Functional Safety – SIL

Safety Instrumented Systems in the Process Industry

Endress+Hauser

People for Process Automation


People for Process Automation
People for
Process
Automation

Foreword

"Functional safety" has come into focus since the publication of the IEC/EN 61508 and IEC/EN 61511 standards. The term SIL (safety integrity level) is used frequently in this context.
But what is SIL?

This brochure is intended to provide an initial overview of "functional safety". The content of the brochure is essentially limited to areas and applications where Endress+Hauser products are used.

Those in need of more detailed information can find it by looking into the associated literature and the pertinent rules and regulations. Therefore, the information in this brochure should be considered as examples and cannot be used for a specific design.

You can find detailed information and SIL certifications for Endress+Hauser products at

www.endress.com/SIL.

Table of contents

1. Danger and risk

We are constantly exposed to a wide variety of hazards during our day-to-day lives. The broad variety of these hazards extends to major disasters, severe injuries or damage that can affect the health of people, the environment and property. It is not always possible to eliminate a danger and the associated risk. As a result, society has to live with the dangers of earthquakes, floods and other disasters. While only limited protection from such events is possible, protective measures for the dire effects of these events can be considered in great detail.

Lawmakers in various areas have created laws and other legal regulations that define the respective requirements regarding safety.

In Europe, the European Commission has published corresponding directives for protecting people and the environment. In Germany, professional associations and other institutions as a legal means of accident insurance have issued and continually monitor regulations. Today, international regulations specify requirements related to protecting the health of people and the environment for systems and products. They define specific product properties for achieving the corresponding safety goals.

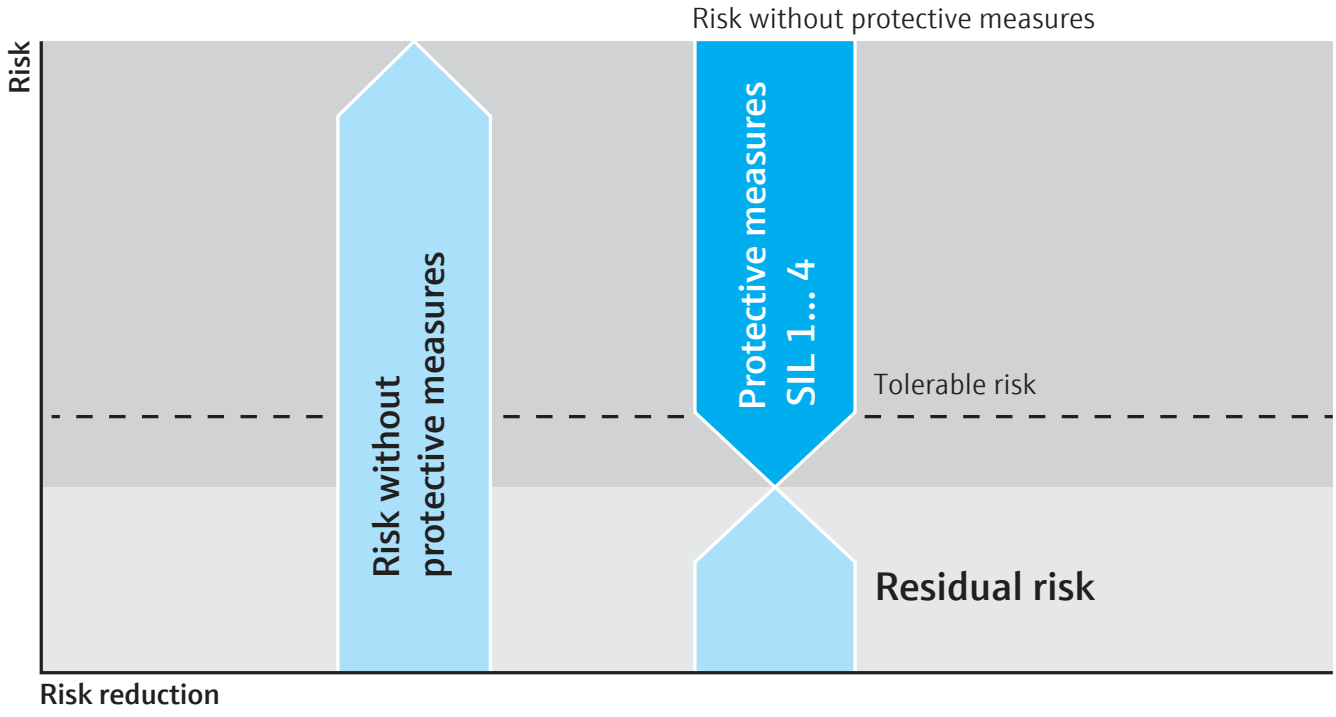
Defining risk:

Risk = The probability that a dangerous event will occur × The extent of damages (costs) from a dangerous event.

The acceptable residual risk depends on various factors:

- Country/Region
- Society
- Laws
- Costs

The acceptable residual risk has to be estimated on a case-by-case basis. It has to be acceptable to society.



2. Directives and standards for functional safety

The catalyst was an accident releasing toxic gas in the city of Seveso in Northern Italy in July 1976. Since then, EC Directive 96/82/EC has defined the legal stipulations for facilities posing a significant potential hazard (Seveso II Directive). In Germany, this directive was implemented through the Hazardous Incidence Ordinance in the Federal Immission Control Act and the Ordinance on Industrial Safety and Health (12th BImSchV and BetrSichV).

In this context, a distinction must be made between product safety in a general sense and products developed and designed specifically for safety-related functions. For the latter, DIN EN 61508 is indispensable, as it has since come to define the state of the art of technology for functional safety.

It defines four safety levels: SIL 1 through SIL 4. IEC/DIN EN 61508 is a generic, i.e. application-independent, standard. It is a base standard, making it generally applicable for all electrical, electronic and programmable electronic systems (E, E, PES). It is the first set of rules and regulations globally published for safety functions in safety-critical applications.

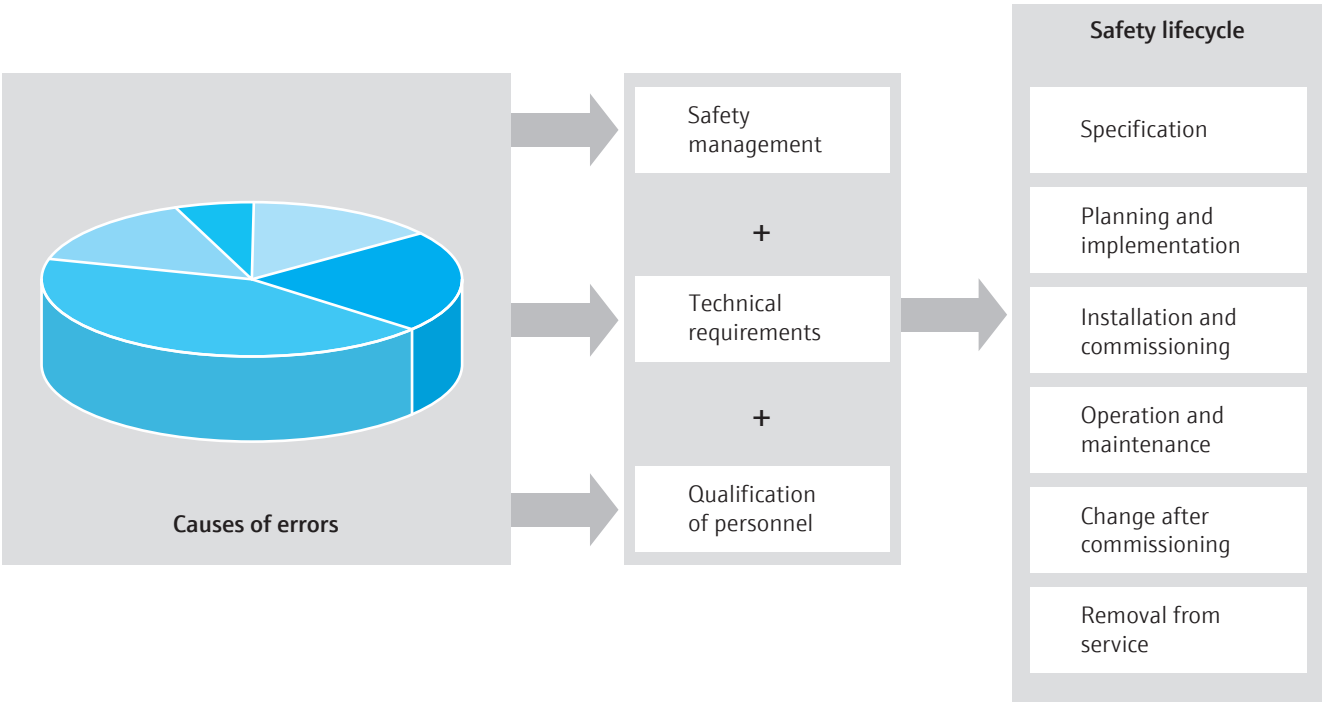
To whom do IEC/DIN EN 61508 and IEC/DIN EN 61511 apply? Hazard and risk analysis can be used to find all of the risks related to a system. This can be used to determine whether safety instrumented systems are required. Functional safety is used in the process industry where comparable safety systems with a corresponding standard were used previously. These kinds of products can be used in other systems with a similar safety risk. It is important to remember that the entire safety instrumented system with all of its components must be considered. In addition, IEC/DIN EN 61511 has been derived from IEC/DIN EN 61508 as a base standard for the process industry. Likewise, IEC/DIN EN 62061 was derived from it for the Machinery Directive and IEC/DIN EN 50156 was derived for furnace technology.

Changes in relation to the previous safety standards The requirements for safety-related systems are broken down in the IEC/DIN EN 61508 standard for functional safety. Sensors, control systems or actuators (final element) must have a SIL classification as defined by the standard. While purely qualitative consideration used to be typical for safety-related classification, the new standard requires quantitative consideration of the entire system and documentation for a corresponding functional safety management system. The user and monitoring organizations have to clarify which economically feasible measures have to be required. The objective is to prevent systematic errors in safety-related systems and to control random failures and limit the probability of dangerous failures (risk) in a defined way.

3. Lifecycle

Users of safety-related systems have to undertake suitable measures for analyzing and reducing risk throughout the entire lifecycle. The IEC/DIN EN 61508 standard prescribes certain steps for this:

- Defining and analyzing risks according to detailed probability of failure on demand reports for the entire safety circuit (loop) from the sensor to the control system to the final element (actuator) throughout the entire lifecycle.
- Determining and implementing the measures (management of functional safety).
- Use of suitable (qualified) equipment.



4. Risk reduction

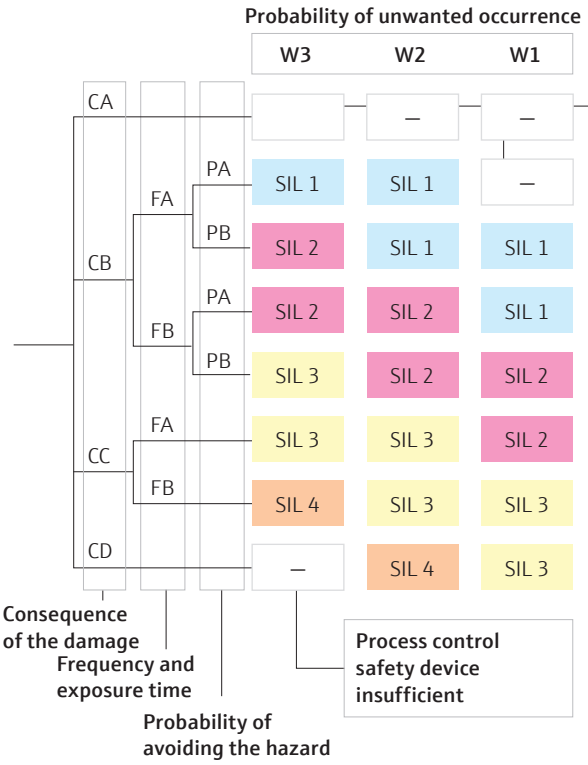
Each technological application also means a safety-related risk. The greater the hazard to people, the environment or property, the more countermeasures are necessary to minimize the risk. Industrial applications see many systems and machines with different hazard potential. In order to achieve the required level of safety for such systems, the safety-related parts for protective and safety systems have to work correctly and behave so that the system remains in a safe state or moves to a safe state in case of error.

The objective of IEC EN 61508 is to prevent or control errors in safety-related systems and to limit the probability of dangerous failures in a defined way. Quantitative documentation is required for any residual risk that remains. The risk reduction required is achieved by combining all of the protective measures. The residual risk should not exceed the tolerable risk. Finally, the plant operator must bear and accept the remaining residual risk.

5. Determining the required SIL

Different systems cause different risks. As a result, the requirements for the failure safety of safety instrumented systems (SIS) also increase as risk increases. The IEC/DIN EN 61508 and IEC/DIN EN 61511 standards define four different safety levels that describe the measures for controlling risk in these components. These four safety levels are called safety integrity levels, or SIL.

The higher the numerical value of the safety integrity level (SIL), the greater the reduction in risk. This means the SIL is the dimension for the probability that the safety system can correctly fulfill the required safety functions for a specific time frame. The average probability of failure (PFD or PFH) decreases by a factor of 10 per safety level.



Reference: IEC 61511

No safety instrumented system
(e.g. technical measures)

Consequence of the damage

CA Slight injury to one person or minor harmful environmental effects, such as those not covered by the Hazardous Incidence Ordinance.

CB Severe, irreversible injury to one or more persons or the death of one person or temporary, large-scale harmful environmental effects such as those denoted by the Hazardous Incidence Ordinance.

CC Death of several persons or persistent, large-scale harmful environmental effects, such as those denoted by the Hazardous Incidence Ordinance.

CD Catastrophic consequences, death of large numbers of people.

Frequency and exposure time

FA Rare to more often

FB Frequent to permanent

Probability of avoiding the hazard

PA Possible under certain circumstances

PB Hardly possible

Probability of unwanted occurrence

W1 Very slight

W2 Slight

W3 Relatively high

The SIL attained is determined using the following characteristic quantities:

- Probability of dangerous failures of a safety function (PFD or PFH),
- Hardware fault tolerance (HFT),
- Safe failure fraction (SFF),
- Type of the components (Type A or Type B),
- Proof test interval (recurrent function test),
- Useful lifetime

6. Operating modes: Low demand and high demand

Two operating modes are used when classifying the SIL of equipment: Low demand mode and high demand mode.

Low demand mode For low demand mode, it can be assumed that the safety system is not required more than once per year. In this case, the SIL value is derived from the PFD value (probability of failure on demand). Low demand mode is typical in the process industry.

Low demand mode

Safety integrity level	**PFD** (average failure probability of the safety function with low demand)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

High demand mode For high demand mode, it can be assumed that the safety function is required continuously or once per hour on average. High demand mode is typical in systems or machines where constant monitoring is required (manufacturing industry).

High demand mode

Safety integrity level	**PFH** (probability of a dangerous failure per hour)
SIL 4	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-6}$ to $< 10^{-5}$

7. Which devices can be used for which SIL?

In order to attain a safety integrity level (SIL 1 to SIL 4), the entire SIS has to meet the requirements for systematic errors (software) and random errors (hardware). This means the result when calculating the safety circuit has to match the required SIL. Normally this depends on the structure and architecture of the safety device. As a result, SIL 2 equipment in redundant voting structures can be used in SIL 3 systems. Due to the redundant structure of the system using equal SIL 2 equipment, in a homogeneous redundancy with regard to systematic errors the software has to meet SIL 3.

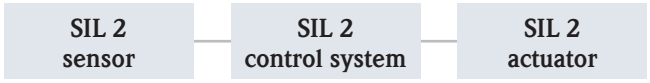
Types of errors Within a safety circuit, there is a distinction between systematic and random errors. In order to meet the required SIL, both of the respective error types have to be considered.

Random errors Random errors result from faults in the hardware and normally only occur during operation. The errors and the associated failure probability can be calculated.
The calculations are made for individual components at the component level. This provides the PFD value and forms the basis of the calculation for determining the SIL value.

Systematic errors Systematic errors are typically errors in development, design or project configuration. The largest portion of systematic errors normally occurs in the device software. In order to meet the requirement for a specific SIL (e.g. SIL 3) for systematic errors, the entire system has to be designed to SIL 3 accordingly. Alternatively, this can be achieved if two different devices (diverse redundancy), or devices with different technology are used.

Calculating the safety function Architecture also has to be considered when designing and calculating a safety circuit. You must determine if you are dealing with a single-channel or multichannel system. In order for a system to actually meet the requirements for a required SIL, systematic errors have to be avoided using safety management corresponding to the SIL. The examples listed here are shown in a simplified manner and cannot cover all applications. For example, in Germany VDE/VDI 2180 Part 4 provides important support along with the simplified approximation formulas for the must commonly used voting structures.

Single-channel architecture

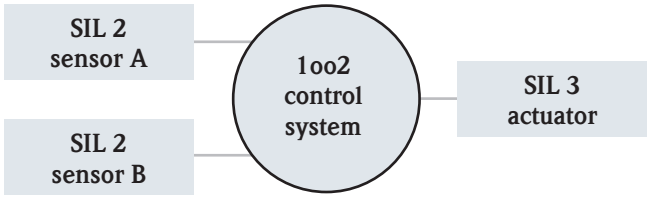


For a single-channel structure, the addition of the PFD or PFH values of individual components has to be taken into account to determine the safety integrity level (SIL) of the system. This is the only way to ensure that the entire safety loop meets the requirements for the required SIL.

Important:

The lowest SIL of the subsystems (sensor, control system, actuator) determines the safety integrity level for the entire system.

Two-channel architecture



Determining the PFD or PFH for multichannel architecture is more complicated. You can find simplified approximation formulas for calculating the PFDav in VDI/VDE 2180 Part 4.

Source
IEC/DIN EN 61508 Part 1 – Part 7 | IEC/DIN EN 61511 Part 1 – Part 3 | VDI/VDE 2180

8. Characteristic data

Safety integrity of the hardware (HFT, SFF) The following characteristic quantities are additionally used for SIL classification:

- The hardware fault tolerance (HFT)
- The safe failure fraction (SFF)

The following tables show the relation.
A distinction is made between systems of Type A and systems of Type B in this context.

Systems of Type A A system can be considered Type A if the failure behavior at the components that are required for the safety function can be described in simple terms. These components include metal film resistors, transistors, relays, etc.

Systems of Type B All other systems are complex systems (Type B) if components are in use whose failure behavior is not fully known. These components include microprocessors and semi-conductor circuits.

The failure rates for components can be found in the relevant industrial databases (e.g. Siemens SN 29500).

Hardware fault tolerance (HFT) Hardware fault tolerance refers to the ability of a device to continue to carry out a safety function correctly when errors occur. A HFT of N means that N+1 faults can lead to the loss of the safety function.

Safe failure fraction (SFF) The safe failure fraction describes the percentage of non-hazardous failures. The higher the required SIL is, the higher the SFF has to be. The SFF for a system is determined based on the individual failure rates (λ values) of the individual components.

SFF – HFT – SIL – Type A, Type B

Safe failure fraction (SFF)	Hardware fault tolerance (Type A – simple equipment)			Hardware fault tolerance (Type B – complex equipment)		
	0	1	2	0	1 (0*)	2 (1*)
< 60 %	SIL 1	SIL 2	SIL 3	Not permitted	SIL 1	SIL 2
60% to < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% to < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

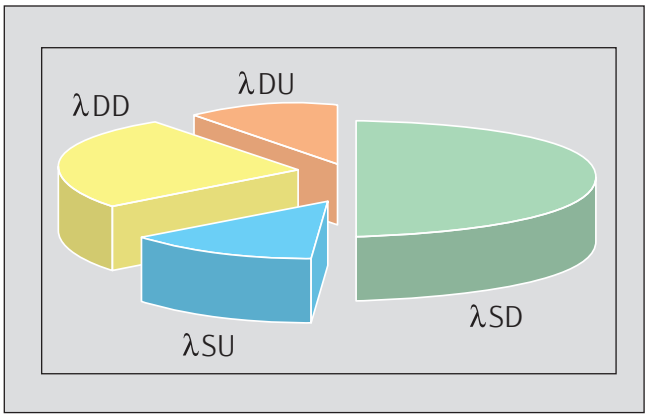
* With verification of the proven performance according to IEC/EN 61511 (only for SIL < 4)

Failure rate The ability of a system to detect failures and respond accordingly plays an important role. Therefore, a distinction is made between dangerous and safe failures as well as the possibility of discover these failures.

The failure rate due to failures is defined by the λ variable and is divided into four groups.

- λ SD = safe detected failure rate
- λ SU = safe undetected failure rate
- λ DD = dangerous detected failure rate
- λ DU = dangerous undetected failure rate

The dangerous, undetected failures (λDU) result in a undetectable loss of the safety function and have to be kept to a minimum using corresponding measures.
The unit used for λ values is FIT
(failure in time, 1 × 10-9 per h)

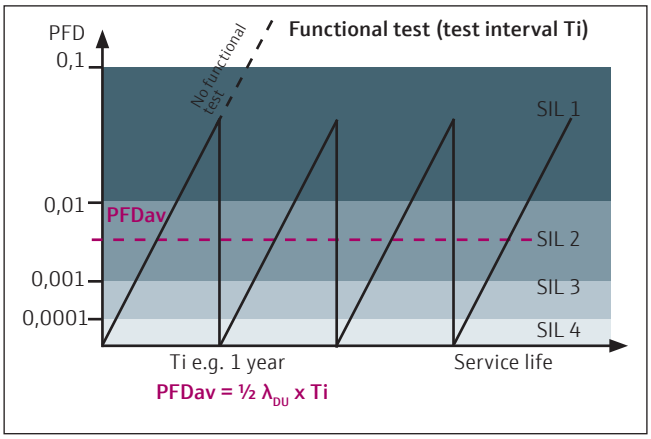


Note: IEC/DIN EN 61508-2:2011 Sec. 7.4.9.5 National footnote N3

The useful lifetime depends strongly on the device itself and its operating condition. After the useful lifetime life has elapsed, the probability of failure can increase with time (approx. 8 to 12 years).
A longer service life can be attained using corresponding measures from the manufacturer and operator (e.g. maintenance measures).

Test interval (Ti) The recurrent functional test (Ti) is used for detected dangerous failures. The safety function of a device must be tested at appropriate intervals. This value is integrated into the calculation of the PFD/PFH characteristic quantity and has to be chosen such that it is within the area required for the target SIL.

The operator is responsible for selecting the type of inspection and the intervals. Testing must be conducted such that it demonstrates the perfect functionality of the safety instrumented system in relation to all of the components. Recommendations for recurrent functional tests can be found in the safety manuals for the equipment.



Useful Lifetime The useful lifetime of safety devices depends mainly on the internal components and the operation conditions (e.g. ambient temperature, vibration, electric load). For electronic components the IEC 61508-2 specifies a typical range between 8-12 years, the ISO 13849-1 assumes a value of 20 years.

During the useful lifetime the components failure rates remain approximately constant. Beyond their useful lifetime the failure rates may increase due to wear out and ageing and the calculated PFDav values are no longer applicable. The user must either perform additional measures (e.g. reduce the proof test interval) or replace the safety device, to ensure that the required SIL rating is maintained. If ageing critical components (e.g. electrolyte capacitors) are avoided in safety devices by the manufacturer and the devices are used under normal ambient conditions the useful lifetime can be expected to correspond rather to the value indicated in the ISO standard than in the IEC standard.

9. Glossary

SIL (Safety Integrity Level)	The **safety integrity level (SIL)** is a benchmark for the safety integrity of a system. The safety integrity is the probability that the system will perform the required safety-related function under all defined conditions within a specified period of time. The SIL is broken down into four distinct levels, where safety integrity level 4 is the highest level of safety integrity and safety integrity level 1 represents the lowest level.
E/E/EPS	Electrical, electronic and programmable electronic systems
Functional safety	The ability of a system carrying out necessary actions to attain or maintain a defined safe state for systems under system control.
Failure rate λ	The failure rate of a system λ, generally divided into four groups by the type of failure: λSD = safe detected failure rate λSU = safe undetected failure rate λDD = dangerous detected failure rate λDU = dangerous undetected failure rate
FIT (Failure In Time)	Failures in the time (1×10^{-9} per h)
HFT (Hardware Fault Tolerance)	A hardware fault tolerance of N means that N+1 faults can lead to the loss of the safety function.
SFF (Safe Failure Fraction)	Portion of safe failures
PFD (Probability of Failure on Demand)	PFD is the probability of a failure of the safety function on demand in low demand mode (probability that the system fails with dangerous results upon demand).
PFH (Probability of Failure per Hour)	For high or continuous demand, the numerical measure of PFH is used, which specifies the probability of a failure of the safety function per hour (dangerous failure rate).
MooN (M out of N)	Architecture with M out of N channels. For instance, this means an architecture with 2 channels where each of the two channels can perform a safety function.
Proof test (Ti)	The proof test is a recurrent function test for detecting failures in an SIL system so that the system can be brought back to a "like-new" state.
SIS	Safety instrumented system

www.adresses.endress.com

CP010082/11/EN/02.13

Endress+Hauser

People for Process Automation