Füllstand | Druck | Durchfluss | Temperatur | Flüssigkeits-analyse | Registrierung | Systeme Komponenten | Services | Solutions

IEC 61508/IEC 61511

Functional safety in the Process Industry – risk reduction with Safety Instrumented Systems

Endress+Hauser

People for Process Automation

Safety Integrity Level

Safety Instrumented Systems

Classified and evaluated instrumentation in the process industry, an important contribution to the safety of personnel, the environment and equipment.

In most countries, safety requirements for man, equipment and the environment, follow state-of-the-art technology, as a binding and legal requirement. This standardis IEC 61508* (Functional safety of electrical/electronic/programmable electronic safety-related systems).

* also avaliable as DIN EN 61508

What is SIL?
Safety Instrumented Systems (SIS) are designed and used to prevent or mitigate hazardous events to protect people or the environment or prevent damage to process equipment.
Safety Integrity Level means risk reduction to a tolerable level. The IEC 61508 standard specifies both the risk assessment (risk graph) and the measures to be taken in the design of safety functions consisting of sensor, logic solver and actuator. These measures include “fault avoidance” (systematic faults) and “fault control” (systematic and random faults).

This generic standard specifies the pertinent requirements for components and systems used in safety functions. It also enables application sector specific standards to be developed (e.g. IEC 61511 „Functional safety: Safety instrumented systems for the process industry sector“). For example, the IEC 61511 defines selection criteria for components of safety functions, like “prior use” demonstration of sensors and actuators.

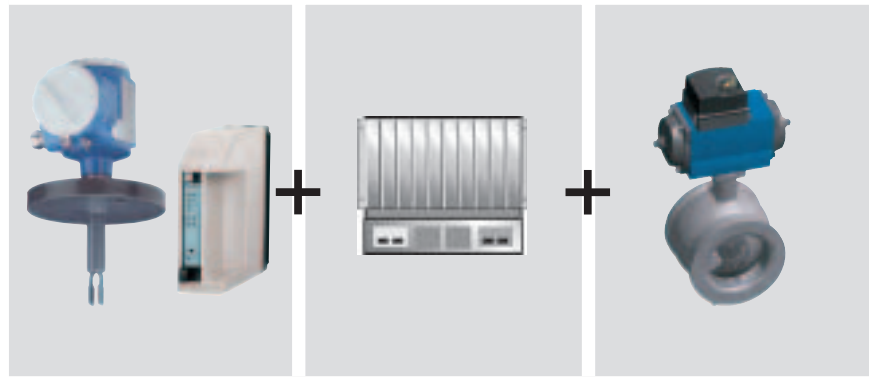
When is IEC 61508 used?
IEC 61508 applies for all applications where electrical, electronic or programmable electronic safety-related systems are used to perform safety functions. It covers all those applications where system malfunctions have a decisive effect on the safety of personnel, the environment and equipment concerned.

The advantages of SIL standardisation

- Internationally harmonised procedures in the evaluation of safety-related systems.
- Evaluation of process control safety-related systems regarding systematic fault and proven random fault statistics.
- Defined “Life Cycle Management” i.e. documentation of all function-relevant steps involved in design and development.
- Complete evaluation of the entire safety function (sensor/transmitter, controller, actuator).
- The required safety can be attained with the SIL evaluated instrumentation; without extensive change of the process technology.

Complete evaluation of a safety function (Safety Loop)

Sensor/transmitter	Controller	Actuator



IEC 61508 / IEC 61511

Safety evaluation and requirements

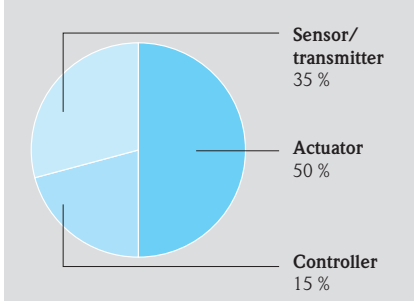
Differences between IEC 61508 and previous standards
For the first time a standard now requires quantitative proof for the residual risk, based on calculating the probabilities of dangerous failures.
This calculation is carried out for the complete safety loop, consisting of measuring point (sensor), controller (e.g. PLC) and actuator (valve).

The probabilities of failure calculated for all individual components are added (PFD) and considered over the entire safety-related technical circuit such as 1oo1 (voting one out of one) or 2oo3. Applying this safety standard, it is not only the individual instrumentation but also its development and production which must be considered (safety lifecycle).

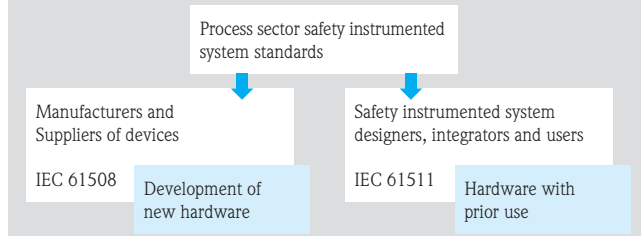
SIL	PFD_{av}
4[1)]	$\geq 10^{-5} ... < 10^{-4}$
3	$\geq 10^{-4} ... < 10^{-3}$
2	$\geq 10^{-3} ... < 10^{-2}$
1	$\geq 10^{-2} ... < 10^{-1}$

Dependance of SIL on the allowable average probability of failure of a safety-related system operating in low demand mode of operation.

The PFD_{av} is generally classified for the entire safety system as follows:



Relationship between IEC 61508 und IEC 61511



For risk reduction, both standards IEC 61508 and IEC 61511 basically define the following steps:

- Risk definition and assessment according to detailed probabilites of failure from sensor over controller to actuator for the overall component life time.
- Specification and implementation of measures for risk reduction.
- Use of suitable instrumentation (evaluated or certified).
- Periodic test for correct operation of the safety functions.

Risk graph according to IEC 61508/61511

		W3	W2	W1
C1		–	–	–
C2	F1 P1	SIL 1	–	–
	F1 P2	SIL 1	SIL 1	–
	F2 P1	SIL 2	SIL 1	SIL 1
	F2 P2	SIL 3	SIL 2	SIL 1
C3	F1	SIL 3	SIL 3	SIL 2
	F2	SIL 4[1)]	SIL 3	SIL 3
C4		–	SIL 4[1)]	SIL 3

Consequences
C1 minor injury
C2 serious permanent injury to one or more persons; death of one person.
C3 death of several persons
C4 very many people killed

Exposure time
F1 rare to more often
F2 frequent to permanent

Avoidance of hazard
P1 possible under certain circumstances
P2 almost impossible

Probability of unwanted occurance
W1 very slight
W2 slight
W3 relatively high

[1)] SIL 4 cannot be achieved only with components.

SFF, HFT, SIL

Relationship between safety-related parameters

Safe Failure Fraction (SFF)
Fraction of failures which do not have the potential to put the safety-related system in a hazardous or fail-to-function state.

Hardware Fault Tolerance (HFT)
Ability of a functional unit (hardware) to continue to perform a required function in the presence of faults or errors. An HFT of N means, that N+1 faults could cause a loss of the safety function.

In addition to holding at maximum for probabilities of failure (PFD) the **Safety Integrity Level (SIL)** of a safety function according to IEC 61508 depends on the combination of SFF and HFT.

The difference between "simple" and "complex" devices
The behaviour of "simple" (type A) devices under fault conditions can be completely determined. The failure modes of all constituent components are well defined. Such components are metal film resistors, transistors, relays, etc.

The behaviour of "complex" (type B) devices under fault conditions cannot be completely determined. The failure mode of at least one component is not well defined. Such components are e. g. microprocessors, ASICs.

The failure rates of these components can be found in reference tables.

Type A: "simple" devices (all faults known and describable)			
SFF Safe Failure Fraction	HFT Hardware Fault Tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 - < 90 %	SIL 2	SIL 3	SIL 4
90 - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Type B: "complex" devices (not all faults known and describable)			
SFF Safe Failure Fraction	HFT Hardware Fault Tolerance		
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 - < 90 %	SIL 1	SIL 2	SIL 3
90 - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

For "prior use" instruments, the HFT may be reduced by 1 (for SIL ≤ 3 only) under defined conditions, according to IEC 61511.

Parameters

which are required for planning

There are several procedures to evaluate components such as sensors and actuators:

- **Complete evaluation according to IEC 61508**
  Complete evaluation of the hardware (HW) and software (SW). Fault avoidance and fault control measures are observed during the development, production and operation of the product (safety lifecycle). This is usually carried out for products to be developed.
- **“Prior use” according to IEC 61508/61511**
  For the evaluation of already developed and manufactured components, IEC 61511 specifies the suitability of an instrument based on the proven-in-use capability of an instrument including the instruments software and the accompanying modification procedures.

Information required by the planner or user

In order to carry out all necessary measures, the requirements for the Safety Integrity Level, resulting from risk graph analysis, must be met. Depending on the determined Safety Integrity Level (SIL 1, 2, 3 or 4), all important parameters for the safety-related implementation of an application have to be defined.

Safety	Freedom from unacceptable risk
E/E/PES	Electrical/electronic/programmable electronic system System for control, protection or monitoring based on one or more E/E/PES
Functional safety	The ability of a system to carry out necessary actions to achieve or maintain a defined safe state.
Safety function	Function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC (equipment under control), in respect of a specific hazardous event
SIL (Safety Integrity Level)	IEC 61508 defines four discrete Safety Integrity Levels (SIL1 to SIL4). Each level corresponds to a probability range for the failure of a safety function. The higher the Safety Integrity Level of the safety-related systems, the lower the probability that they will not perform the requested safety function.
SFF (Safe Failure Fraction)	Percentage of failures without the potential to put the safety-related system into a dangerous or fail-to-function state.
PFD_{av}	Average probability of failure on demand
λ_{SD}	Failure rate for all safe detected failures
λ_{SU}	Failure rate for all safe undetected failures
λ_{DD}	Failure rate for all dangerous detected failures
λ_{DU}	Failure rate for all dangerous undetected failures
HFT (Hardware Fault Tolerance)	Ability of a functional unit (hardware) to continue to perform a required safety function in the presence of faults or errors. A Hardware Fault Tolerance of N means that N+1 faults could cause a loss of the safety function.
T_1 (years)	Proof-test interval Periodic test performed to detect failures in a safety-related system.
MTBF	Mean time between failures
MTTR	Mean time to restoration
Voting “MooN”	M out of N channel architecture: Classification and description of safety-related systems regarding redundancy and applied selection process. “N” denotes how often the safety function is performed (redundancy). “M” denotes how many channels have to work properly. Pressure measurement example: 1oo2 architecture – A safety-related system decides that a predefined pressure limit is exceeded when one of two pressure sensor reaches this limit. If a 1oo1 architecture is used, there is only one pressure sensor available.
MooND	M out of N channel architecture with diagnostics
Low demand mode	Mode of operation where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency.
High demand or continuous mode	Mode of operation where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-test frequency.
IEC 61508 (part 1 to 7)	Functional safety of electrical/electronic/programmable electronic safety-related systems (Target group: Manufacturers and Suppliers of Devices)
IEC 61511 (part 1 to 3)	Functional safety: Safety Instrumented Systems for the process industry sector (Target group: Safety Instrumented Systems Designers, Integrators and Users)

Your added benefits with Endress+Hauser

- All important safety-related parameters from a single source, standard up to SIL 2: pressure – temperature – level – flow-system components.
- Uniform and compact “safety manuals” for transparency and safety in planning, commissioning and performance checks of safety-related systems.
- Safety-related evaluation of software updates to the existing standard according to IEC 61508.

Safety Integrity Level SIL Endress+Hauser

Endress+Hauser develops instrumentation according to IEC 61508 for all important areas in process technology.

The newest listing of SIL field instrumentation and documentation (e.g. safety manuals) is found under www.endress.com/SIL.

09.03/MMC

Endress+Hauser – Instruments International

Endress+Hauser GmbH+Co. KG
Instruments International
Colmarer Straße 6
79574 Weil am Rhein
Germany
Tel. +49 7621 975 02
Fax +49 7621 975 345
http://www.endress.com
info@ii.endress.com

CP 002Z/27/en/04.04
LL/INDD 2.0

Endress+Hauser

People for Process Automation