EXTECH
Safety Systems

Functional Safety (SIL) basics for Process Control

There is a lot of information published on Functional Safety & Safety Integrity Level (SIL) and it is difficult to know where to turn to or what to believe. I will try to provide a basic overview, cover some of the misconceptions and consider some of the implications on a process control loop.

Functional Safety is a Culture, not a “Certificate”

Safety Instrumented Systems (SIS) often referred to Emergency Shutdown Systems (ESD) are put in place in addition to the Basic Process Control System (BPCS) e.g. DCS or PLC to independently monitor the process and bring the plant to a safe state as or when control is lost.

IEC/SANS 61508 and IEC/SANS 61511 provide a framework to assess risk & safety in process control environments. They are not prescriptive in how to implement safety, but compliance allows users and product designers to demonstrate best practice and to fulfil legal health and safety obligations. Importantly, the management of Functional Safety applies throughout the lifecycle of a process plant, from initial design through to de-commissioning.

The SIL is an attribute of the complete safety instrumented function, not of a single device.

In order to claim SIL capability, manufacturers of devices intended for use in functional safety applications should provide statistical data on the failure modes and failure rates (PFDavg) of the equipment. In addition, manufacturers must state how the requirements for Architectural Constraints are achieved for the specified SIL level and demonstrate how systematic errors have been controlled in the design, development and manufacturing processes. The primary concern is that failures of individual elements of the SIF could lead to the failure or impairment of the overall safety function. Manufacturers should supply a Safety Manual that explains how to use the failure data and how to install, maintain and proof test the equipment to achieve

safe operation. This is important, because the desired failure mode will depend on the way in which a product is used. As an example, one plant might be safe for a high temperature whilst another might be safe if temperature is low. One process might be safe with the valve failing to the open position, whilst another requires the valve to close on failure. It is also important to look at the complete loop from the Sensor Element (SE) e.g. temperature or flow transmitter to the 'Logic Solver' to the Final Element (FE) like a shut-off valve. The whole loop (known as the Safety Instrumented Function, or SIF) has to be assessed together considering failure rate data & failure mechanisms.

There is a perception that if you buy several SIL3 devices & use a SIL3 Logic Solver, then the SIF will meet the requirements for SIL3. This is not necessarily the case. The situation is made worse in cases where suppliers state 'Up to SIL3' on datasheets.

What is SIL?

SIL stands for Safety Integrity Level. A SIL is a measure of safety system performance, in terms of the average probability of failure on demand (PFDavg) or probability of dangerous failures per hour. This numerical convention was chosen to provide an objective measure for comparison of alternate designs and solutions.

There are four discrete integrity levels associated with SIL: SIL 1, SIL 2, SIL 3, and SIL 4, but SIL 4, the highest level of integrity, is not normally used in the process industries. The Safety Integrity Level (SIL) is essentially a measure of the probability of success of a Safety Instrumented Function (SIF) to take a process to a safe state upon demand. This can also be expressed as the order of magnitude level of risk reduction provided by a SIF, i.e. >10 to ≤100 for SIL 1 up to >10 000 to ≤100 000 for SIL 4.

SANS/IEC 61508-2 includes two tables stating the relationship between SIL and PFDavg or dangerous failure rate. In general terms, 'demand mode' applies where the SIF is required to operate less than once per annum, and 'continuous mode' more than once per annum.

From IEC 61508-1 Edition 2.0 2010:

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 2 – Safety Integrity levels – target failure measures for a safety function operating in low demand of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	≥ 10^{-9} to < 10^{-8}
3	≥ 10^{-8} to < 10^{-7}
2	≥ 10^{-7} to < 10^{-6}
1	≥ 10^{-6} to < 10^{-5}

Table 3 – Safety Integrity Levels – Target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

The SIL applies to the whole SIF rather than to an individual element. To achieve the required reliability of a SIF then multiple parallel or redundant instrument loops are often needed, with voting in the 'logic solver' to resolve the status. Thus, the SIF, or sub-systems within the SIF, may be structured as 1oo1 (One out of One), 1oo2, 2oo3 to achieve the requisite low probability of failure. The use of such redundant architectures is described by the term 'Hardware Fault Tolerance' (HFT), where HFT > 0 implies a level of redundancy.

This also follows from the need to follow SANS/IEC 61508 and SANS/IEC 61511 requirements for HFT. The HFT requirements in SANS/IEC 61511 are more onerous than in SANS/IEC 61508. As can be seen from the table in SANS/IEC 61511, SIL3 requires HFT=1. This means that redundant hardware is required so that a single dangerous failure does not compromise the integrity of the SIF. Redundancy increases the availability of the SIF.

From IEC 61511-1 Edition 2.0 2016:

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand mode)	1
3 (any mode)	1
4 (any mode)	2

Table 3 – Safety Integrity Levels – Target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

It is the responsibility of the plant operator to determine the number of Safety Instrumented Functions, and their required SIL, for a process plant. This will typically follow from an identification of process risks identified during the 'HAZOP' process. In a well-designed plant, there are likely to be very few SIL3 SIFs, because SIFs of this level imply the requirement to control potentially catastrophic event scenarios. However, in many cases, there is a general over-specification to SIL3 without understanding the implications & costs. In the author's opinion <5% of loops on a nuclear plant should be SIL3. Even less on a Petrochemical plant. The process should be reviewed and/or redesigned to eliminate the SIL3 requirement by other means. This could include design changes to reduce inventory, improve layout or use mechanical means of protection, such as pressure relieve valves in an over-pressure scenario. In the author's experience SIL3 is often requested without realising that significant hardware has to be redundant – HFT; 1oo2; 2oo3 as previously discussed, i.e. Redundant Field devices, Intrinsically Safe interfaces and within the SIS

Something to think about: A safety function aiming at SIL3 is designed to achieve a Risk Reduction Factor of between 1000 and 10000. i.e. without that safety function in place, the risk of a calamitous event is more than 1000 times greater than is acceptable according to the Tolerable Risk Definition for the plant. Do you

trust a single device to give that level of protection? How are you going to maintain that single instrument loop and operate the plant while it is out of action? Which instrument manufacturer will offer a process transmitter that is rated at greater than SIL2 for a single device? For applications in the Process Industry: SANS/ IEC 61511 sector standard is followed. This is more likely to require hardware redundancy of instrument loops to meet the Hardware Fault Tolerance requirements.

Summary – Facts of life

- SANS/IEC 61508 is aimed at manufacturers and device suppliers, or OEMs. SANS/IEC 61511 is aimed at users and system integrators in the process industries
- SANS/IEC 61508 is not mandatory, but considered best practice worldwide.
- Certification of elements intended for use in Functional Safety applications is not mandatory, but the availability of credible failure data is in order to determine the SIL achieved for a SIF.
- A Safety Manual is required for all elements intended for use in functional safety applications.
- Design of safety function is responsibility of the user not the vendor
- Only complete safety instrumented functions can have a SIL.
- The SIL of a safety function is limited by the systematic SIL capability of the components

Useful to remember

- An item is highly reliable if it adequately performs its objective to a high degree, for the period of time specified, under the operating conditions specified. Therefore, there is a high probability that it will perform its intended function for a specified period of time, usually operating hours, without requiring corrective maintenance. This is normally expressed as Probability of Failure on Demand (PFDavg).
- An item is highly available if it does not fail very often and, when it does, it can be quickly returned to service. Therefore, there is a high probability that the device will be operating successfully at a given moment in time. This is a measure of the “uptime” and is defined in units of percent.
- In Functional Safety terms, a system is considered to be safe, if it is reliable in performing its safety function. The system may fail more frequently in modes that are not considered to be dangerous – in which case these spurious failures will occur as ‘nuisance trips’ of the Safety Instrumented System.
- Consequently, a safety system may have a lower availability in total, due to safe failures, than a non-safety system performing a similar function. However, nuisance trips could also potentially be dangerous.
- ‘SIL’ is not a guarantee of quality or reliability, except in a defined safety context.

Note:

IEC61511:2003 – equivalent to SANS61511: some parts are 2015 & others 2016.

The SANS document needs updating to IEC61511:2016

IEC61508:2010 – equivalent to SANS61508:2013

Further reading:

http://www.mtl-inst.com/images/uploads/AN9025_Rev_4.pdf
http://www.mtl-inst.com/images/uploads/AN9030_Rev_4.pdf
http://www.mtl-inst.com/images/uploads/AN9036_Rev_2.pdf

For more info, please contact:

Gary Friend
gary@extech.co.za;
sales@extech.co.za
www.extech.co.za
Tel : +27 (0)11 791 6000