Safety Integrity Levels - Applying Them To Your Process and Plant

Mike Young, Reliability Engineer Mike Young is a reliability engineer at General Monitors, responsible for SIL assessment for all products.

The global importance of SIL (Safety Integrity Levels) has grown substantially in the oil/gas, petrochemical and other process industries over the last 10 years. However, for many end users, systems integrators, and product vendors, SIL is often misinterpreted and incorrectly implemented. This problem leads to confusion and difficulties in selecting the plant instrumentation and automation components necessary to operate a plant and its processes safely.

Functional Safety and SIS Background

As defined by IEC standard 61508, Functional Safety is provided by control systems to an overall process or plant. Major accidents and the increasing use of electrical or programmable electronic safety systems have driven the need for safety systems that prevent dangerous failures or to control them when they arise. Functional Safety is achieved when every safety function is successfully carried out and the process risk is reduced to the desired level.

A Safety Instrumented System is designed to prevent or mitigate hazardous events by taking a process to a safe state when predetermined conditions are violated. Each SIS has one or more Safety Instrumented Functions (SIF). A SIF loop has a combination of logic solver(s), sensor(s), and final element(s).

Safety Integrity Level (SIL)

A SIL is a measure of safety system performance, in terms of probability of failure on demand (PFD). This convention was chosen based on the numbers: it is easier to express the probability of failure rather than that of proper performance (e.g., 1 in 100,000 vs. 99,999 in 100,000).

There are four discrete integrity levels associated with SIL: SIL 1, SIL 2, SIL 3, and SIL 4. The higher the SIL level, the higher the safety level, and the lower probability that a system will fail to perform properly.

As the SIL level increases, the installation and maintenance costs of the system also increase. Specifically for the process industries, SIL 4 systems are so complex and costly that they are not economically beneficial to implement. If a process includes so much risk that a SIL 4 system is required to bring it to a safe state, then there is a fundamental problem in the process design that needs to be addressed by a process change or other non-instrumented method.

It is a very common misconception that individual products or components have SIL ratings. Rather, products and components are suitable for use within a given SIL environment, but are not individually SIL rated. SIL levels apply to safety functions and safety systems (SIFs and SISs). The logic solvers, sensors, and final elements are only suitable for use in specific SIL environments, and only the end user can ensure that the safety system is implemented correctly. The equipment or system must be used in the manner in which it was intended in order to successfully obtain the desired risk reduction level. Simply buying SIL 2 or SIL 3 suitable components does not ensure a SIL 2 or SIL 3 system.

Can a Fire and Gas System Be Considered a Safety Instrumented System?

There has been much industry debate over the categorization of Fire and Gas Systems (FGS) as Safety Instrumented Systems (SIS), especially as the concept of functional safety matures in the marketplace. Fire and gas detection field devices and technologies are fundamentally different from other forms of plant instrumentation.

Incorrect detector placement and poor environmental conditions can prevent the product from detecting a hazardous gas leak or flame, even when the unit is functioning properly. When a safety hazard is undetected, then the appropriate safety action (shut down, deluge, venting, etc.) cannot be initiated. Because of this, many end-users and system integrators are wondering if the functional safety standards are applicable to a FGS.

A FGS that automatically initiates process actions to prevent or mitigate a hazardous event and subsequently takes the process to a safe state can be considered a Safety Instrumented Function (SIF) or SIS. The FGS would need to be composed of the appropriate logic solver(s), sensor(s), and final element(s).

Correct sensor placement, proper system utilization, and the installation of a diverse set of detection technologies, are extremely important issues that must be considered when determining whether a FGS can technically be classified as a SIS. If there is incorrect placement of the gas or flame detectors and hazardous gases and flames are not adequately detected, then the SIF / SIS will not be effective, regardless of the system SIL rating. Correct sensor placement is more important than deciding whether a FGS should be SIL 2 or SIL 3.

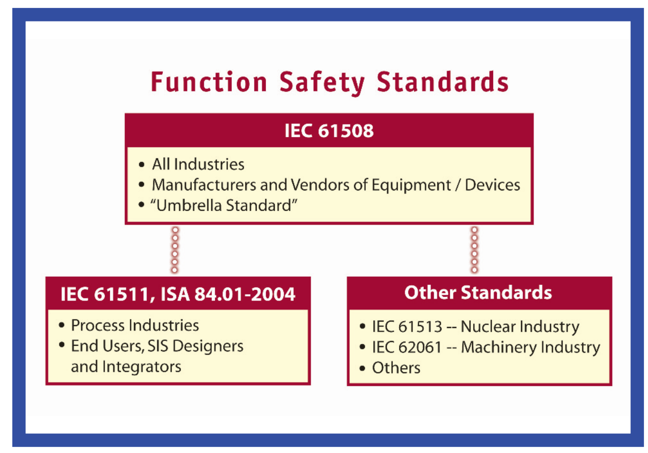
Risk Management and Selecting a SIS or SIL Level

The identification of risk tolerance is subjective and site-specific. The owner / operator must determine the acceptable level of risk to personnel and capital assets based on company philosophy, insurance requirements, budgets, and a variety of other factors.

When determining whether a SIL 1, SIL 2, or SIL 3 system is needed, the first step is to conduct a Process Hazard Analysis to determine the functional safety need and identify the tolerable risk level. After all of the risk reduction and mitigation impacts from the Basic Process Control System (BPCS) and other layers of protection are taken into account, a user must compare the residual risk against their risk tolerance. If there is still an unacceptably high level of risk, a risk reduction factor (RRF) is determined and a SIS / SIL requirement is calculated. The RRF is the inverse of the Probability of Failure on Demand for the SIF / SIS (see table below).

Table - Performance requirements for the different SILs according to IEC61511

Safety Integrity Level	Probability of Failure on Demand	Risk Reduction
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤ 100,000
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$	>1,000 to ≤ 10,000
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1,000
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100



Example of SIS/SIF/SIL Determination

A simple example will help illustrate the concepts of SIS, SIF, and SIL. Consider the installation of a pressure vessel containing flammable liquid. It is maintained at a design operating pressure by the BPCS. If the process control system fails, the vessel will be subjected to an over-pressure condition that could result in a vessel failure, release of the flammable contents and even fire or explosion. If the risk in this scenario is intolerable by the facility owner, a SIS will be implemented to further reduce the risk to a tolerable level.

The SIS system will be independent from the BPCS and will act to prevent or mitigate the hazardous condition resulting from pressure vessel over-pressure. The SIS will have a SIF which might include a pressure transmitter which can sense when an intolerable level of pressure has been reached, a logic solver to control the system logic, and a solenoid valve which might vent the contents of the vessel into a safe location (flare stack, environment, storage tank, etc.), thus bringing the pressure vessel to a safe state.

If the risk reduction factor required from the Process Hazard Analysis is a factor of 100 then a SIL 2 level of SIF performance would be specified. Calculations for the components of the entire SIF loop will be done to verify that the PFD of the safety function is 10^{-2} , meaning that the SIF is SIL 2 or reduces the risk of the hazard by a factor of 100.

This one SIF may constitute the entire SIS, or the SIS may be composed of multiple SIF's that are implemented for several other unacceptable process risks in the facility.

SIL Resource Center

To help process and plant engineers better understand the implications of SIL, General Monitors has created an online SIL Resource Center as part of its gas and flame micro site. The center includes technical articles, SIL FAQs, Common SIL Myths, Useful SIL Links, a SIL Products List and more.

The company's technical staff is also available worldwide to assist process and plant engineers with their questions about SIL and its application to fire and gas detection systems.

Conclusion

The bottom line is you can't buy safety out of a box. As with any Safety Instrumented Function, the Fire and Gas System design must be assessed according to the strengths and weaknesses of the equipment and appropriately applied to the plant application so the FGS provides optimal protection, coverage, and safety.