
	Incorrect commissioning	
	Incorrect operation	
	Incorrect maintenance	
	Process influences	
	Program errors in application software	
	Force majeure (lightning flash, overvoltage, ...)	
	Test errors	
Devices	Specification errors	Component failures
	Incorrect sizing	Soft errors
	Incorrect design of components	
	Design errors	
	Programming errors in firmware and system software	
	Test errors	

Table 1: Incomplete listing of systematic errors and random failures in systems and devices

2.6 Technical requirements

To assess suitability of equipment for safety instrumented systems (sensors, controllers, actuators, interface blocks) the following methods can be used.

- Proof by certification
  - Which data base was used for classification?
  - How were the data collected?
  - Which conditions are associated with the application?

- Verification by proven-in-use
  - Evidence by manufacturer
  - Evidence by end user

- Proof by type examination (up to SIL 2)

The limits of these considerations are:

- No evaluation of process connections and interfaces (like tubing)
- No failure rates for mechanical components
- Critical time considerations (response times)

Generally a standardization of hardware and software is beneficial.

2.7 Qualification of personnel

Personnel responsible for safety-related systems should be qualified as follows:

- Use of professionals
- Continuous training
- Regular exchange of experience
- Use of the same team for the same requirements

For effective functional safety management of safety-related systems, a planning team and an assessment team should be established and the four eye principle.

Requirements for the planning team:

- Technical knowledge related to process engineering, technologies and techniques used.
- Safety knowledge based on knowledge of laws, standards and guidelines as well as technological safety standards.

Requirements for the assessment team:

- Define which other safety professionals should be involved in the assessment.
- Define which resources are necessary to carry out the assessment.
- Independence from the planning team

2.8 Requirements for a legally sound implementation

In summary, it can be concluded that a legally sound and cost-effective implementation of safety instrumented systems can be achieved amongst other things by the following measures:

- Creation of a Functional Safety Management System
- Standardization of hardware and software (e.g. by using certified or proven-in-use components)
- Documentation of requirements and activities / evidence
- Use of professionals

3 Design and planning of safety instrumented systems

Once the plant risk is identified, the design and planning of appropriate safety systems can be started. The reading of VDI / VDE 2180 is recommended (in particular Part 3).

3.1 General Requirements

The following general requirements should be considered amongst others in safety instrumented systems:

- The installation of a safety instrumented system should be simple and clear.
- The critical process variable has to be measured as directly as possible.
- A safety instrumented system should not be changed during operation.
- A strict separation of process control equipment and safety instrumented systems is beneficial and highly recommended.

3.2 Component selection

3.2.1 Operability

Amongst others, the following variables can affect the functional safety of components. This should be considered doing component selection.

Environmental influences:

- Mechanical influences (e.g. vibration, shock, impact, static forces)
- Corrosion and other chemical attack
- Pollution
- Temperature
- Moisture
- Power supply (overvoltage, undervoltage)
- Electromagnetic influences
- Radioactivity

Influences of process media:

- Mechanical influences (e.g. pulsation, turbulence, cavitation)
- Physical influences
- Chemical influences
- Thermal influences

3.2.2 Proof of suitability

All components of safety instrumented systems must have a proof of suitability. For this, there are the following options:

1. Components with proof of functional safety by the manufacturer: The proof is provided by a certificate of an external Notified Body.
2. Proven-in-use components (assessment of proven-in-use with support of the manufacturer): The proven-in-use evaluation of a device for a particular application can be determined by the end user, including a manufacturer's declaration.
3. Proven-in-use components (assessment of proven-in-use by the end user): For devices without SIL certificate the end user can self-declare proven-in-use in his plant.

Components assessed according to options 2 and 3 have been proven in comparable applications. However, their area of application is limited.

Components assessed according to option 1 can be used in all safety-related applications. The proof of suitability at the end user is carried out by a shortened procedure in various applications (see, e.g. NAMUR recommendation NE 130).

3.2.3 Required information

For planning and design of safety instrumented systems the following information must be available to the end user in advance:

- Device name and permitted versions
- Safety function of the device
- Safety-related output signal of the device
- Device type (A or B)
- Mode of operation (low demand mode, high demand mode)
- Valid hardware version
- Valid software version
- Type of assessment of the device (full assessment according to IEC 61508, proven-in-use assessment, evaluation of field data (prior use according to IEC 61511), FMEDA)
- Availability of a functional safety manual
- Systematic safety integrity
- Hardware safety integrity
- Failure rates (λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU})
- Assessment by external Notified Body?
- Availability of a Functional Safety Management at the manufacturer?
- Availability of a manufacturer quality management system: How does a manufacturer track safety-related systematic faults?

Notes on failure rates:
It can be assumed that various device manufacturers use different methods and tools in the determination of failure rates of their devices. The used data base and the considered working temperatures may differ. In addition, manufacturers may use different scopes of device evaluation (e.g. failures of mechanical components considered or not).

Therefore, the failure rates of different device manufacturers cannot be directly compared. Thus, they provide no statement about the quality of the device.

It is recommended to end users to define maximum values for the acceptable failure rates. All devices with ratings below these maximum values can be used when technically suitable.

3.3 The Functional Safety Manual

The Functional Safety Manual (Safety Manual) is an important part of a safety-related device, according to IEC 61508:2010, Annex D. It is even a mandatory requirement.

It must contain all the information to enable the integration of a device to a safety-related system. These are basically:

- Design of the measuring system
- Safety function
- Permitted device types (e.g. permissible hardware and software version)
- Instructions for installation, commissioning, operation, maintenance, repair, modification and decommissioning (safety lifecycle)
- Restrictions for use in safety-related systems
- Failure rates (λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU})
- Device type (A or B)
- Hardware fault tolerance
- Systematic capability
- Device behavior during operation
- Proof test (instructions and recommendations)

4 Safety loop calculation

4.1 Preliminary remarks

A safety instrumented system consists of three subsystems (see Figure 5):

- Sensor subsystem
- Logic subsystem
- Actuator subsystem

Sensor and actuator subsystems can consist of several sensor and actuator groups. In addition, interface components like power supply units have to be considered.

Each of these groups MooN consists of N channels, where M channels are sufficient to fulfill the safety function.

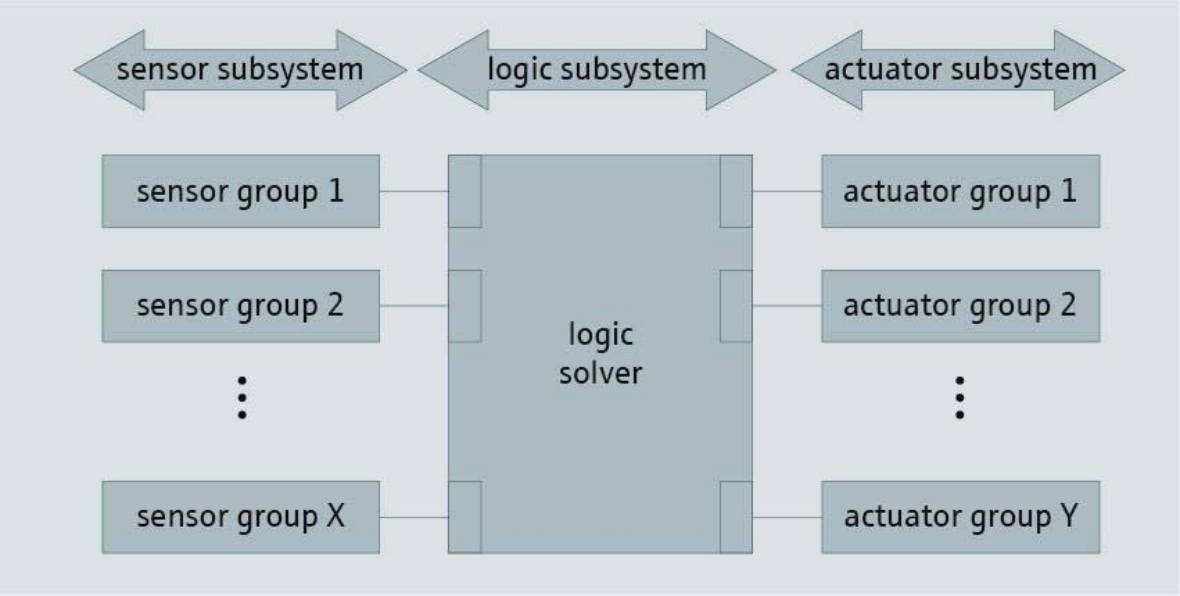


Figure 5: Structure overview of a safety instrumented system

A mathematical proof for safety instrumented systems is required in IEC 61511-1: 2016, Clause 11.9.1.

4.2 Calculation formulas

References for PFD_{avg} and PFH calculation formulas:

Reference	Contents
VDI/VDE 2180 Part 4, Clause 6.1	Approximation formulas for PFD_{avg} for different architectures MooN. Attention must be paid to the specified conditions for the applicability of the formulas.
IEC 61508-6:2000, Annex B	Formulas for PFD_{avg} and PFH (excluding Proof Test Coverage (PTC) and duration of use).
IEC 61508-6:2010, Annex B	Formulas for PFD_{avg} and PFH (including Proof Test Coverage (PTC) and duration of use). Only the formula for the architecture 1oo2 is referred to explicitly.

For the consideration in this chapter, the approximation formulas from VDI/VDE 2180 Part 4 are used.

The approximation formulas are:

$PFD_{1oo1} \approx \frac{1}{2}\lambda_{DU} \cdot T_1$
$PFD_{1oo2} \approx \frac{\lambda_{DU}^2 \cdot T_1^2}{3} + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$
$PFD_{1oo3} \approx \frac{\lambda_{DU}^3 \cdot T_1^3}{4} + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$
$PFD_{2oo2} \approx \lambda_{DU} \cdot T_1$
$PFD_{2oo3} \approx \lambda_{DU}^2 \cdot T_1^2 + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$

Meaning of symbols:

PFD	Average probability of failure on demand of the safety instrumented systems, later referred to as PFD_{avg}
λ_{DU}	Failure rate of dangerous undetected failures
T_1	Proof test interval (specified in hours)
β	Proportion of undetected common cause failures (Common Cause Factor). A method for determining β is specified in IEC 61508-6 Annex D. In practice, the value of β is usually in the range 5% to 10%.

The exact calculation formulas based on IEC 61508-6: 2010 are given in chapter 6.2.

4.3 Sample calculations

In this section, sample calculations are performed based on the approximation formulas. It is assumed that the individual components are suitable for achieving the required SIL levels. The parameters used in the calculations are examples.

Important note:

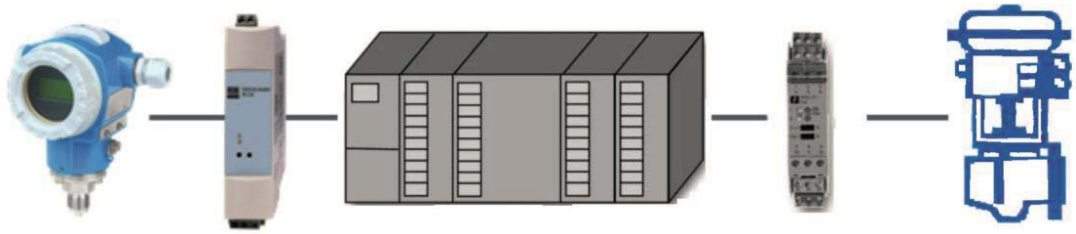
The calculations shown refer exclusively to random failures. In addition, a safety instrumented system must always be checked for systematic integrity.

Note:

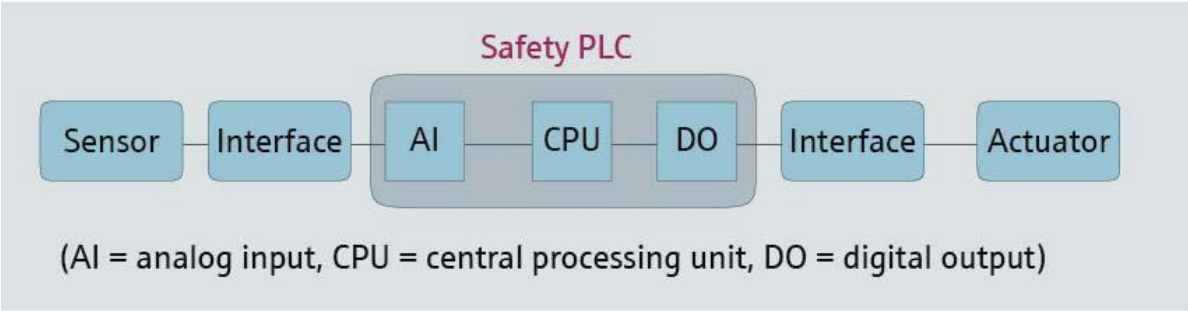
The considered examples are very simplified and serve for basic understanding only. These examples cannot be used for an exact calculation!

4.3.1 Single-channel protective system

Example: Single channel pressure monitoring



Block diagram:



Used approximation formula:

$$PFD_{1oo1} \approx \frac{1}{2}\lambda_{DU} \cdot T_1$$

Parameters (example values) and individual results:

Component	Sensor	Interface	Safety PLC			Interface	Actuator
			AI	CPU	DO		
λ_{DU} [1/h]	6.5×10^{-8}	6.3×10^{-8}	3.2×10^{-9}	3.0×10^{-9}	2.8×10^{-9}	6.6×10^{-8}	6.0×10^{-8}
T_1 [h]	8760	8760	87600	87600	87600	8760	8760
Hardware Safety Integrity	2	2	3			2	2
Systematic Safety Integrity	3	3	3			3	3
PFD_{avg} (1oo1)	2.9×10^{-4}	2.8×10^{-4}	1.4×10^{-4}	1.3×10^{-4}	1.2×10^{-4}	2.9×10^{-4}	2.6×10^{-4}

Overall result:

$PFD_{avg} = 2.9\times10^{-4} + 2.8\times10^{-4} + 1.4\times10^{-4} + 1.3\times10^{-4} + 1.2\times10^{-4} + 2.9\times10^{-4} + 2.6\times10^{-4} = 1.5\times10^{-3}$

This protective system is mathematically suitable for safety functions up to SIL 2 ($PFD_{avg} < 1\times10^{-2}$). The review of the systematic suitability gives SIL 3 (see table).

Note: As some components have a hardware safety integrity of SIL 2, the entire protective system can only be used for safety functions up to **SIL 2**.

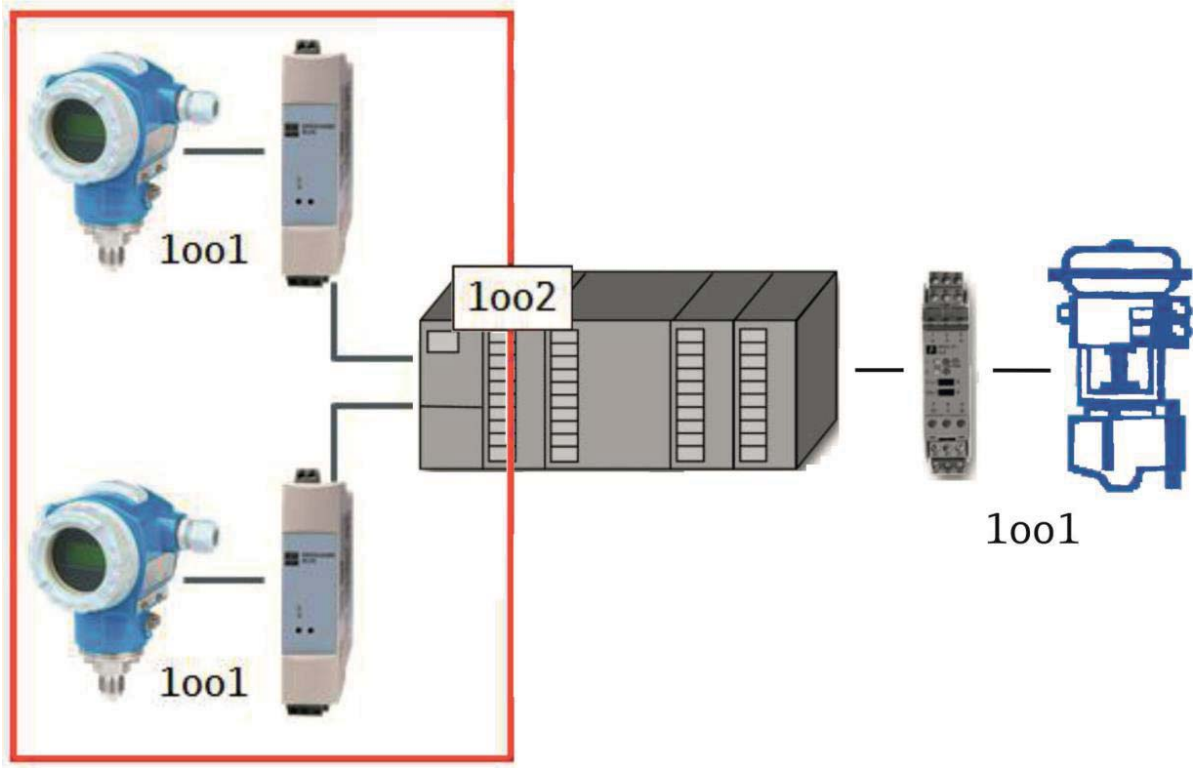
4.3.2 Multichannel protective system

Parameters used for calculation in this section (example values):

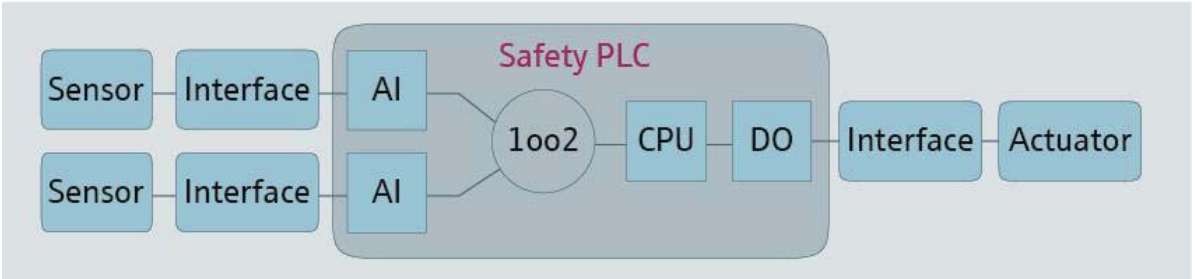
Component	Sensor	Interface	Safety PLC			Interface	Actuator
			AI	CPU	DO		
λ_{DU} [1/h)	6.5×10^{-8}	6.3×10^{-8}	3.2×10^{-9}	3.0×10^{-9}	2.8×10^{-9}	6.6×10^{-8}	6.0×10^{-8}
T_1 [h]	8760	8760	87600	87600	87600	8760	8760
Hardware Safety Integrity	2	2	3			2	2
Systematic Safety Integrity	3	3	3			3	3

4.3.2.1 Homogeneous redundant sensor subsystem

Example: Pressure monitoring with homogeneous redundant sensor subsystem in voting 1oo2



Block diagram:

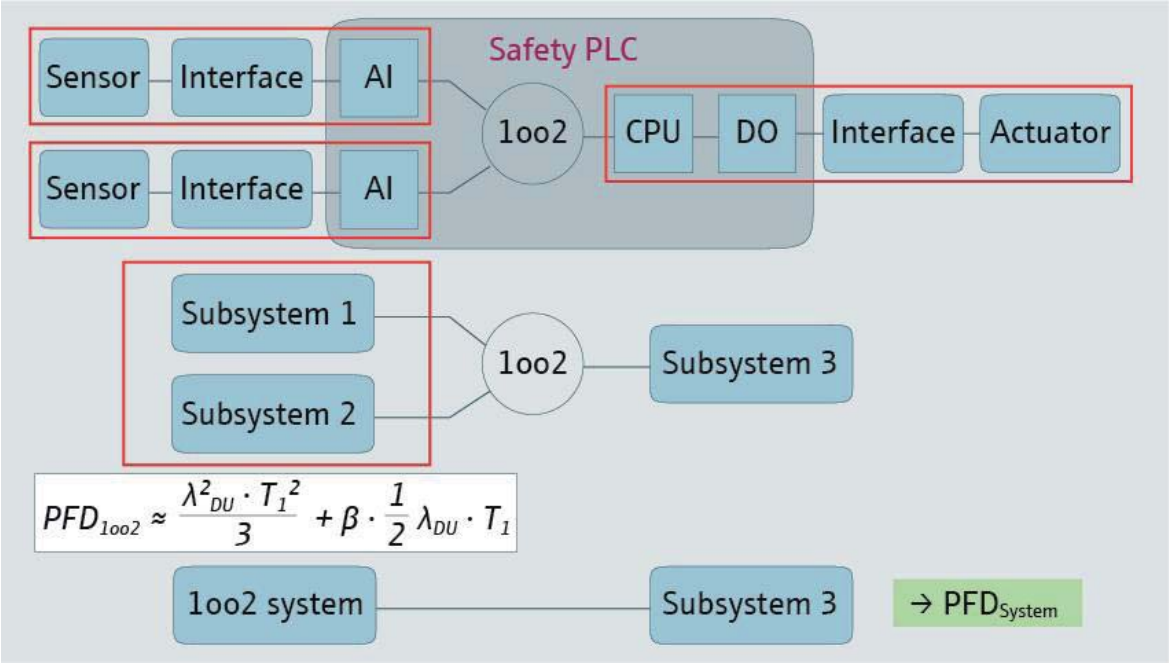


Used approximation formulas:

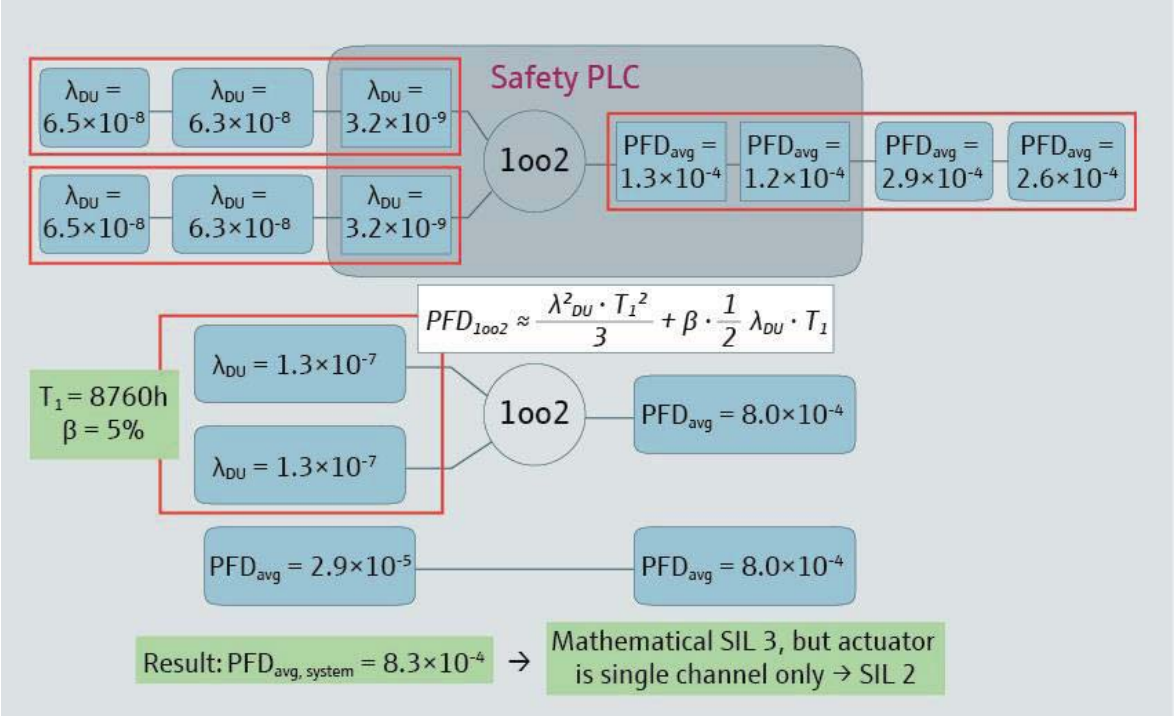
$$PFD_{1oo1} \approx \frac{1}{2}\lambda_{DU} \cdot T_1$$

$$PFD_{1oo2} \approx \frac{\lambda_{DU}^2 \cdot T_1^2}{3} + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$$

Procedure for calculation:



Performing the calculation:



Overall result:

PFD_{avg} = 8.3×10^{-4}

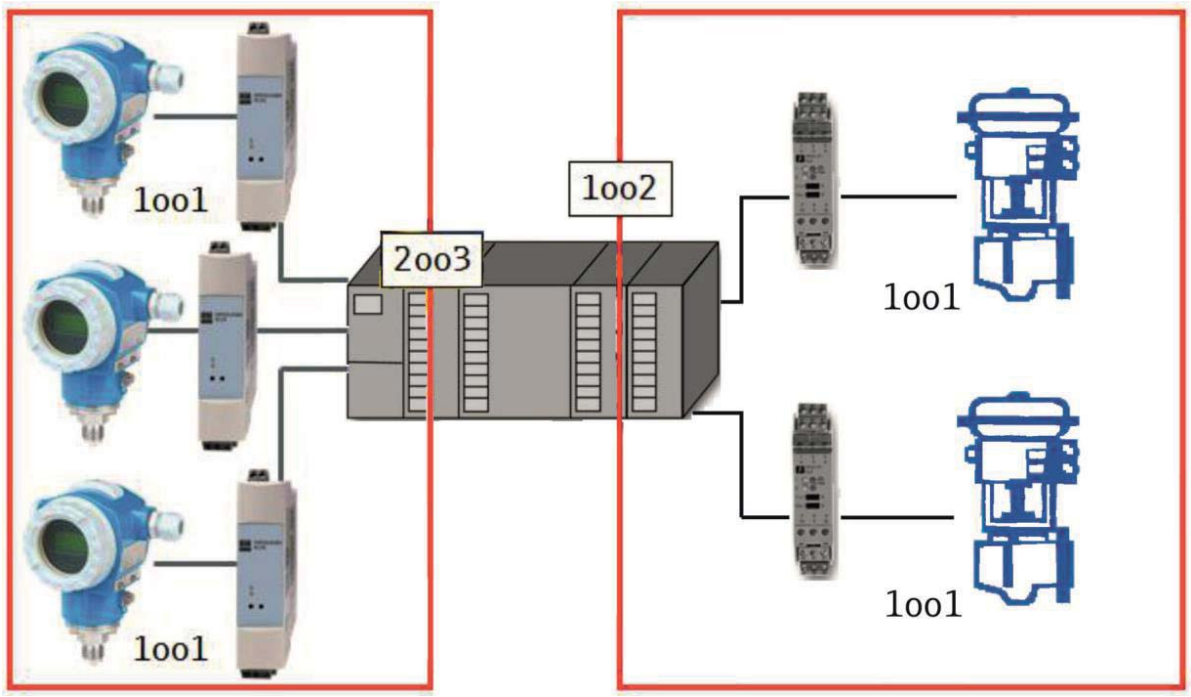
This protective system is mathematically suitable for safety functions up to SIL 3 ($PFD_{avg} < 1\times10^{-3}$). Note that the actuator interface and the actuator are configured only in single channel architecture and have hardware safety integrity of SIL 2. Hence, the entire protective system can only be used for safety functions up to **SIL 2**.

4.3.2.2 Homogeneous redundant sensor and actuator subsystems

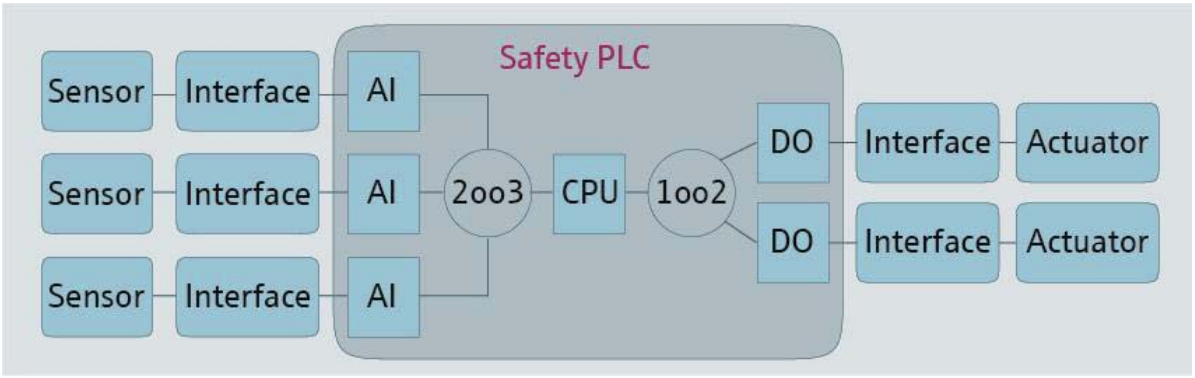
Example: Pressure monitoring with homogeneous redundant sensor subsystem in voting 2oo3 and homogeneous redundant actuator subsystem in voting 1oo2.

Note:

For reasons of availability, the voting 2oo3 is frequently preferred to 1oo2 system architecture.



Block diagramm:



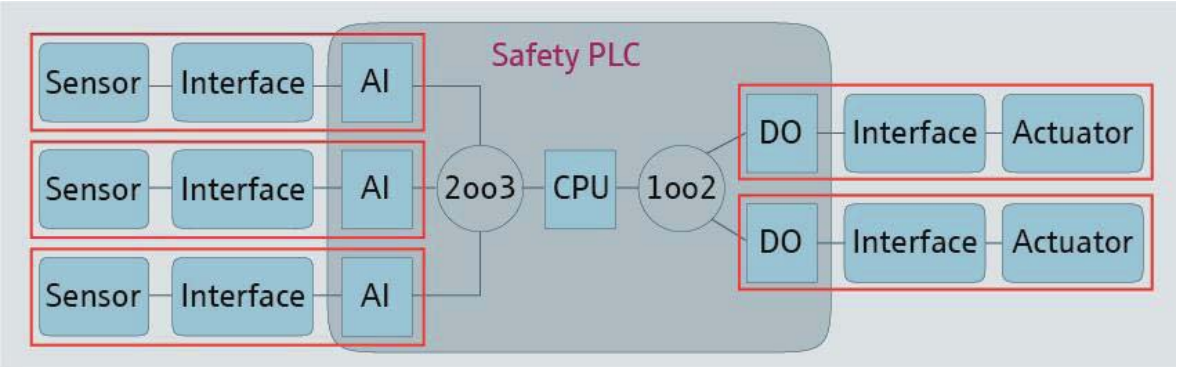
Used approximation formulas:

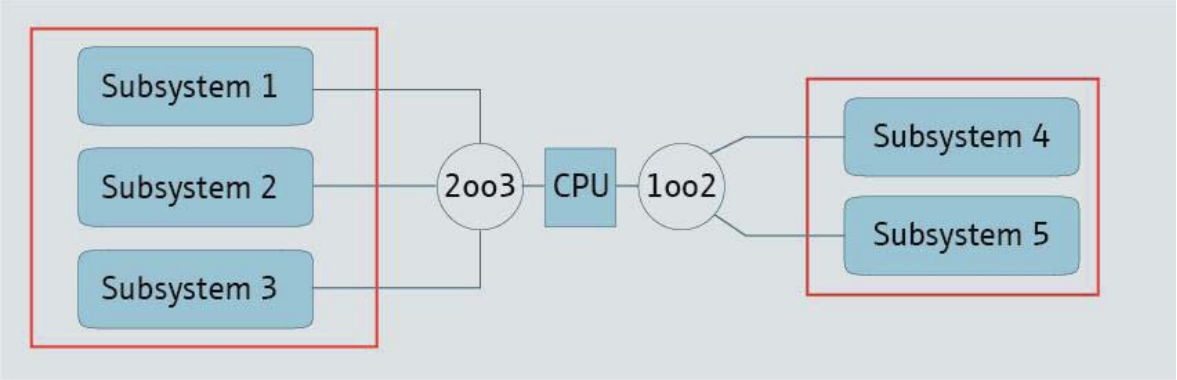
$$PFD_{1oo1} \approx \frac{1}{2}\lambda_{DU} \cdot T_1$$

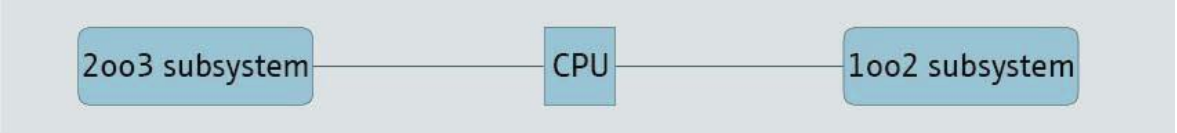
$$PFD_{1oo2} \approx \frac{\lambda_{DU}^2 \cdot T_1^2}{3} + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$$

$$PFD_{2oo3} \approx \lambda_{DU}^2 \cdot T_1^2 + \beta \cdot \frac{1}{2}\lambda_{DU} \cdot T_1$$

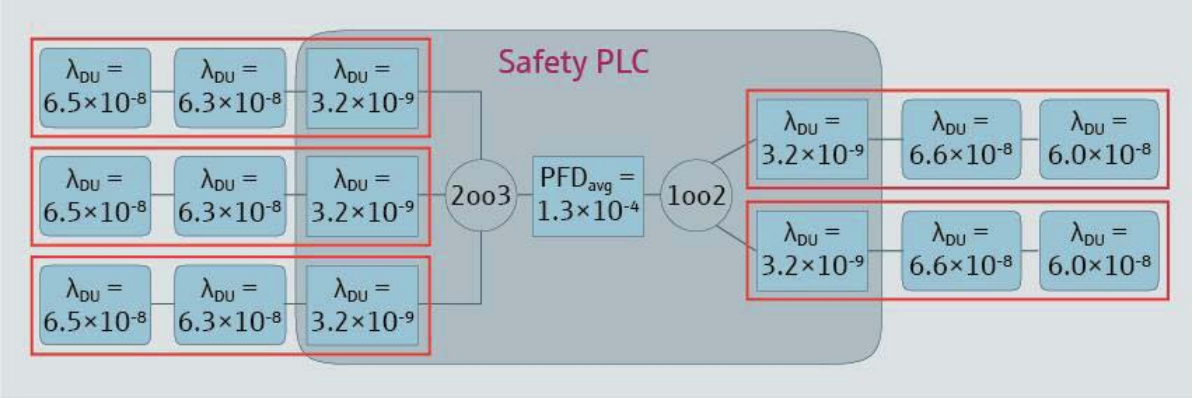
Procedure for the calculation:

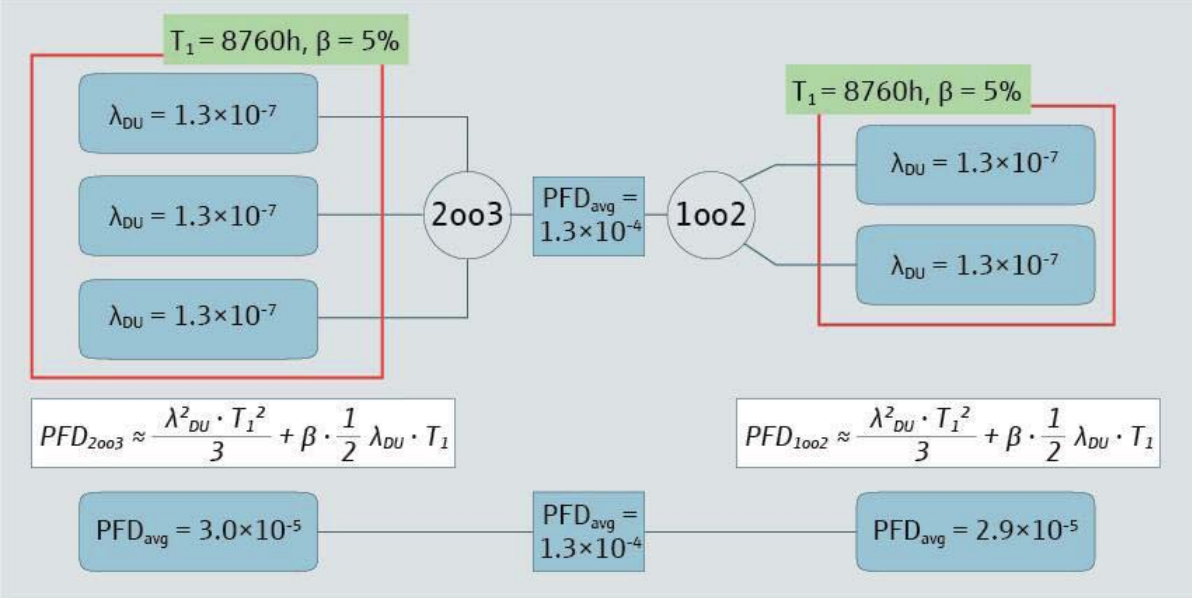






Performing the calculation:





Overall result:

$PFD_{avg} = 1.9 \times 10^{-4}$

This protective system is suitable for safety functions up to SIL 3 ($PFD_{avg} < 1 \times 10^{-3}$).

5 Life cycle of Safety Instrumented Systems

In the operation of safety instrumented systems, additional aspects need to be considered compared to standard installations. These are summarized in the following sections.

5.1 Commissioning

Before commissioning of safety-related devices, the following documentation must be available:

- Operating Manual
- Functional Safety Manual
- Operator requirements (e.g. end user documentation)

The procedure for commissioning is as follows:

- Standard installation according to operating manual
- Device parameterization and lock for safety-related use, if required in the Functional Safety Manual

Commissioning may be carried out by any expert of the operator or the manufacturer or a contractor. The Operating Manual and the Functional Safety Manual must be observed in its entirety.

Commissioning should be documented as follows:

- Create commissioning protocol (e.g. according to customer specifications or proposal in Functional Safety Manual)
- Filing and managing the commissioning documentation by the operator

5.2 Safe parameterization

Goal of safe parameterization is to configure all parameters necessary for the safety function and to check them for correctness. Moreover, the parameters are protected by a lock to prevent manipulation during the execution of the safety function.

To activate the safety function (SIL mode) a sequence of operations has to be performed. Operation can be carried out via local display (if available) or by an operator tool (e.g. FieldCare).

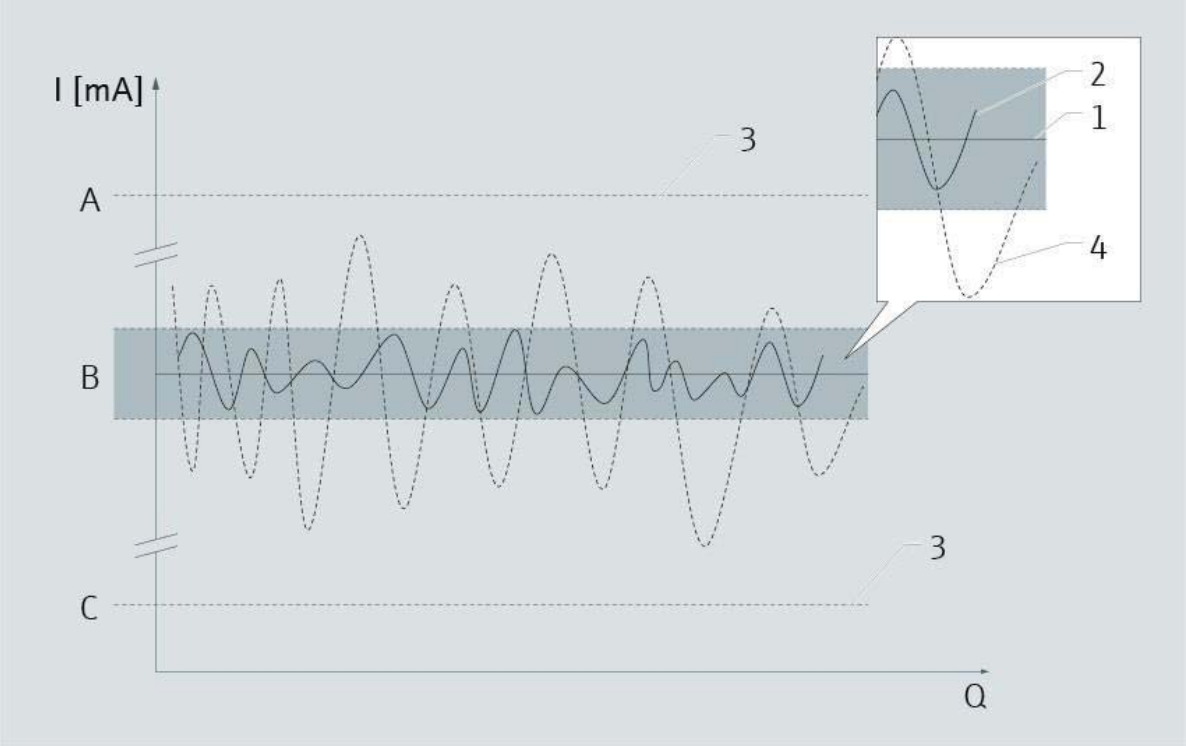
During the commissioning sequence, critical parameters are either automatically set to factory defaults by the device or transferred to local display/operator tool to the settings and confirm the correctness when passing through the startup sequence. After parameterization the SIL mode of the device must be activated with a SIL-lock code.

The device-specific parameterization can be found in the corresponding Functional Safety Manual.

5.3 Device behavior during normal operation and during failures

The safety-related output signal of the device shows a different behavior depending on the device status. This is shown in the table below using the example of an output signal 4...20 mA (see Figure 6).

Device state	Explanation	Device behavior
Normal operation	No device failures	**1** The device behaves within specification.
Failure λ_{SD}	Safe detected failure	**3** The device shows a failure signal.
Failure λ_{SU}	Safe undetected failure	**2** The output signal is within the specified tolerance band.
Failure λ_{DD}	Dangerous detected failure	**3** The device shows a failure signal.
Failure λ_{DU}	Dangerous undetected failure	**4** The output signal can be outside the specified tolerance band.



A High Alarm (≥ 21.0 mA)
B Tolerance band (e.g. ± 2 %)
C Low Alarm (≤ 3.6 mA)

Figure 6: Device behavior during normal operation and during failures

5.4 Proof test

5.4.1 General

Safety-related devices must be inspected for functionality at appropriate intervals. The relevant parameter is the time interval for periodic testing (proof test interval T_1). This value is to be included in the calculation of PFD_{avg}. It should be chosen so that PFD_{avg} stays within the required SIL range.

Proof tests serve to detect dangerous undetected failures (dangerous undetected ≙ λ_{du}) in a safety-related system. It is the goal to bring a safety system to an "as new" condition or as close as practical to this condition.

Responsibility of the end user is to choose the proof test procedure and the time intervals (T_1). The test shall be carried out such that the proper function of the safety system is proven observing the interaction of all components. The proof test intervals for different subsystems may be of different lengths.

The proof tests must be carried out, documented and managed by the end user. For this purpose, a proof test protocol should be created. The proof test is based on the proposal in Functional Safety Manual or operator requirement.

To ensure a controlled process a proof test protocol with control of timing is recommended. In the test instruction, the test procedure should be described in detail. The test documentation should be transparent and permanently available.

IEC 61511 allows both the proof test of the entire safety system as well as the test of subsystems only.

5.4.2 Effect of the proof test interval on PFD_{avg}

Failures are subject to an exponential distribution. The failure rate λ is constant with respect to time t and the following equation applies to the reliability function R(t).

$$R(t) = e^{-\lambda \cdot t}$$

The reliability indicates the degree of probability that a component will meet the requirements for a certain period of time.
The probability of failure P(t), by definition, indicates the probability that a component has failed before reaching a certain point in time. The failure probability function P(t) = PFD(t) is described as follows.

$$PFD(t) = P(t) = 1 - R(t) = 1 - e^{-\lambda \cdot t}$$

Simplification:
Assuming $x \ll 1$ it follows: $1 - e^{-x} \approx x$
From this it follows for PFD(t) under the conditions λ = const. and $\lambda \cdot t \ll 1$

$$PFD(t) = \lambda \cdot t$$

The failure rate λ is composed as follows: $\lambda = \lambda_{DU} + \lambda_{DD}$
For λ_{DD}, the mean time to restoration (MTTR) must be taken into account and for λ_{DU} the total time including MTTR for λ_{DU} must be considered. From this follows:

$$PFD(t) = \lambda_{DU} \cdot (t + MTTR) + \lambda_{DD} \cdot MTTR$$

In practice, the fractions caused by MTTR are neglected for the calculation of PFD(t). Assuming that MTTR = 8h << the operating time t, it follows:

$$PFD(t) = \lambda_{DU} \cdot t$$

Since the probability of failure is a linear curve, the mean value can be calculated simply by the integral of PFD(t).

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{1}{\mathrm{t}} \cdot \int_0^{T_1} \mathrm{PFD(t)}\ \mathrm{dt}$$

$$\mathbf{PFD_{avg} = \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD} \cdot MTTR}$$

Again, the approximation from practice can be used and the proportions of MTTR neglected, since MTTR << t. From this follows:

$$\mathbf{PFD_{avg} = \frac{1}{2} \cdot \lambda_{DU} \cdot T_1}$$

5.4.3 Ideal proof test

In Figure 7 an ideal proof test is shown, using the above derived formulas. However, this case does not occur in practice, because there is no perfect proof test. In a real proof test the Proof Test Coverage is to be considered.

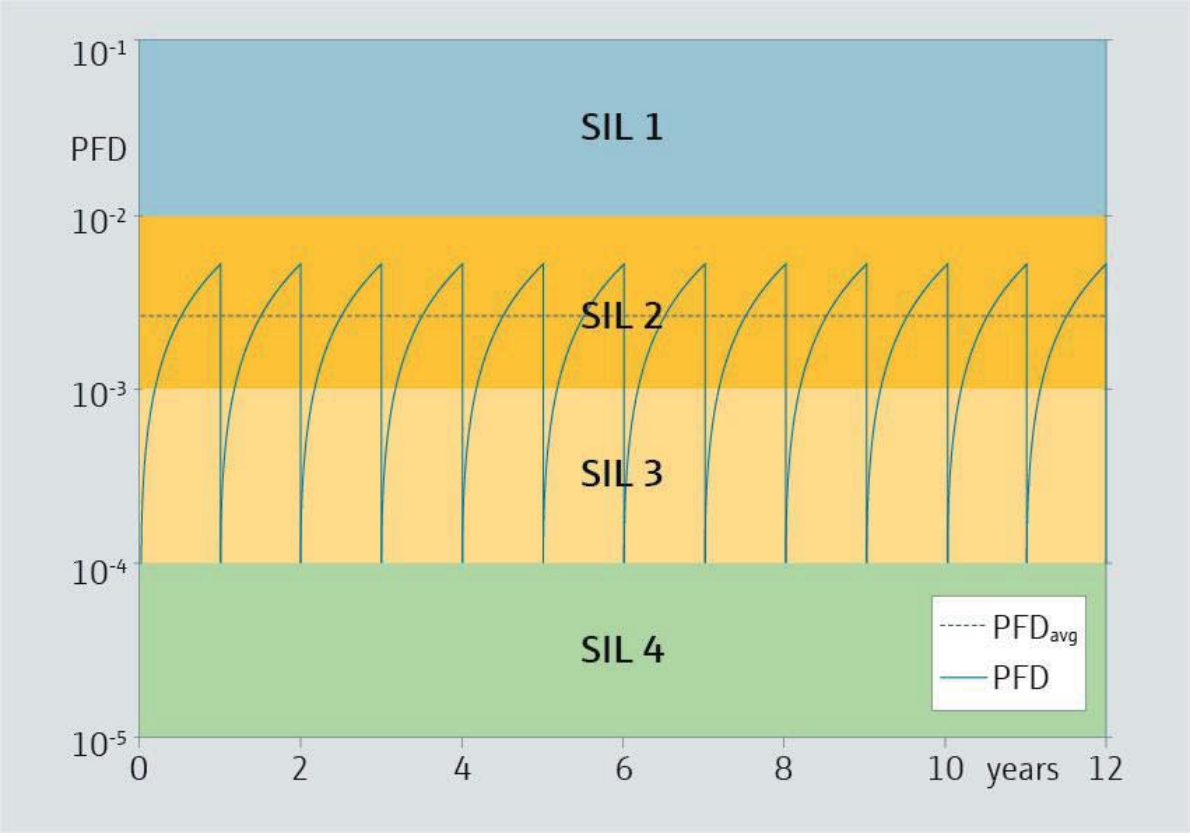


Figure 7: Ideal proof test

5.4.4 Proof Test Coverage

The effectiveness of a proof test is expressed by the "Proof Test Coverage" (PTC). This describes how close a safety system can be brought to the "as new state". A proof test includes testing all safety functions. In multiple channel safety instrumented systems, each channel has to be tested separately.

The Proof Test Coverage has a great influence on the test result, and consequently, the value of PFD_{avg} and the achievable SIL. PTC depends on the test sequence and is specified in the functional safety manuals. If PTC decreases, the untested proportion of the SIS increases over time. This is shown in the following figures for different values of the PTC (99% - complex test procedure, 90%, 50% - simple test procedure) and a proof test interval of T_1 = 1 year.

To calculate the average probability of failure, the approximation is used from the following formula:

$$PFD_{avg} = \lambda_{DU} \cdot \left(\frac{T_1}{2} + \mathrm{MTTR}\right) \cdot \mathrm{PTC} + \lambda_{DU} \cdot \left(\frac{T}{2} + \mathrm{MTTR}\right) \cdot (1 - \mathrm{PTC}) + \lambda_{DD} \cdot MTTR$$

$$\boldsymbol{PFD_{avg} = \frac{1}{2}\lambda_{DU} \cdot T_1 \cdot \mathrm{PTC} + \frac{1}{2} \cdot \lambda_{DU} \cdot \mathrm{T} \cdot (1 - \mathrm{PTC})}$$

(T total operating time of the system, here 12 years)

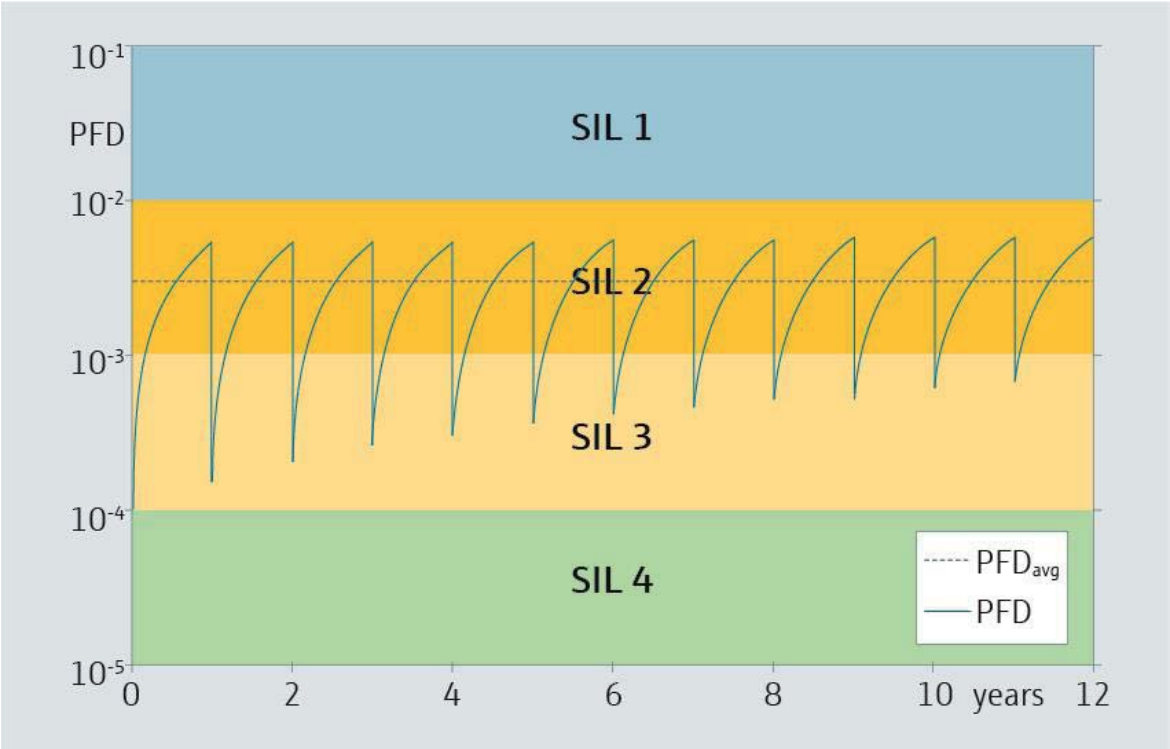


Figure 8: Proof test with PTC = 99%

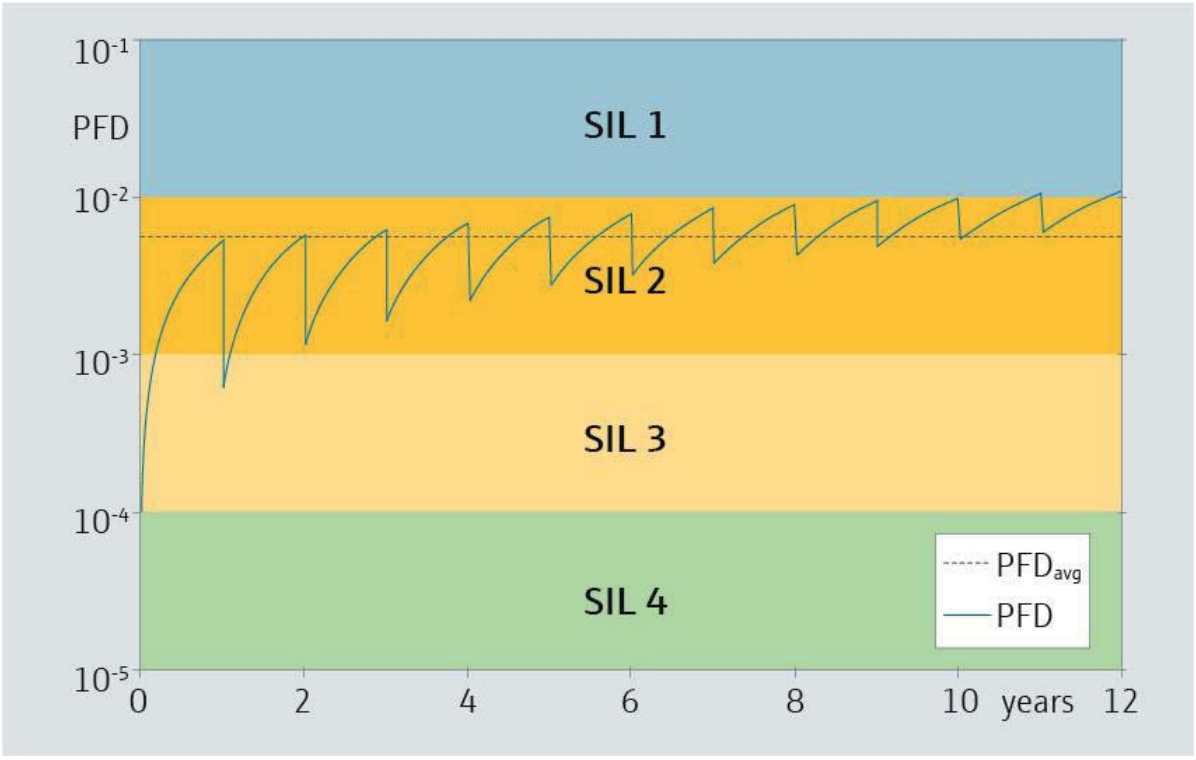


Figure 9: Proof test with PTC = 90%

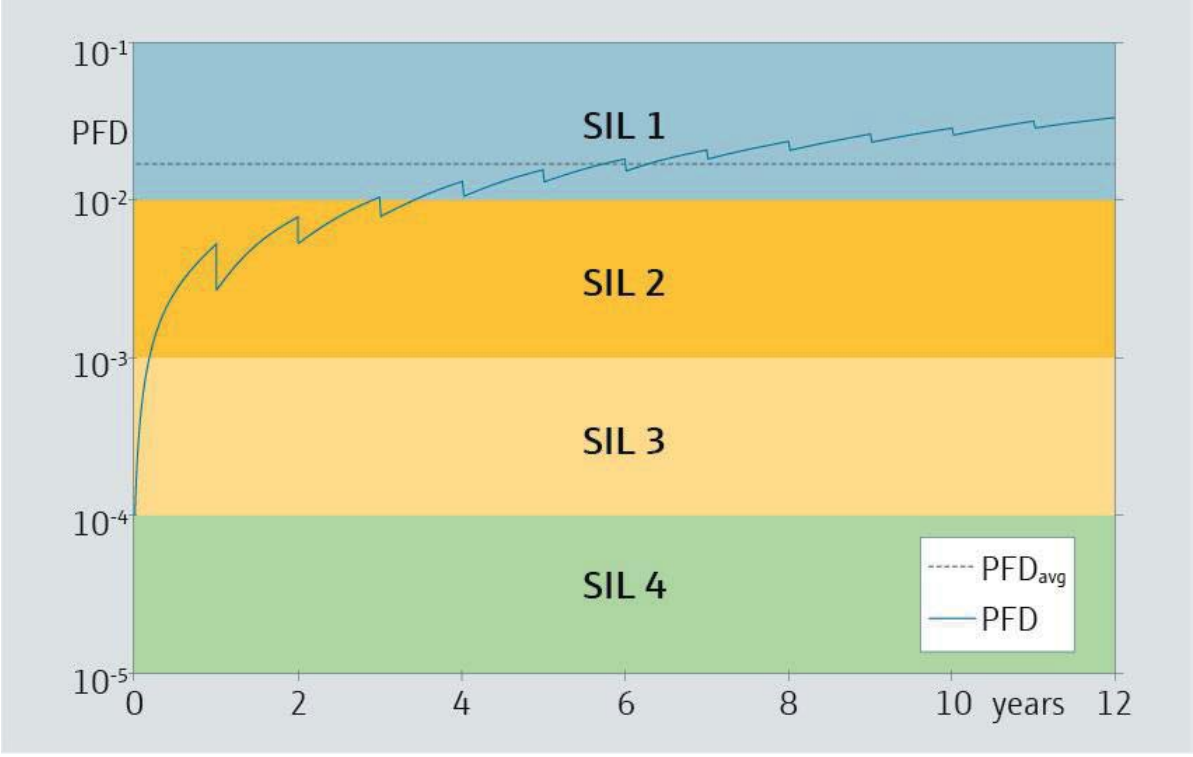


Figure 10: Proof test with PTC = 50%

In the case of a simple proof test (PTC = 50%) it may be useful at regular intervals (e.g. every 4 years) to introduce a more complex proof test. The result then looks as shown in Figure 11.

It is derived from the following formula for the average probability of failure with two Proof Test Coverages and different proof test intervals.

$$PFD_{avg} = \frac{1}{2} \cdot \lambda_{DU} \cdot T_1 \cdot PTC_1 + \frac{1}{2} \cdot \lambda_{DU} \cdot T_2 \cdot (1 - PTC_1) + \frac{1}{2} \cdot \lambda_{DU} \cdot T \cdot (1 - PTC_2)$$

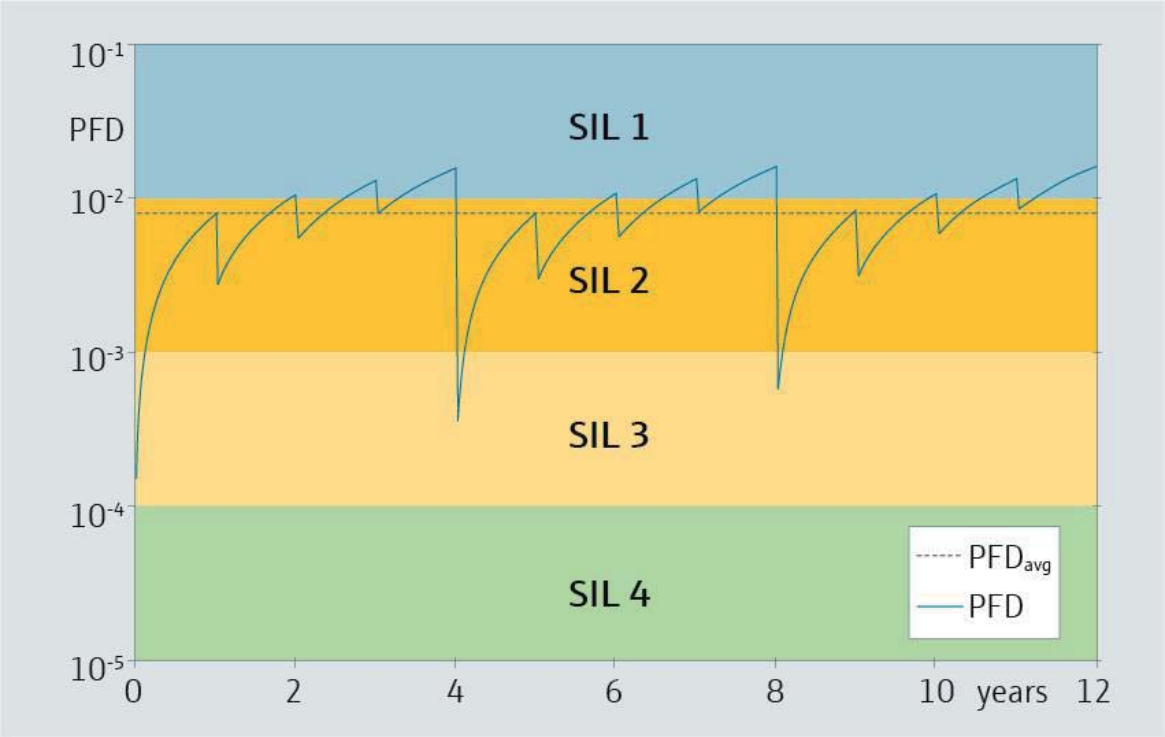


Figure 11: Proof test with PTC 50% (annually) and 99% (every 4 years)

This leads to an improvement of PFD_{avg} with reasonable overhead.

5.5 Repair

Repair means a 1:1 replacement of components. It brings a device in an "as new" condition or as close as practical to this condition (source: IEC 61508-4:2010, Section 3.8.5).

A repair of safety-related components can be carried out by qualified personnel of the end user or a service technician of the manufacturer. Repair of defined components may be done following the manufacturer's repair instructions. Only original spare parts must be used.

If a device was operated in a safety-related application and a device error cannot be excluded, the replaced component must be sent to the device manufacturer for fault analysis.

For repairs to safety-related devices the following cases and procedures can be distinguished (see VDI/VDE 2180, Part 3, Section 2.2.3.):

1. Repair of a single-channel safety instrumented system:
   - One fault leads to failure of the safety instrumented system.
   - The repair must be done immediately after detection of the fault.
   - During repair, the plant must be shut down or appropriate actions taken to achieve or maintain the safe state.
2. Repair of a single fault tolerant, multichannel safety instrumented system:
   - After detection of a fault the process can be operated safely, while repairing the defective part. The designated repair time must be respected.
   - Otherwise, alternative measures must be taken.

5.6 Modification

Modifications are changes desired by the end user to already delivered and installed devices. Usually modifications on safety-related components are performed in the manufacturer's factory. Modifications to safety-related components at the end user's location are possible only after approval by the manufacturer. In this case, the modifications should be performed and documented by a qualified manufacturers' service engineer.

5.7 Useful lifetime

How long can a device be operated as part of a safety instrumented system? The useful lifetime depends on various factors.

During the useful lifetime, i.e. the time after early failures (burn-in) and before late failures (wear-out), the failure rate of a device can be regarded as constant (IEC 61508-4: 2010, section 3.6.16, Note 2). Most probabilistic assessments for failure behavior are based on this assumption.

Useful lifetime depends strongly on the device itself and its operating conditions (particularly temperature). Experience has shown that useful lifetime is often in the range of 8 to 12 years. However, it may be significantly less if devices are operated near their specification limits.

Longer useful lifetimes can be achieved by appropriate measures of the manufacturer and the operator (see DIN EN 61508-2:2011, Clause 7.4.9.5, Note 3, N3).

Measures taken by manufacturer:

- Appropriate equipment design (e.g. avoid aging critical components)
- Active fault behavior, i.e. errors should be detectable or devices should fail safety-related
- Device-specific maintenance guidelines

Measures taken by end user:

- Application-specific maintenance measures
- Reduction of critical application conditions (e.g. protection against environmental influences)
- Design of safety function so that equipment failures lead to a safe plant condition
- Verification by failure data recording

6 Appendix

6.1 References

6.1.1 Standards

Designation	Title
IEC 61508:1998	Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 1
IEC 61508:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems, Edition 2
IEC 61511-1:2016	Functional safety – Safety instrumented systems for the process industry sector
VDI/VDE 2180, Part 1 bis 6	Safeguarding of industrial process plants by means of process control engineering (PCE)

6.1.2 Relevant NAMUR recommendations

The following NAMUR recommendations are of relevance to practical implementation of functional safety. The list does not claim to be complete.

NAMUR recommendation	Title
NE 073	Phases accompanying documentation of safety-related process control equipment
NE 093	Verification of the Safety-Related Reliability of SIS based on Field Experience
NE 106	Test Intervals of Safety Instrumented Systems
NE 126	Provisions to Safeguard Existing Standards for Process Control System Safety Equipment
NE 130	“Prior use”-Devices for Safety Instrumented Systems and simplified SIL Calculation
NE 142	Functional Safety of Electrotechnical Elements
NE 154	Functional Safety in Batch Processes

6.1.3 Selected Internet Resources

The following table lists some information on functional safety with no claim to completeness.

Source	Contents
www.endress.com/SIL	Overview of SIL evaluated Endress+Hauser products with certificates and Functional Safety Manual for download
www.iec.ch/functionalsafety/	Web site of the International Electrotechnical Commission (IEC) for functional safety
www.vde.com/funktionale-sicherheit	Functional Safety website of VDE
www.61508.org	Homepage of “61508 Association“

6.2 Calculations according to IEC 61508:2010

In the following the formulas for PFD_{avg} and PFH for different architectures of subsystems based on IEC 61508-6:2010 are specified.

Input values:

λ_{DD}	Detected dangerous failure rate
λ_{DU}	Undetected dangerous failure rate
MRT	Mean repair time (hour)
MTTR	Mean time to restoration (hour)
T_1	Proof test interval (hour)
T_2	Interval between demands (hour)
β	The fraction of undetected failures that have a common cause. A method for determining β is specified in IEC 61508-6 Annex D. In practice, the value of β is usually in the range 5% to 10%.
β_D	The fraction of detected failures that have a common cause.
PTC	Proof Test Coverage

Terms:

$$\lambda_D := \lambda_{DU} + \lambda_{DD}$$

$$t_{CE} := \frac{\lambda_{DU} \cdot PTC}{\lambda_D} \cdot \left(\frac{T_1}{2} + MRT \right) + \frac{\lambda_{DU} \cdot (1 - PTC)}{\lambda_D} \cdot \left(\frac{T_2}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

$$t_{GE} := \frac{\lambda_{DU} \cdot PTC}{\lambda_D} \cdot \left(\frac{T_1}{3} + MRT \right) + \frac{\lambda_{DU} \cdot (1 - PTC)}{\lambda_D} \cdot \left(\frac{T_2}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

$$t_{G2E} := \frac{\lambda_{DU} \cdot PTC}{\lambda_D} \cdot \left(\frac{T_1}{4} + MRT \right) + \frac{\lambda_{DU} \cdot (1 - PTC)}{\lambda_D} \cdot \left(\frac{T_2}{4} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

$$CCF := \beta \cdot \lambda_{DU} \cdot PTC \cdot \left(\frac{T_1}{2} + MRT \right) + \beta \cdot \lambda_{DU} \cdot (1 - PTC) \cdot \left(\frac{T_2}{2} + MRT \right) + \beta_D \cdot \lambda_{DD} \cdot MTTR$$

Meaning of terms:

t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures
t_{G2E}	Voted group equivalent mean down time (hour) for 1oo3 architecture
CCF	Common Cause Factor

Calculation formulas for PFD_{avg}:

$$PFD_{1oo1} := (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE}$$

$$PFD_{1oo2} := 2 \cdot ((1 - \beta) \cdot \lambda_{DU} + (1 - \beta_D) \cdot \lambda_{DD})^2 \cdot t_{CE} \cdot t_{GE} + CCF$$

$$PFD_{2oo2} := 2 \cdot (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE}$$

$$PFD_{2oo3} := 6 \cdot ((1 - \beta) \cdot \lambda_{DU} + (1 - \beta_D) \cdot \lambda_{DD})^2 \cdot t_{CE} \cdot t_{GE} + CCF$$

$$PFD_{1oo3} := 6 \cdot ((1 - \beta) \cdot \lambda_{DU} + (1 - \beta_D) \cdot \lambda_{DD})^3 \cdot t_{CE} \cdot t_{GE} \cdot t_{G2E} + CCF$$

Calculation formulas for PFH:

$$PFH_{1oo1} := \lambda_{DU}$$

$$PFH_{1oo2} := 2 \cdot \left(\left(1-\beta\right) \cdot \lambda_{DU} + \left(1-\beta_D\right) \cdot \lambda_{DD} \right) \cdot \left(1-\beta\right) \cdot \lambda_{DU} \cdot t_{CE} + \beta \cdot \lambda_{DU}$$

$$PFH_{2oo2} := 2 \cdot \lambda_{DU}$$

$$PFH_{2oo3} := 6 \cdot \left(\left(1-\beta\right) \cdot \lambda_{DU} + \left(1-\beta_D\right) \cdot \lambda_{DD} \right) \cdot \left(1-\beta\right) \cdot \lambda_{DU} \cdot t_{CE} + \beta \cdot \lambda_{DU}$$

$$PFH_{1oo3} := 6 \cdot \left(\left(1-\beta\right) \cdot \lambda_{DU} + \left(1-\beta_D\right) \cdot \lambda_{DD} \right)^2 \cdot \left(1-\beta\right) \cdot \lambda_{DU} \cdot t_{CE} \cdot t_{GE} + \beta \cdot \lambda_{DU}$$

6.3 Overview calculation tools

The following table lists some software tools for calculation of safety instrumented functions. These tools are liable to costs. The tool manufacturer is liable for the correctness of calculations carried out.

Tool name	Provider
exSILentia / SILver (www.exida.com/exSILentia/)	exida.com
SILCaS (silcas-tool.com/)	ProSolTech (Distributor) (www.prosoltech.com/)
SILence (www.hima.de/Produkte/silence/Silenceregistrierung.php)	HIMA
TRAC (www.abbconnectit.com/trac/)	ABB Engineering Services

7 Glossary

Term	Explanation
Device type A	Devices where the failure rates and failure modes of all components are clearly known in all cases.
Device type B	Devices where the device behavior in case of error is not fully determinable (e.g. programmable or configurable devices).
Failure rate λ	Probability of failure of a component (e.g. resistor, µC). The failure rate unit is FIT (Failure In Time, 1 FIT = 10^{-9} / h).
FMEDA (Failure Modes, Effects and Diagnostic Analysis)	Analytical method for electronic circuits and mechanics for the quantitative determination of failure modes and failure rates. Failure rates: ▪ λ_{SD}: Total failure rate for safe detected failures ▪ λ_{SU}: Total failure rate for safe undetected failures ▪ λ_{DD}: Total failure rate for dangerous detected failures ▪ λ_{DU}: Total failure rate for dangerous undetected failures
Functional Safety	Part of the overall system safety which depends on the correct functioning of safety-related systems to reduce risk. Functional safety is achieved when each safety function is performed as specified.
Hardware Fault Tolerance (HFT)	A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.
Hardware Safety Integrity	Part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure.
High demand mode	Mode of operation where the safety function is frequently performed on demand, in order to transfer an equipment under control into a specified safe state, and where the frequency of demands is greater than once a year.
Low demand mode	Mode of operation where the safety function is only performed on demand, in order to transfer an equipment under control into a specified safe state, and where the frequency of demands is no greater than once a year.
Measurement error of a standard device	Specified device accuracy without consideration of safety concerns.
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PFD_{avg}	Average probability of dangerous failure of a safety function at low demand mode of operation.
PFH (probability of failure per hour)	Failure probability of a safety function at high or continuous mode of operation.

Term	Explanation
Proof test interval (T_1)	Time interval between periodic tests performed to detect dangerous hidden failures in a safety-related system.
Random failure	Error with not reproducible cause. Its occurrence is not predictable.
Redundancy	Using multiple elements or systems to perform the same function. Redundancy can be implemented by identical elements (homogeneous redundancy) or with different elements (diverse redundancy).
Residual risk	Remaining risk despite protective measures.
Risk	Combination of the probability of occurrence of harm and the severity of that harm.
Safe Failure Fraction (SFF)	Ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.
Safe state	Status of a system when safety is achieved.
Safety function	Function which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event.
Safety Instrumented System (SIS)	Instrumented system used to implement one or more safety (instrumented) functions.
Safety Integrity Level (SIL)	Four discrete levels (SIL 1 to SIL 4). The higher the SIL of a safety-related system, the lower the probability that the system does not perform the required safety function.
Safety Life Cycle	Description of all necessary activities in the implementation of safety-related systems from the concept phase to the decommissioning.
Safety measuring error	Changed measurement accuracy for safety-related functions compared to the specification for standard operating accuracy.
Safety-related system	System which performs safety functions in order to reach or maintain a safe state for equipment under control.
Software Safety Integrity	Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of software related failures
Systematic fault	Error with generally identifiable and reproducible cause.
Systematic Safety Integrity	Part of the safety integrity of a safety-related system relating to random hardware failures in a dangerous mode of failure.
Useful lifetime	Time between early failures (burn-in) and before late failures (wear-out) where the failure rates of components can be considered constant.

Term	Explanation
Voting MooN	Typical channel architectures: ▪ 1oo1: Single-channel system. A failure of the device leads to loss of the safety function. ▪ 1oo2: Dual-channel system. A failure of both devices leads to loss of the safety function. ▪ 2oo2: Dual-channel system. A failure of one devices leads to loss of the safety function. ▪ 2oo3: Three-channel system. A failure of two devices leads to loss of the safety function.

Contact

Endress+Hauser GmbH+Co. KG
Hauptstraße 1
79689 Maulburg
Germany

Tel +49 7622 28 0
Fax +49 7622 28 1438
info@pcm.endress.com
www.pcm.endress.com

WP01032F/00/EN/01.16

Endress+Hauser

People for Process Automation