Functional Safety - SIL

What does functional safety mean?

According to IEC 61508, functional safety related to systems used to carry out safety functions whose failure has a considerable impact on the safety of both persons and the environment.

In order to achieve functional safety, a safety function in the event of a failure must ensure that a technical plant is led to or maintained in a safe state.

Functional safety does not deal with basic dangers of a product or a plant such as rotating parts for example, but with hazards, which might be caused by a plant due to the failure of a safety function.

A major objective of functional safety is to reduce the probability of dangerous failures and consequently to minimize the risk for people and environment to a tolerable level.

Altogether, functional safety - in combination with further actions such

Standards Applicable.

IEC 61508 is an international standard applicable for the complete safety lifecycle of safety -related systems containing electrical, electronic or programmable electronic components (E/E/PE). The requirements by the standards are transplanted to other e.g. mechanical components where appropriate.

The standard is applicable for plant designers and operators as well as device manufacturers.

It is complemented by further standards such as IEC 61511 for the process sector.

as fire protection, electrical safety or explosion protection - significantly contributes to the overall safety of a plant.

What is SIL?

SIL is a term closely linked to functional safety. SIL is the abbreviation for Safety Integrity Level and a measuring unit for risk reduction with safety functions.

The higher the potential hazards from processes or plants, the more demanding the requirements for reliability of safety functions.

IEC 61508 defines four different safety integrity levels, SIL 1 through SIL 4.

SIL 4 has the highest level of safety integrity and SIL 1 the lowest. For each level, various target failure probability measures are specified which may not be exceeded by the safety function.

Risk assessment is used to determine the required SIL.

The standards IEC 61508 / 61511 define a recognized method of risk evaluation for safety related system used in the process industry.

The HAZOP team (hazard & operability studies) of the plant makes a safety instrumented assessment i.e., identification of potential hazards for persons and environment of all the processes where safety functions are involved in the plant.

Each of the potentially dangerous process is examined to determine the resulting hazard and consequence due to failure. Risk assessment defines the extent and occurrence probability of the risk and whether process must be protected by a safety function highlighting desired SIL level the safety function must achieve.

Then depending on the required SIL, the components for implementing the safety function will be selected. The devices used in the safety loop are tested for classification in compliance with safety integrity levels.

On the basis of safety figures of implemented devices, verification is made for each safety function whether the demanded SIL is achieved and if not additional actions will have to be taken.

Functional safety is achieved if safety functions work reliably in case of failure. In the valve sector, the following safety functions are of crucial importance.

" SAFE OPENING

" SAFE CLOSING

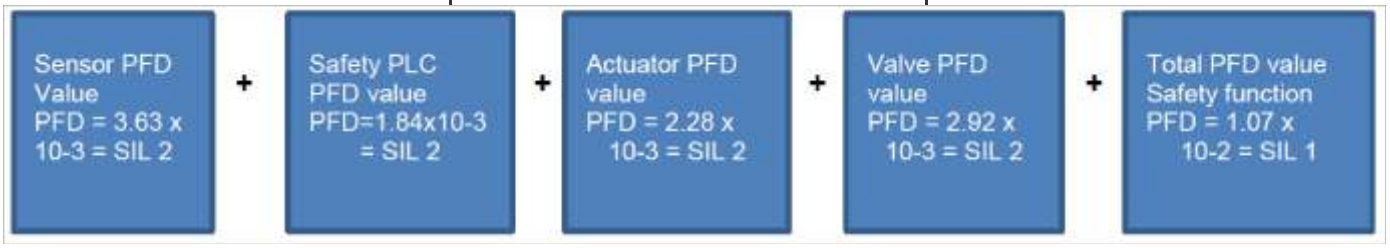
" SAFE STAND STILL / STOP

" SAFE END POSITION FEEDBACK

Since the valve and Actuators form part of a safety instrumented system while assessing demand at SIL for a safety function, the safety figures of all

Target PFD_{avg} Measures for Low Demand Type

Safety Integrity Level	Allowed PFD_{avg} measure(low demand)	Theoretically allowed failures for a safety function on demand
SIL 1	$= 10^{-2}$ to $< 10^{-1}$	One allowed dangerous failure in 10 years
SIL 2	$= 10^{-3}$ to $< 10^{-2}$	One allowed dangerous failure in 100 years
SIL 3	$= 10^{-4}$ to $< 10^{-3}$	One allowed dangerous failure in 1000 years
SIL 4	$=10^{-5}$ to $< 10^{-4}$	One allowed dangerous failure in 10000 years



individual devices form the safety instrumented system must be considered.

The very important safety figures considered are Average probability of dangerous failure on demand PFDavg ,Failure rates ?, Safe failure fraction SFF, Hardware fault tolerance, Device type A or B, Mean time between failures MTBF, Interval for proof tests etc.

A safety integrity level is always claimed for the complete safety function. Therefore, consideration of PFD values for the individual components is insufficient.

For e.g.:- Calculation of the total PFD value of a safety function

The PFD value of individual components is added to determine the SIL capability of the safety function. The resulting PFD value of a safety function is then compared with the allowed total probability of dangerous failure on demand for the required SIL. Should the calculation show that the selected hardware components do not achieve the required SIL, SIL capability has to be improved by additional actions such as diagnosis and redundancy.

The partial valve stroke test is performed regularly to verify device function. Actuator or Valve travel a predefined distance forth and back to test whether device actually operates.

PVST is a recognized anticipated test method to increase the availability for device for safety function.

The proof test deals with a comprehensive system verification done periodically.

Redundant system architecture is used to increase the probability that the safety function is performed in case ofemergency. Two or more device of a safety relatedsystems are subjected to redundant operation.

Depending on the safety requirement different M oo N configuration makes sense. For a 1oo2 (One out of two)configuration one out of two devices are sufficient to perform required safety function.

For e.g.:- 2003 (Two out of Three) implies configuration 2 out of 3 devices must function properly. Redundant systemarchitecture can increase hardware fault tolerance and consequently SIL capability.

Article by:

Mr. MN Balachandra
Vice-President, Marketing,
AUMA India Pvt Ltd.