SIL 101: How safe do I need to be?

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 still a somewhat ambiguous concept that often is misinterpreted and incorrectly implemented. In order to fully understand SIL and its implications, it is important to grasp the overarching concept known as Functional Safety, and how it applies to Safety Instrumented Systems (SIS) within the process industries.

Functional Safety and SIS Background

Functional Safety, as defined by IEC standard 61508, is the safety that control systems provide to an overall process or plant. The concept of Functional Safety was developed in response to the growing need for improved confidence in safety systems. Major accidents around the world, as well as the increasing use of electrical, electronic or programmable electronic systems to carry out safety functions, have raised awareness and the desire to design safety systems in such a way as to prevent dangerous failures or to control them when they arise. Industry experts began to address functional safety and formalize an approach for reducing risk in the process plant environment through the development of standards IEC 61508, IEC 61511, and ANSI/ISA 84. Previous safety standards were generally prescriptive in nature, not performance based.

An emphasis on quantitative risk reduction, life-cycle considerations, and general practices make these standards different from their predecessors. Functional Safety is a term used to describe the safety system that is dependent on the correct functioning of the logic solver, sensors, and final elements to achieve a desired risk reduction level. 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. Other common terms for SISs are safety interlock systems, emergency shutdown systems (ESD), and safety shutdown systems (SSD). Each SIS has one or more Safety Instrumented Functions (SIF). To perform its function, a SIF loop has a combination of logic solver(s), sensor(s), and final element(s). Every SIF within a SIS will have a SIL level. These SIL levels may be the same, or may differ, depending on the process. It is a common misconception that an entire system must have the same SIL level for each safety function.

Safety Integrity Level

SIL stands for Safety Integrity Level. 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 associated safety level, and the lower probability that a system will fail to perform properly. As the SIL level increases, typically the installation and maintenance costs and complexity 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. Additionally, 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. Just buying SIL 2 or SIL 3 suitable components does not ensure a SIL 2 or SIL 3 system.

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. A risk level that one owner determines is tolerable may be unacceptable to another owner.

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.

The SIL level equals the number of zeros in the minimum Risk Reduction Factor. With SIL 2, for example, the minimum Risk Reduction Factor is 100 (see table below). Selecting the appropriate SIL level must be done carefully. Costs increase considerably to achieve higher SIS / SIL levels.

Typically in the process industry, companies accept SIS designs up to SIL 2. If a Process Hazard Analysis indicates a requirement for a SIL 3 SIS, owners will usually require the engineering company to re-design the process to lower the intrinsic process risk.

Safety Integrity Level	Risk Reduction Factor	Probability of Failure on Demand
SIL 4	100,000 to 10,000	10^{-5} to 10^{-4}
SIL 3	10,000 to 1,000	10^{-4} to 10^{-3}
SIL 2	1,000 to 100	10^{-3} to 10^{-2}
SIL 1	100 to 10	10^{-2} to 10^{-1}

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 deemed to be intolerable by the facility owner, a SIS will be implemented to further reduce this risk situation to a tolerable risk 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.

Our SIL and SIS Approach

MSA is fully committed to SIL and SIS. We feel that focusing on functional safety is an excellent opportunity for us to partner with our customers to understand their specific needs and applications, and to develop optimal safety solutions for their unique operating environments.

We have based our approach to ensuring a high level of functional safety on the IEC 61508 and 61511 standards. The programs that we have developed encompass a comprehensive set of activities conducted both in-house and with the assistance of leading safety experts from around the world. In their totality, these programs have resulted in an integrated system for the designing of products, assessing their functional safety, improving robustness and validating performance.

An extensive Failure Mode Effects and Diagnostics Analysis (FMEDA) is now conducted early in the development process for each new product, and it is used throughout the development cycle to improve functional safety. At MSA, the FMEDA is a critical design tool that helps us develop products that offer the highest level of safety. FMEDA is a critical design tool – not just a post design paper study to obtain a so-called “target SIL rating”.

MSA, Berlin • Phone: +49 (0)30 6886-0 • E-mail: info.de@MSAsafety.com