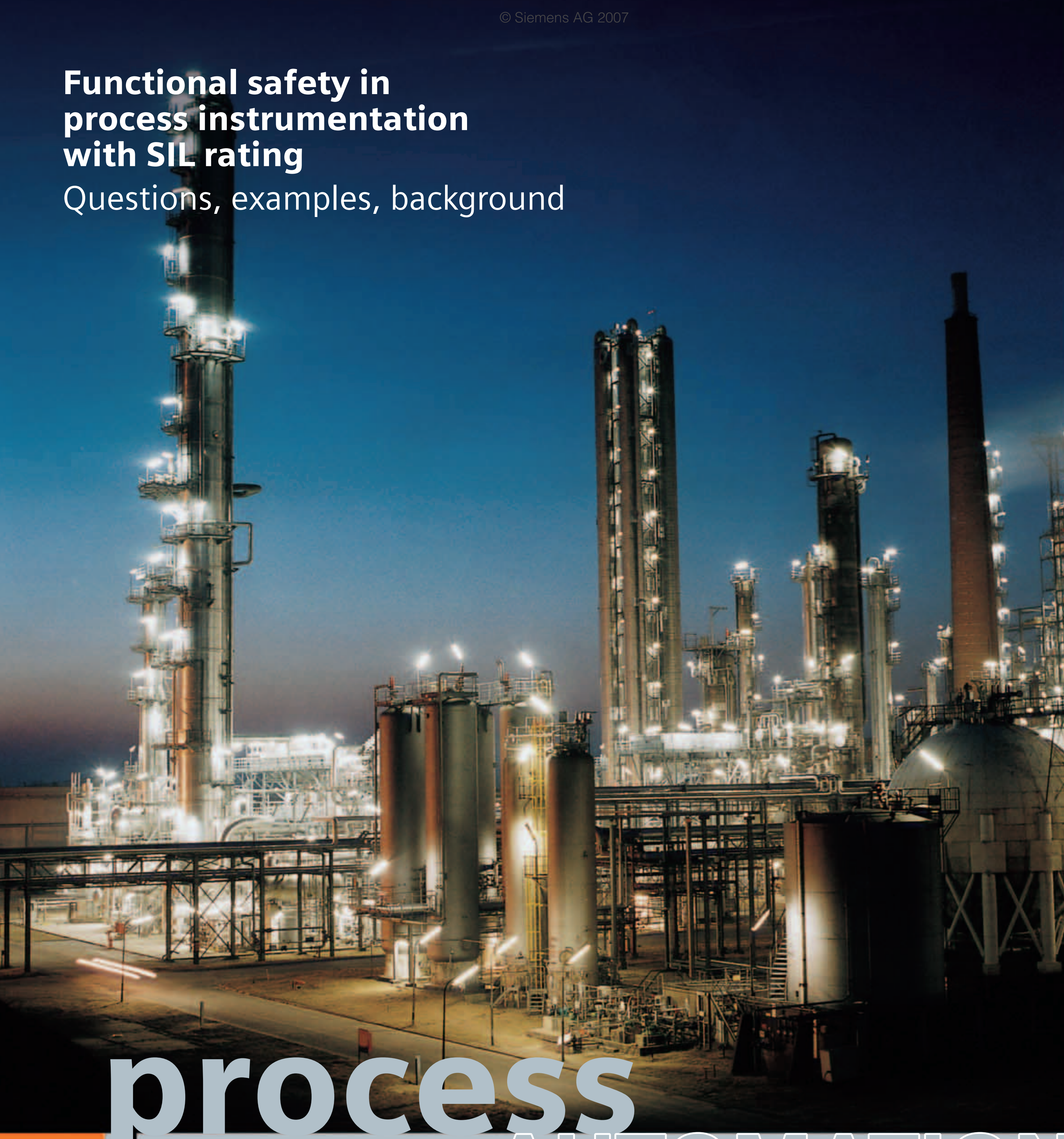
Functional safety in process instrumentation with SIL rating

Questions, examples, background



Brochure • April 2007

process AUTOMATION

SIEMENS

Since the rlease of IEC 61508, the topic of "Functional safety" in the process industry has come to the fore. Often, the expression SIL is used to reference this standard. But what exactly does SIL mean?

In this brochure, we will provide you with an introduction to the topic with emphasis on instrumentation for process engineering. We want to provide fundamental understanding without using the language of the standard. As a result, some descriptions may appear to experts to be too inexact or superficial.

This brochure can only be an introduction to the topic. If you require detailed information, you must refer to the corresponding literature and the relevant standards. The calculation examples shown here must therefore only be considered as the basic procedure, and cannot be applied to "real" calculations.

The information in this brochure has been produced to the best of our knowledge. However, errors may nevertheless have slipped in. Any resulting responsibility will therefore not be accepted.

Contents


Hazards and risks

In everyday life we are constantly exposed to many different hazards. The extent of these hazards extends up to major catastrophes which can have severe detrimental effects on health and the environment. We are not always able to avoid a hazard with its associated risks. For example, a high proportion of the world population lives with the hazards of earthquakes or flooding. There are no protective measures against the events themselves; however, protective measures do exist for the consequences of such events (e.g. dams or dikes, or buildings resistant to earthquakes).

Definition of a risk:

Risk = Probability of the occurrence of a hazardous event x consequences (costs) of a hazardous event

The accepted residual risk depends on the following factors:

- Region/country
- Society of the respective region/country
- Laws
- Costs

This accepted residual risk must be assessed individually. What is acceptable for one person may be unacceptable for someone else.

Reduction of risks

Every day hazards are assessed according to their risk level, and accepted or not. If someone plans a long journey, selection of the means of transport can influence the risk of an accident. The traveler can reduce the hazard to a residual risk which is acceptable for him. But there is always a residual risk.

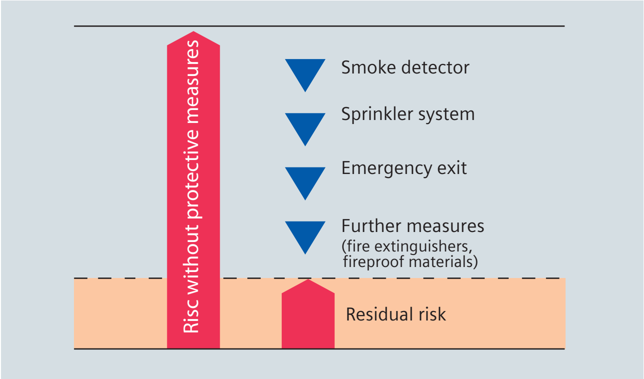
Protective measures

We can protect ourselves by reducing the probability of the occurrence of a hazard or by limiting its effect.

Our world is being increasingly dominated by electrical and electronic systems. These systems have increased the number of potential hazards we have, but these systems can also be used to prevent or mitigate the consequences of these hazards.

A simple example:

Various protective measures can reduce the risk of damage to a building from fire.

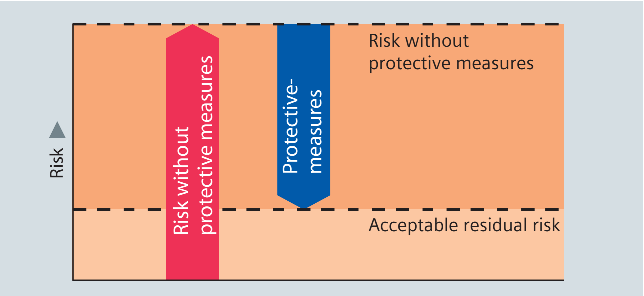


Appropriate emergency exits and escape routes can be provided when planning the building. Smoke detectors can trigger an alarm which signals the hazard to persons inside and outside the building. The installation of fire doors and the use of fireproof materials prevents further spreading of a fire.

Automatic sprinkler systems control the flames, and fire extinguishers are also available for fighting the fire. This example shows that there are many possibilities for reducing a risk. The protective measures are matched to the respective requirements, for the risks in a warehouse are different from those in home.

Protective measures in industry

The many machinery and plants in industrial use all have potential hazards. In order to protect personnel and the environment from hazard, as well as the machines and plants from damage, risks are determined and subsequently reduced by applying appropriate protective measures.



Representation of risk reduction

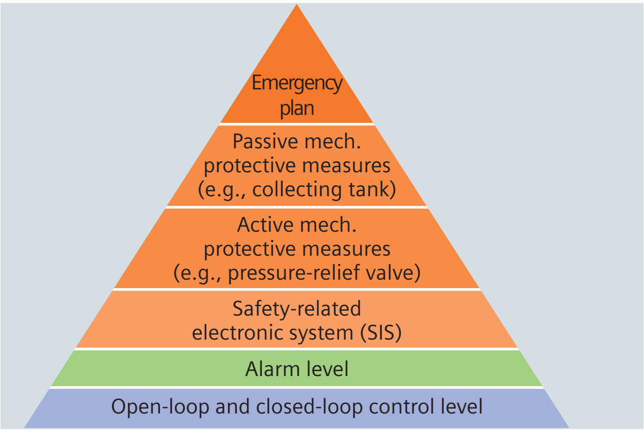
The measures required to reduce a risk can sometimes be very simple, but also extremely complex.

Examples:

- Structural measures (e.g. build concrete walls around production plants)
- Distribution of hazard
- Evacuation plans
- Safety-relevant control and protection equipment
- ... and many more

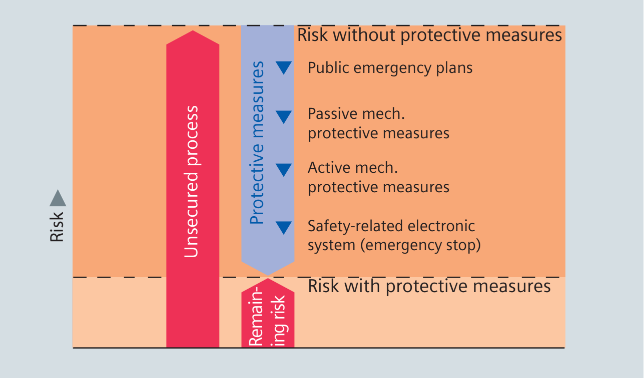
As shown by the example, measures that decrease the risk are partially attributed to completely different approaches. These approaches are also called layers of protection. These different layers of protection are structured hierarchically and are to be viewed independently of each other. If one layer fails, the next higher layer steps in to limit or avoid damage.

The layer of protection model below shows what types of protective measures typically exist:



The layers of protection must be independent in their function. Thus, devices for open-loop and closed-loop control technology from the lowest level should generally not be used simultaneously for safety applications of a higher level.

Overall risk reduction results from the measures of the individual layers of protection and must result in an acceptable residual risk.



Representation of risk reduction

The measures which are finally applied frequently depend on how high the residual risk may be while still being acceptable - and what costs are necessary to achieve this. Safety-relevant control and protection equipment can make a significant contribution to reducing risks in machinery and plants.

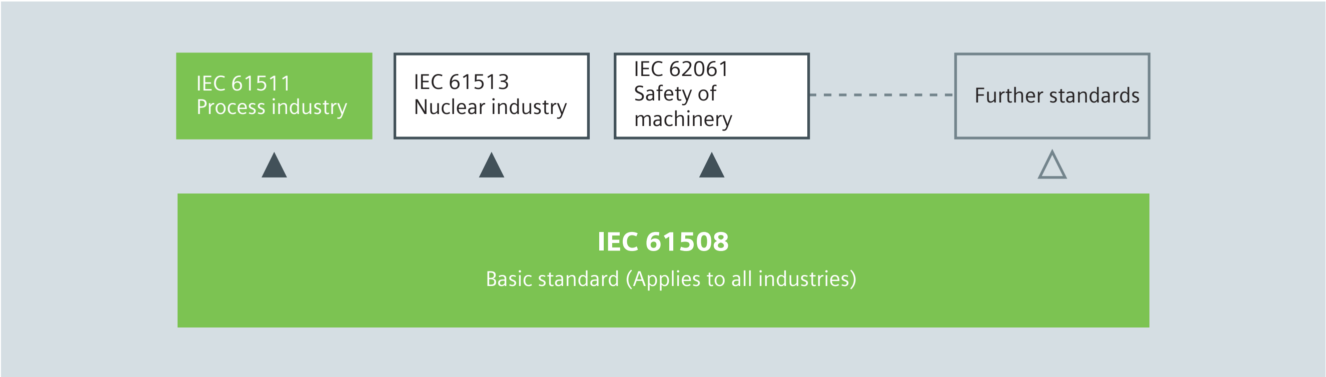
Automation engineering systems are increasingly handling safety-relevant tasks. For example, processes representing a hazard to mankind and the environment are monitored by safety systems. These access the process in the event of a fault, and can reduce the risk of a hazardous state. Functional safety is the correct functioning of such equipment.

Up to now, national standards have existed for the planning, construction and operation of safety instrumented systems. On the German market, for example, the manufacturers and owners of such plants could refer to the safety standards DIN/VDE 19250, DIN/VDE 19251 and DIN/VDE 801. The design of the safety-relevant equipment could be described using these standards and the requirement categories (AK 1-8).

Since many countries had different standards for the correct functioning of safety-relevant equipment, a globally applicable IEC basic standard for functional safety was adopted in 1998. A series of standards was derived from this, in which the organizational and technical demands placed on safety instrumented systems and their implementation were defined.

A uniform standard for plants in the process industry was adopted on August 1, 2004. The following two standards are of significance to process instrumentation:

- IEC 61508 (basic standard)
  Globally applicable as the basis for specifications, drafts and operation of safety instrumented systems (SIS).
- IEC 61511 (application-specific standard for the process industry)
  Implementation of IEC 61508 for the process industry



Standards used for functional safety

For whom is IEC 61508 relevant?

Based on a hazard and risk analysis, all hazards can be determined which result from a plant and its associated control systems. This determines whether a SIS is necessary to guarantee appropriate protection against possible hazards. If this is the case, the associated concepts must be appropriately incorporated in the development of this plant.

A SIS is only one possibility for coping with these hazards. IEC 61508 defines appropriate methods for achieving functional safety for associated systems.

What systems are affected by IEC 61508?

IEC 61508 must be applied to safety-relevant systems if these contain one or more of the following devices:

- Electrical equipment (E)
- Electronic equipment (E)
- Programmable electronic equipment (PE)

The standard covers potential risks caused by the failure of safety functions. Not covered are hazards resulting from the E/E/PE devices themselves, e.g. electric shock. The standard is generally applicable to safety-relevant E/E/PE systems, independent of their respective application.

Safety Instrumented System (SIS)

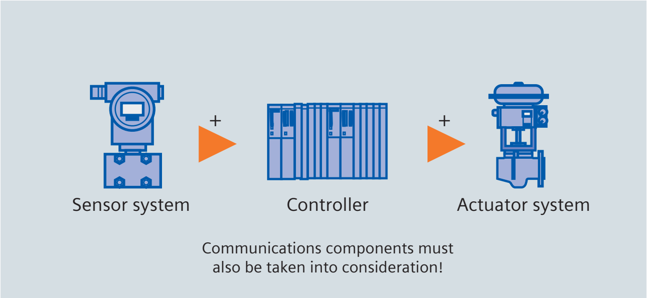
A Safety Instrumented System (SIS) is used to secure a hazardous process and to reduce the risk of an accident.

Process instruments are components of a Safety Instrumented System. This comprises the significant components of a complete safety-relevant process unit:

- Sensor
- Logic Solver
- Actuator

Components of an SIS

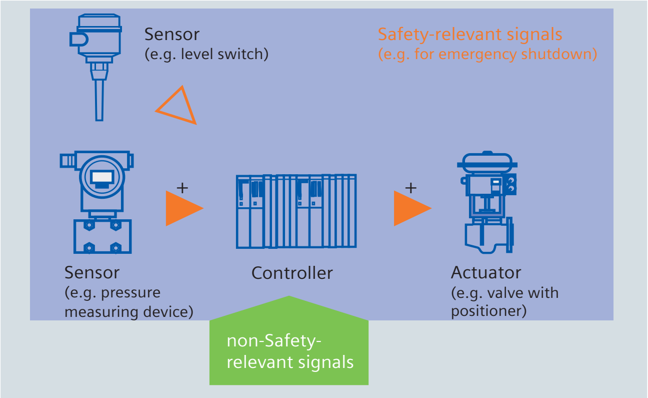
All units together constitute an SIS. In order to be able to evaluate the functional safety of an SIS, it is therefore necessary to consider the complete processing system (from sensor up to actuator).



Representation of an SIS

Several sensors, actuators, or control components can be used within an SIS.

It may also be the case that safety-relevant and non-safety-relevant components are connected together within a plant. However, only the safety-relevant components are considered for the SIS.



Signals to be processed in a plant

Determination of required SIL

Different risks originate from plants or plant components. As the risk increases, the demands made on the Safety Instrumented System (SIS) also increase. The standards IEC 61508 and IEC 61511 therefore define four different safety levels which describe the measures for handling the risks of these components. These four safety levels are the **safety integrity level (SIL)** defined by the standards.

The higher the number of the safety integrity level (SIL), the higher the reduction of the risk. The SIL is therefore a relative measure of the probability that the safety system can correctly provide the required safety functions for a specific period.

There are different approaches for determining the required SIL of a plant or plant component. The standards IEC 61508 and IEC 61511 (application of IEC 61508 for the process industry) include various methods for defining the SIL. Since the topic is extremely complex, only that necessary to obtain basic understanding is presented here.

A quantitative method

The risk of a hazardous process is determined by the probability with which a hazardous event could occur without existing protective measures, multiplied by the effect of the hazardous event. It is necessary to determine how high the probability is which can lead to a hazardous state. This probability can be estimated by applying quantitative risk assessment methods, and defined by a numeric limit.

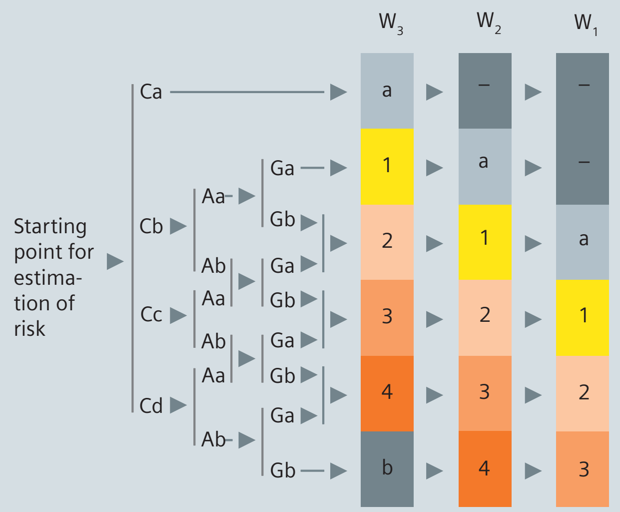
The probability can be determined by:

- Analysis of failure rates in comparable situations
- Data from relevant databases
- Calculation with application of appropriate prediction methods

The exact methods of calculation cannot be treated further here. If required, details can be found in IEC 61508 Part 5.

A qualitative method

The qualitative method is a simplified model which readily shows which SIL is required for which hazards.



a: no special safety requirements
b: a single SIS is insufficient
1, 2, 3, 4: safety integrity level (SIL)

Determination of SIL according to the "qualitative method"

Extent of damage	
C_a	Light injury of a person, small environmental damage
C_b	Severe injury or death of a person
C_c	Death of several persons
C_d	Death of very many persons

Duration of stay of a person in the dangerous area	
A_a	Seldom to frequent
A_b	Frequent to permanent

Aversion of danger	
G_a	Possible under certain conditions
G_b	Hardly possible

Probability of occurrence	
W_1	Very low
W_2	Low
W_3	Relatively high

A small example...

A new production facility needs to be build in a chemical plant.

The process used to produce the chemical product is the main factor determining the configuration of the facility. Since the operation of this type of facility can generally pose a risk to people and the environment, potentials risks and effects must be examined and adequate protective measures must be included in the project if necessary. For example, a separation column is considered as part of the plant.

A HAZOP analysis (Hazard and Operability Study) is created to assess the safety risks that can be mitigated by the operation of a separation column. The examination is compiled by various experts such as process technicians, production engineers, occupational health and safety experts, technicians, operating personnel, plant management, etc. in order to consider many different aspects of the safety risk of the facility. The various points of view are used to create a risk analysis (fault examination), which is in turn used to determine the protection or countermeasures that are needed.

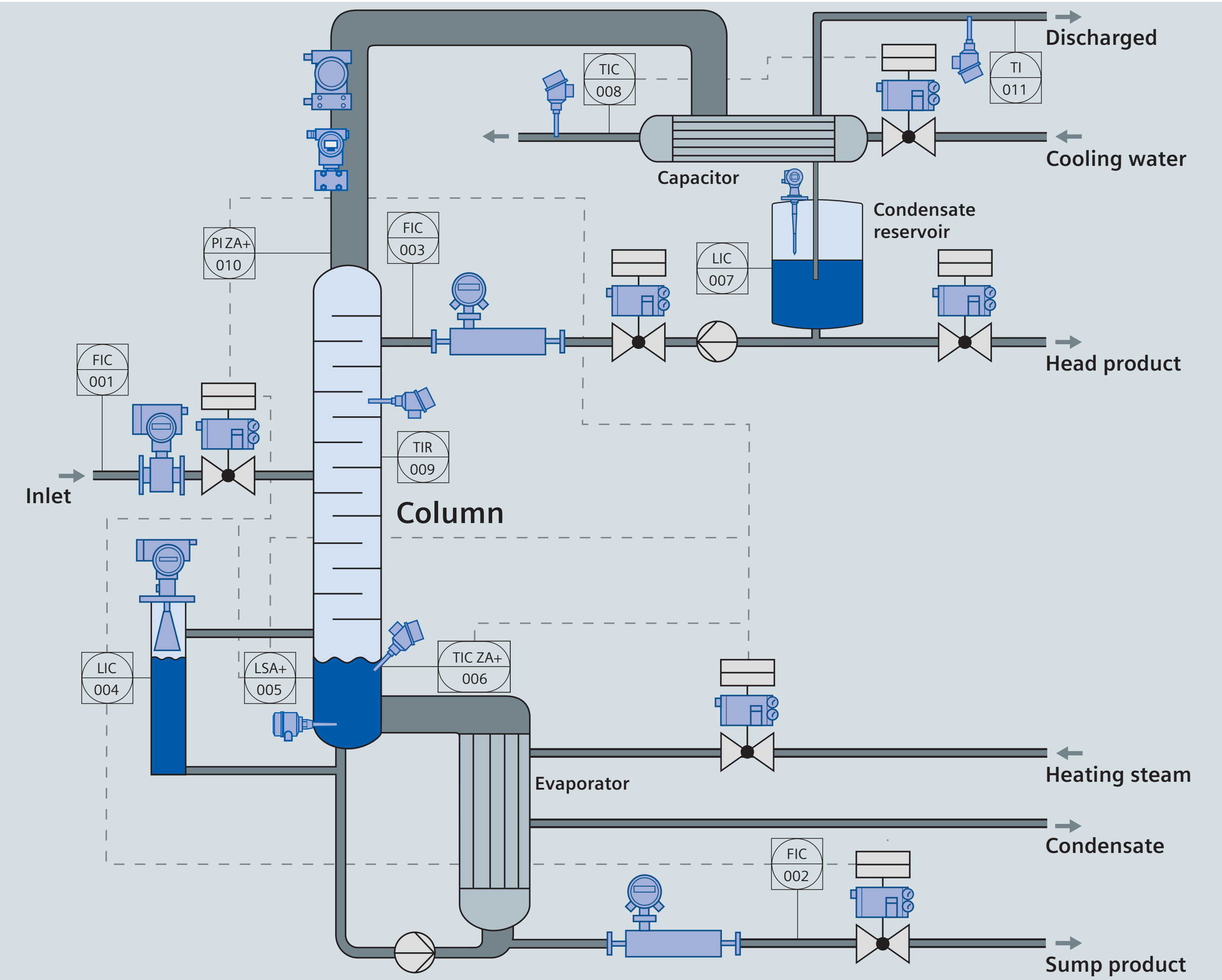


Diagram of the separation column

The risk analysis results in a fault examination, part of which is shown here:

No.	Fault	Cause(s)	Effect(s)	Countermeasures(s)
1	Wrong or contaminated input products into the column	Change in the mixture composition of the inflow from upstream parts of the plant	Temperature/pressure increase in the column	• Changes in the inflow composition do not take place suddenly but are instead gradual and are noted by the continuous quality analyses.
2	Power failure	Local or plant-side electrical defect	Breakdown of cooling and heating as well as the pumps and/or pressure and temperature increase	• All controls and instruments enter the safety mode. • The column automatically enters the safety mode (when heating is switched off and the infeed is closed).
3	Overfilling in the column sump	Failure of the fill level control LIC 004	Flooding of the lower column floors with the risk of destroying the floors	• Overfill safety LSA+ 005 closes heating steam and inflow valve
4	Overfilling of the condensate reservoir	Failure of the fill level control LIC 007	Flooding of the capacitor and loss of cooling power, temperature increase in the column	• See Temperature in the column too high
5	Temperature in the column too high	Loss of cooling water on the head capacitor	Pressure increase and penetration of the lower boiler steam into the discharged air, Instance A) With safety valve: Activation of the safety valve and substance release into the environment Instance B) Without safety valve: Exceeding of the maximum permissible pressure in the column with loss of integrity	• Pressure monitoring PI ZA+ 010 closes heating steam and inflow valves • Many temperature measurement points for the quick response of operating personnel in the case of an abnormal temperature increase.
6	Temperature in sump too high	Control errors in the heating steam supply line	Overheating of the sump product above the maximum permissible temperature, corrosion reaction with gas production, pressure increase above the maximum permissible storage pressure	• Temperature monitoring TIC ZA+ 006 closes heating steam

The measuring points "pressure monitoring at the column head" (010) and "temperature monitoring at the column floor" (006) were identified as being safety-relevant. The existence of a safety valve for pressure monitoring was emphasized in particular.

In connection with the diagram for determining the required SIL level on page 9, the corresponding classifications result for pressure and temperature monitoring in the separation column.

	Pressure monitoring		Temperature
	with safety valve	without safety valve	
Extent of damage	C_b	C_c	C_c
Length of stay in the hazard zone	A_b	A_b	A_b
Potential for aversion of hazard	G_b	G_b	G_b
Probability of event occurrence	W2	W2	W1
Safety Integrity Level	**SIL 2**	**SIL 3**	**SIL 2**

Low demand and high demand modes

Since applications in the process and production industries vary greatly, different demands are also placed on the SIS. For this reason, each of these industrial sectors has a different system in which the demand rate on the SIS is defined. A differentiation is made between the systems using the probability of SIS failure on demand (PFD).

Low demand

Mode with low demand rate on the safety system. There must not be a demand on the safety system more frequently than once per year.

SIL	PFD	Max. accepted failure of SIS
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	One hazardous failure in 10 years
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	One hazardous failure in 100 years
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	One hazardous failure in 1000 years
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	One hazardous failure in 10000 years

Failure limits for a safety function used in low demand mode

High demand

Mode with high demand rate or continuous demand on the safety system. The safety system works continuously or has a demand more frequently than once per year.

SIL	PFH (per hour)	Max. accepted failure of SIS
SIL 1	$\geq 10^{-6}$ to $< 10^{-5}$	One hazardous failure in 100000 hours
SIL 2	$\geq 10^{-7}$ to $< 10^{-6}$	One hazardous failure in 1000000 hours
SIL 3	$\geq 10^{-8}$ to $< 10^{-7}$	One hazardous failure in 10000000 hours
SIL 4	$\geq 10^{-9}$ to $< 10^{-8}$	One hazardous failure in 100000000 hours

Failure limits for a safety function used in high demand mode

High demand mode (continuous mode) is mainly used in production engineering. Continuous monitoring of working processes is frequently required here to guarantee the safety of mankind and the environment.

Low demand mode (on demand) is typically found in the process industry. A typical example is an emergency shutdown system which only becomes active when the process becomes out of control. This normally occurs less than once a year. For this reason, high demand mode is usually of no significance for process instrumentation in most cases.

The considerations in this brochure therefore apply exclusively to low demand systems.

Comparison between SIL and AK

DIN 19250/19251 and DIN 0801 were German industry standards and were used as the basis for the evaluation of safe products before the international standard IEC 61508 was introduced.

DIN 19250 defined requirement categories (AK) instead of the safety integrity levels (SIL1 - 4) of the new international standard IEC61508.

The basic principle for application of the requirement categories (AK) is based on the fact that, through the exclusive use of devices of a particular requirement category, the total system also fulfills this requirement category. In addition, only the computer components of an SIS have been considered.

Two considerations are made for the application with SIL:

1. **Examination of the systemic faults**
   As with application of AK, it also applies here that the SIL-capability of all important components also results in fulfillment of the SIL rating for the complete system.
2. **Examination of the random failures**
   The entire SIS is calculated here. It may occur here, for example, that the demands are not fulfilled despite all devices being rated at a given SIL capability.

SIL

The SIS is examined in its entirety. The failure probability, and thus the SIL level, must be calculated. To this end, the individual failure probabilities of all components of the SIS are included in the calculation. It may therefore occur that, despite exclusive use of SIL 2 components, the SIL 2 level is not achieved in a SIS! The systematic failures of the entire SIS must also be taken into consideration.

AK

Only the computer components in a SIS are considered. For example, in order to design a plant in compliance with AK4, all corresponding components must at least also correspond to AK4.

The following table shows a comparison between the requirement categories AK and the safety integrity levels.

DIN 19250 Requirement category	IEC 61508 Safety integrity level
AK 1	Not defined
AK 2 AK 3	SIL 1
AK 4	SIL 2
AK 5 AK 6	SIL 3
AK 7 AK 8	SIL 4

Comparison between AK (DIN 19250) and SIL (IEC 61508) (may not completely agree in a few cases)

Who does the SIL classification apply to?

In the case of plants that must meet safety technology requirements, the participants are affected for different reasons:

- **Plant operators**
  Place the demands on the suppliers of safety technology components. These must provide proof of the remaining risk potential.
- **Plant constructors**
  Must appropriately design the plant.
- **Suppliers**
  Confirm the classification of their products.
- **Insurance companies, authorities**
  Request proof of a sufficient reduction in the residual risk of the plant.

What devices can be used with which SIL?

In order to achieve a level (SIL 1 - 4), the complete SIS must fulfill the demands for the systematic failures (particularly the software) and the random failures (hardware). The calculated results of the complete SIS must then correspond to the target SIL.

In practice, this primarily depends on the design of the plant or measuring circuit. In an SIL 3 plant, for example, devices with a lower SIL can also be used within certain limits.

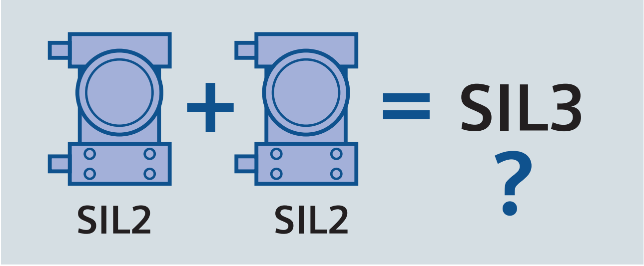
For safety reasons, it is more advantageous if at least two redundant devices are used. A small positive side-effect is that the cost of two SIL 2 devices is usually lower than that of one SIL 3 device.

SIL 4 cannot be implemented using conventional devices.

If two SIL 2 devices are used in redundant mode, is this automatically SIL 3?

No. It is always the case that the calculated failure probability of the complete SIS must result in SIL 3. Redundant operation of SIL 2 devices permits a reduction in the probability for random failures. Whether this is sufficient for SIL 3 must be determined by considering systematic and random failures. In terms of systematic failures (e. g. software), the entire system must also meet the requirements for SIL 3.

This procedure applies analogously to other SIL levels.



Types of faults

A differentiation is made in a safety instrumented system between systematic faults and **random** faults. **Both types of faults must be considered individually in order to fulfill a demanded SIL level.**

Random faults

Random faults do not exist at the time of delivery. They result from failure of individual components of the hardware, and occur at random during operation. Examples of random faults include: Short-circuit, interruption, drift in component values, etc. The fault probability and the associated failure probability can be calculated. The individual hardware components of an SIS are calculated. The results are expressed by the PFD value (average probability of failure on demand), and are the calculation basis for determining the SIL value.

Systematic faults

Systematic faults already exist at the time of delivery of every device. These are typically development faults or faults in the design or configuration. Examples include software faults, incorrect dimensioning, incorrect rating of measuring device, etc. Faults in the device software make the largest contribution to the systematic faults. The fundamental consideration with systematic software faults is that faults in the programming can also result in faults in the process.

Common cause faults

Common cause faults of the hardware can be caused by external factors, such as electromagnetic interference (EMC) or other environmental factors, such as temperature or mechanical load. They have a simultaneous effect on multiple components of a "safety instrumented system".

When using devices in a redundant configuration, systematic faults are common cause. As a result, special measures must be used to avoid systematic faults during development. This includes, for example, qualitative requirements of the IEC standard for the development process, the change process, and the HW/SW architecture of the device.

The device manufacturer must provide data on the SIL rating with respect to systematic faults. This information is usually present in the conformity certificate of the individual devices. This information can be supported by certificates produced by independent organizations such as the TÜV (German Technical Inspectorate) or companies specialized in testing such as exida.

This rating is not part of quantitative calculations, but only provide information on the SIL rating of the device with respect to systematic faults.

In order to fulfill the systematic fault requirements for a certain SIL (e.g. SIL 3), the complete SIS must be appropriately designed. The simplest consideration in this case is that all components possess an SIL 3 rating for systematic faults.

Complete redundancy with systematic faults

It is also possible to use SIL 2 components if measures have been taken which do not allow a systematic fault at the SIL 2 level. For example, if SIL 2 pressure measuring devices are to be used in an SIL-3-SIS, it must be ensured that different device software is used. This is achieved e.g. by using two different devices, best of all from different manufacturers (complete redundancy, also see the figure on page 21). Complete redundancy can also apply if different technologies are used instead of different devices (if meaningful), for example with a pressure measuring device and a temperature measuring device.

Calculation examples (random faults)

Calculation of an SIS with an SIL 2 sensor

Prevailing values:

PFD sensor A	$1.5 * 10^{-3}$	(suitable for SIL 2)
PFD controller	$1.3 * 10^{-4}$	(suitable for SIL 3)
PFD actuator	$7.5 * 10^{-4}$	(suitable for SIL 3)

Example of a 1oo1 Sensor

(1 unit of 1 available unit required for functioning)

Sensor A SIL 2 ▶ Controller (e.g. PLC) SIL 3 ▶ Actuator SIL 3

$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 1.5*10^{-3} + 1.3*10^{-4} + 7.5*10^{-4}$

$PFD_{Sys} = 2.38*10^{-3}$ (SIL 2)

By using these components, the SIS achieves the PFD for SIL 2.

SIL	PFD
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$

Calculation of an SIS exclusively with SIL 3 components

Prevailing values:

PFD sensor B	$6.09 * 10^{-4}$	(suitable for SIL 3)
PFD controller	$1.3 * 10^{-4}$	(suitable for SIL 3)
PFD actuator	$5.0 * 10^{-4}$	(suitable for SIL 3)

Example of a 1oo1 Sensor

(1 unit of 1 available unit required for functioning)

Sensor B SIL 3 ▶ Controller (e.g. PLC) SIL 3 ▶ Actuator SIL 3

$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 6.09*10^{-4} + 1.3*10^{-4} + 5.0*10^{-4}$

$PFD_{Sys} = 1.24*10^{-3}$ (SIL 2)

By using these components, the SIS achieves the PFD for SIL 2.

This example clearly shows that the SIS does not achieve the PFD for SIL 3 despite the exclusive use of SIL 3 components.

SIL	PFD
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$

Important note:
The calculations shown refer exclusively to random faults! Whether an SIS actually fulfills the demands of the required SIL must additionally be checked with respect to the systematic faults.

Comment:

The examples shown here are presented very simply, and only to provide basic understanding. These examples cannot be applied to an exact calculation!

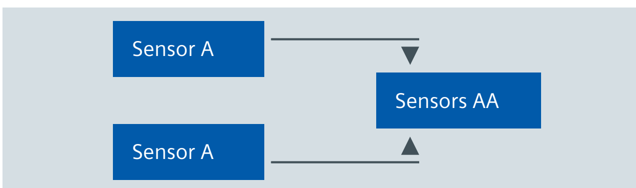
The following abbreviations are used in the calculation examples:

Abbreviation	Explanation
PFD	Mean failure probability of function for the demand
PFD_{Sys}	Failure probability of the system (the complete SIS)
PFD_S	Failure probability of sensor
PFD_L	Failure probability of logic components/controller
PFD_A	Failure probability of actuator

Calculation of an SIS with redundant sensors

Prevailing values:

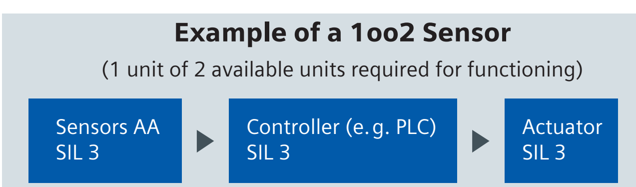
PFD sensor A	$1.5 * 10^{-3}$	(suitable for SIL 2)
PFD sensor A	$1.5 * 10^{-3}$	(suitable for SIL 2)



$PFD_S = 1.52*10^{-4}$

Determination of the PFD value for the redundant connection of the two sensors is too complex to be presented here understandably. The value can vary greatly, for example if different technologies, manufacturers or device designs are used.

PFD sensor AA	$1.52 * 10^{-4}$	(suitable for SIL 3)
PFD controller	$1.3 * 10^{-4}$	(suitable for SIL 3)
PFD actuator	$6.8 * 10^{-4}$	(suitable for SIL 3)



$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 1.52*10^{-4} + 1.3*10^{-4} + 6.8*10^{-4}$

$PFD_{Sys} = 9.62*10^{-4}$ (SIL 3)

By using these components, the SIS achieves the PFD for SIL 3.

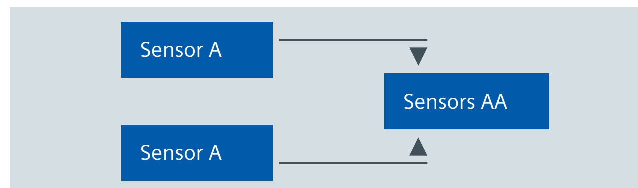
This example clearly shows that the complete SIS achieves the PFD for SIL 3 despite the use of SIL 2 components.

SIL	PFD
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 3	**$\geq 10^{-4}$ to $< 10^{-3}$**
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$

Calculation of an SIS with redundant sensors (poorer actuator value)

Prevailing values:

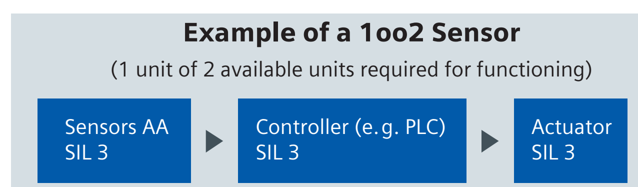
PFD sensor A	$1.5 * 10^{-3}$	(suitable for SIL 2)
PFD sensor A	$1.5 * 10^{-3}$	(suitable for SIL 2)



$PFD_S = 1.52*10^{-4}$

Determination of the PFD value for the redundant connection of the two sensors is too complex to be presented here in a comprehensible manner. The value can vary greatly, for example if different technologies, manufacturers or device designs are used.

PFD sensor AA	$1.52 * 10^{-4}$	(suitable for SIL 3)
PFD controller	$1.3 * 10^{-4}$	(suitable for SIL 3)
PFD actuator	$7.5 * 10^{-4}$	(suitable for SIL 3)



$PFD_{Sys} = PFD_S + PFD_L + PFD_A$

$PFD_{Sys} = 1.52*10^{-4} + 1.3*10^{-4} + 7.5*10^{-4}$

$PFD_{Sys} = 1.03*10^{-3}$ (SIL 2)

By using these components, the SIS achieves the PFD for SIL 2.

This example clearly shows that the SIS does not achieve the PFD for SIL 3 despite the use of redundant SIL 2 sensors.

SIL	PFD
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$
SIL 2	**$\geq 10^{-3}$ to $< 10^{-2}$**
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$

Is the highest possible SIL advantageous?

Companies operating plants are responsible for proving the functional safety of their plant. They are frequently unsure whether a high or low SIL should be achieved for their plant. The demand for a certain SIL results from determination of the residual risk exhibited by the plant. The lowest possible SIL should always be striven for. This not only results in significant cost advantages, but also permits a far greater selection of devices.

A high SIL is only striven for if it is unavoidable or if cost advantages then result elsewhere, permitting saving again of the extra costs (e.g. by saving expensive additional construction measures).

Why is it advantageous for a company to have a plant in accordance with IEC 61508/61511?

These standards also provide a common base for manufacturers and users to monitor the effectiveness of the development processes. When users choose safe devices to achieve the intended SIL for their plants, they can be sure that uniform methods were used in development.

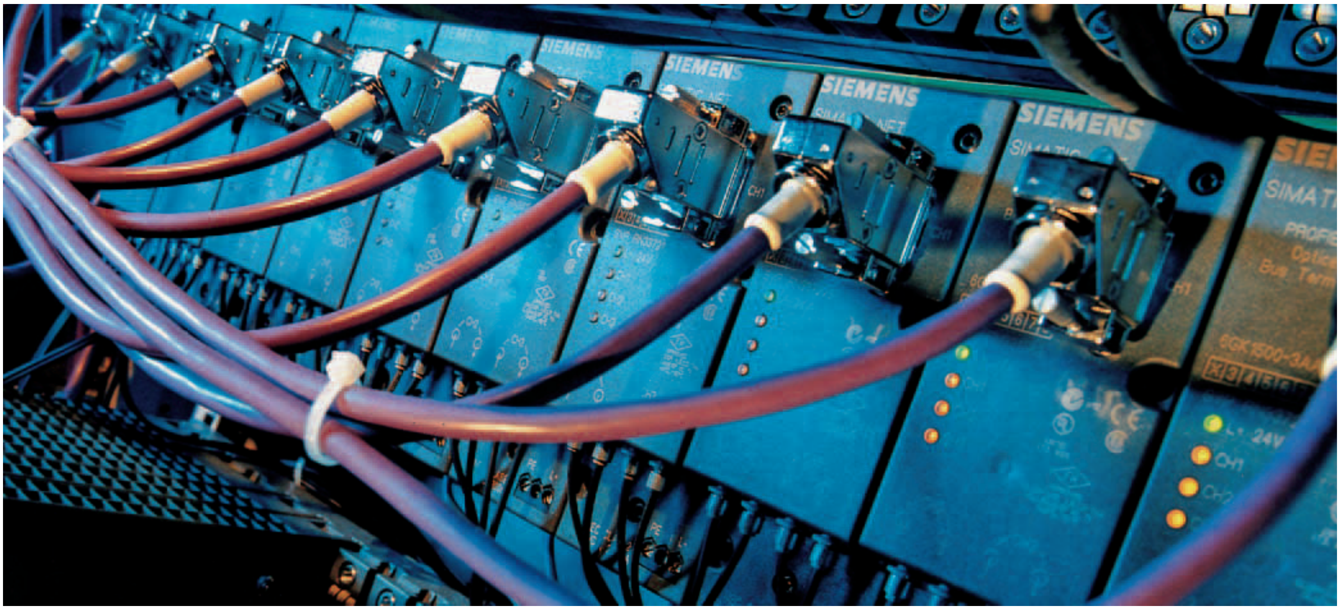
It is then easier for the company operating the plant to provide the proof for risk reduction required by law. This can be required to achieve operating approval for the plant. It is not absolutely essential to use SIL-classified products, however, the demonstrating compliance is greatly simplified since the residual risk is already known (and unambiguous) for these products.

How secure is bus communication?

A clear trend can be observed in the process industry: more and more data is transferred between the components. This occurs by means of various protocols, such as HART, PROFIBUS or Foundation Fieldbus - either with digital signals modulated up to the analog 4 through 20 mA signal or by means of bus communication with a fieldbus.

Due to the variety of possible errors, such as electromagnetic interference (EMC) and the complexity of the bus system, the data transfer in conventional bus systems is not inherently reliable.

Special software algorithms that can ensure reliable transfer are thus required for safe data communication via a bus or fieldbus. The only protocol that currently fulfills these requirements is PROFIBUS with a PROFIsafe profile. PROFIsafe has long since proven itself for safety-relevant applications in the production industry. In the process industry, PROFIsafe is becoming increasingly important with the continuously growing number of available field devices and also contributes to the use of the advantages of the fieldbus technology in safety-relevant systems.



Device ratings by manufacturers

Rating in accordance with IEC 61508

The definitions of IEC 61508 cover the complete product lifecycle from initial concept up to discontinuation of a product. In order to develop a component according to this standard, appropriate procedures and additional technical measures must be taken and verified from development through production. This often makes the development of a failsafe product more expensive than that of a standard component without SIL certification.

Rating in accordance with IEC 61511 (operational proof)

At the moment there are a limited number of devices which have been certified in accordance with the IEC61508 standard. In order to allow a practicable selection of devices, the possibility of operational proof for devices has been permitted in IEC 61511. In practice, the older devices have been used successfully for many years. Therefore a statement on the functional safety can be provided by considering failure statistics under certain conditions. The objective is to determine within a reasonable doubt whether the required functional safety is also actually provided. Evidence must be provided to show a sufficient number of units in the field, and include data on the operating period and conditions of use. The minimum period of use is 1 year and additionally a specified number of operating hours. The operational proof only applies to the version/release of the product for which the proof has been provided. All future modifications of the product must subsequently be carried out in accordance with IEC 61508.

What certificates are required - and who can provide them?

The plant operators require proof of the SIL classification of the components used by the SIS. According to IEC 61511, manufacturer declarations are entirely sufficient. Certificates are neither stipulated by law nor required by the standard.

In order to be able to issue a manufacturer declaration or a certificate, a technical assessment of the safety components used is required. This assessment is often performed by an independent organization such as TÜV or exida. The manufacturer can issue a manufacturer declaration after a successful assessment and can also refer to the test report of the assessment.

In contrast to manufacturer declarations, certificates can only be issued by an accredited organization (e.g. TÜV).

SIL 1	Independent person
SIL 2	Independent department
SIL 3	Independent organization
SIL 4	Independent organization

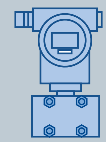
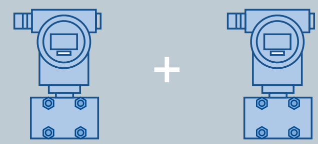
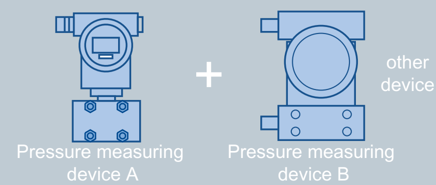
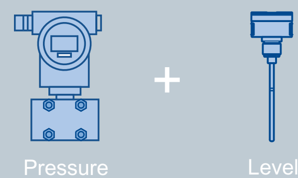
Overview, which instance assesses

The higher the safety required for a plant, the more independent the person must be who carries out judgment of the functional safety.

Declaration of conformity (manufacturer's declaration)	The manufacturer certifies that a particular SIL level has been achieved according to his tests and calculations or as a result of operational proof. The tests are often carried out by a testing authority such as exida or TÜV.
Certificate	Is issued by an independent, accredited organization (e.g. TÜV).

Overview of possible certificates

Possible configurations (single-channel/redundant)

Single-channel configuration One single device	
Redundant, two-channel configuration Two devices of same type	
Completely redundant configuration Two different devices (measure to ensure that systematic faults cannot occur simultaneously)	
Two different technologies	

How is the assessment carried out?

The following elements can be assessed:

- The complete device
- Random faults (only hardware)
- Systematic faults (hardware and software)

New plants – old plants (protection of inventory)

Inventory protection applies to existing plants. However, this means that, with plant conversions or expansions, the newly added parts will be assessed according to the new standards.

Important statements concerning the topic of SIL are summarized again below:

- The device supplier has no influence on the SIL rating of the plant.
- In order to assess whether a Safety Instrumented System (SIS) complies with a required SIL, it is **always** necessary to calculate the failure probability of the random faults.
- In the end, the **value of the failure probability** of the used components is therefore of significance to the company operating the plant. The SIL rating of the device can therefore frequently only be used as an approximate value for the calculation.
- In addition, the processing system must satisfy the systematic fault prevention requirements.
- The statement on the SIL rating of a device only means that it is basically suitable for use in a plant with a corresponding SIL rating.
- The standard requires **assessment** of the functional safety. **Certificates are neither required by the standard nor stipulated by law.**
- The application standard IEC 61511 applies to the process industry.

Further information can be found on the Internet

www.siemens.com/sil

www.siemens.com/safety

www.siemens.com/processanalytics

www.siemens.com/processsafety

www.siemens.com/processinstrumentation

Subject to change without prior notice | Order No. E86060-A6200-A101-A3-7600 | Dispo 09511 | KB 0407 2. ROT 24 EN / 715053 | Printed in Germany | © Siemens AG 2007

Siemens AG

Automation and Drives
Sensors and Communication
P.O. Box 48 48
D-76181 KARLSRUHE
GERMANY

www.siemens.com/processinstrumentation