ITT

ENGINEERED FOR LIFE

Understanding Safety Integrity Levels (SIL) and its Effects for Field Instruments

by Gaurav Mathur

Product Manager (Industrial Switch Division)

Introduction

The Industrial process industry is experiencing a dynamic growth in Functional Process Safety applications. This growth has been driven by increased awareness of destruction of property, injuries and loss of life associated with tragic events that are widely publicized in mass media worldwide. The recent tragedies like the Gulf Oil spill, the fertilizer plant explosion in Texas; nuclear disasters etc. are recent live examples.

Companies have a moral and legal obligation to limit risk posed by their operations. In addition to their social responsibilities, the costs of litigation measuring in the billions of dollars have caught the eye of risk management executives worldwide. As a result, management recognizes the financial rewards of utilizing a properly designed process system that optimizes reliability and safety.

Hence companies are actively taking steps to comply with various national and worldwide safety standards such as ANSI/ISA 84 and IEC 61508/61511. To accomplish this, safety practitioners look to equipment specifically designed and approved for use in Safety Instrumented Systems that utilize Electrical and/or Electronic and/or Programmable (E/E/PE) technologies.

Safety Instrumented Systems (SIS) and functions (SIF)
A Safety Instrumented System (SIS) is designed to be used to implement one or more Safety Instrumented Functions (SIF).

SIS is composed of any combination of primary sensors (like Pressure & Temperature switches), controllers and final control elements for the purpose of taking a process to a safe state when predetermined conditions are violated. These SIS devices are designed and used to prevent or mitigate hazardous events to protect people or the environment or prevent damage to process equipment.

Typical Process Loop

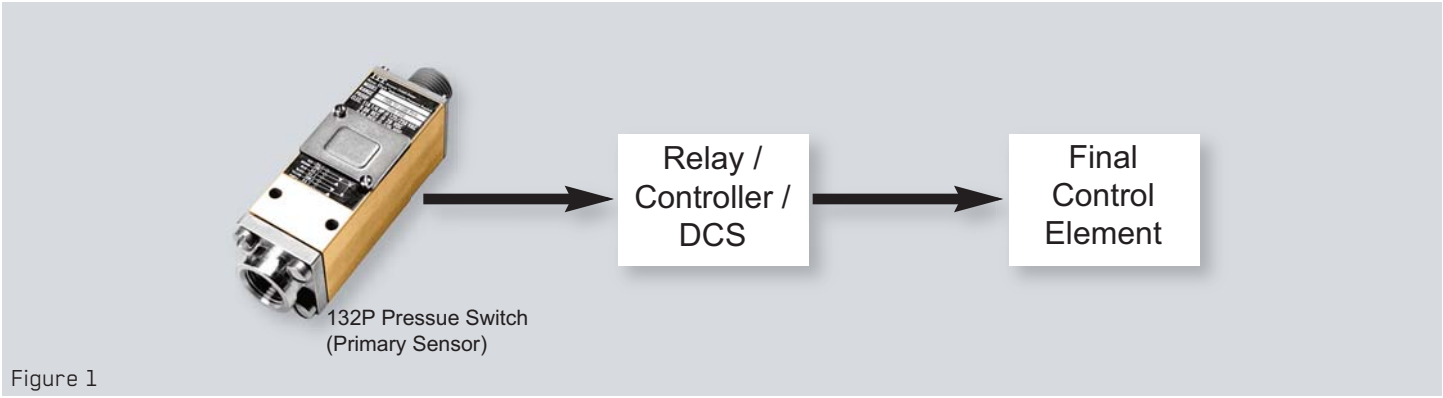

Figure 1

A SIF is a function to be implemented by a SIS that is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event.

Examples of SIF applications include:

- Emergency Shutdown applications in hazardous conditions
- On/ Off control to prevent tank overflow
- Critical loops with zero downtime tolerance
- Open a Valve to Relieve Excess Pressure
- Add Coolant to Arrest Exothermic Runaway
- Automatic Shutdown in absence of operator
- Close a Feed Valve to Prevent Tank Overflow
- Initiate Release of a Fire Suppressant
- Shutdown Fuel Supply to a Furnace

IEC 61508

Safety Integrity Level (SIL) means risk reduction to a tolerable level. To help companies implement a SIS, the International Electro-technical Commission (IEC) developed IEC 61508, the standard for "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems". IEC61508 is a standard that specifies both the risk assessment 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). It provides a design standard for Safety Instrumented Systems to reduce the risk to a tolerable level by following the overall hardware and software safety life cycle procedures, and by maintaining the associated stringent documentation.

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. IEC 61508 has become the benchmark used mainly by safety equipment suppliers to show that their equipment is suitable for use in Safety Integrity Level (SIL) rated systems.

For electro-mechanical products like Pressure and Temperature switches, manufacturers are performing a Failure Modes and Effects and Diagnostic Analysis – FMEDA; hardware only assessment which provides failure data for SIS designers and may also provide proven-in-use data. This does not include any assessment of the product development process which contributes to systematic faults in the product design.

Switches that are fully compliant with IEC 61508 address systematic faults by a full assessment of fault avoidance and fault control measures during hardware and software (if applicable) development.

Safety Integrity Level (SIL)

To determine a SIL, the safety practitioner team RISK/PROCESS HAZARD ANALYSIS (PHA) procedure identifies all process hazards, estimate their risks and decide if that risk is tolerable. Once a SIL has been assigned to a process, the safety practitioner has to verify that the individual components (in our case switches, controller/logic solvers, final elements, etc.) that are working together to implement the individual Safety Instrumented Functions (SIF) comply with the constraints of the required SIL.

Table 1. *The SIL is a measure of the amount of risk reduction provided by a Safety Instrumented Function, with SIL 4 having the highest level of safety integrity, and SIL 1 the lowest. Table 1 describes safety in three columns -- all mathematically related (e.g., RRF = 1/PFD).*

Safety Integrity Level (SIL)	Safety Availability	Probability of Failure on Demand Avg (PFD_{avg})	Risk Reduction Factor (RRF)
SIL 4	>99.99%	0.0001 to 0.00001	10,000 to 100,000
SIL 3	99.90% to 99.99%	0.001 to 0.0001	1,000 to 10,000
SIL 2	99.00% to 99.90%	0.01 to 0.001	100 to 1,000
SIL 1	90.00% to 99.00%	0.1 to 0.01	10 to 100

Safety Availability: The availability of a SIS to perform the task for which it was designed as presented in percentage (%) in order of magnitude steps from 90% to 99% for SIL 1 up through 99.99% to 99.999% for SIL 4.
Probability of Failure on Demand Average (PFD_{avg}): Likeihood that a SIS component will not be able to perform its safety action when called upon to do so. A SIL is based on a PFD average of the safety function.
Risk Reduction Factor (RRF): Defined as $1/PFD_{avg}$, the number of times that risk is reduced as a result of the application of a safeguard (typically a more convenient expression for describing SIF effectiveness than SIL or availability).

Table 2. *To be considered for a specific SIL level application, a Type A "Simple" device (such as a pressure/temperature switch), must achieve a defined SFF rating. The higher SFF permits SIL suitability, plus specifies redundancy levels at each level.*

Safety Failure Fraction (SFF)	Hardware Fault Tolerance (HFT) for Type A Device		
	0	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3
≥ 60%	SIL 2	SIL 3	SIL 4
≥ 90%	SIL 3	SIL 4	SIL4
≥ 99%	SIL 3	SIL 4	SIL 4

Safety Failure Fraction (SFF): The ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure of the subsystem.
Type A Device: A "Simple" device call faults known and describable per IEC 61508.
Hardware Fault Tolerance (HFT): A level of required devices redundancy. For example, a HFT of 1 means that there are at least 2 devices in the system and a dangerous failure of 1 device does not prevent the safety function from performing.

FMEDA/ FMEA Reports

The functions required for field instruments, which are the elements composing the safety instrumented system, are examined below, in consideration of the basic requirements that compose field instruments in IEC61508.

It is the safety instrumented systems' mission to enhance the safety of the process itself by reducing potential inherent risk factors. This is done by reducing the Probability of Failure on Demand (PFD), shown in Table 1. SIL is defined (per Table 1) depends on the PFD levels. A higher SIL means that a safer system can be achieved. For any device used in a SIS, the team must pay close attention to each device's Safety Failure Fraction (SFF) and Probability of Failure on Demand (PFD avg).

For each device in the SIF, both of these numbers have to be compared to the rules outlined in the safety standards to ensure that they are sufficient for use in the required SIL of the SIS. If these devices are classified as Type A, such as our Pressure and Temperature switches, the development process of electrical and mechanical hardware must be assessed and approved for the required SIL level. They do not have any diagnostics capability (no microprocessor) so the assessment will result in a Failure Modes and Effects Analysis (FMEA).

The equipment failures in terms of safety can be roughly divided into two categories: "Fail Safe" and "Fail Dangerous". Fail Safe failures mean those at the level of modules and subsystems inside a switch. For these failures, the system can be migrated to the safe side through automatic diagnoses by the diagnostic functions of the equipment. Failures in CPUs and ASICs correspond to this type of failure mode. On other hand, "Fail Dangerous" failures mean, for example, that an error in operational processes inside a switch cannot be found unless deviations in the relation between input and output signals is determined. Such a situation is very dangerous for the safety of the equipment. In other words, even if an abnormality occurs inside the switch, it appears to be working normally when viewed from the outside. In such a case, although the SIS must ignore the signal from this switch, the switch continues to be used without stopping because the abnormality cannot be detected, leading the system to a hazardous situation. For this reason, the above two failure modes are divided into detectable and undetectable elements, and SFF is determined on the rate of Fail Dangerous Undetected, the most dangerous element for safety.

The calculation methods defined in IEC61508 are shown below, and SFF is determined using these.

$$SFF = (\lambda SD + \lambda SU + \lambda DD)/(\lambda SD + \lambda SU + \lambda DD + \lambda DU)$$

Where:

SFF = Safety Failure Fraction

λSD : Fail Safe Detected

λSU : Fail Safe Undetected

λDD : Fail Dangerous Detected

λDU : Fail Dangerous Undetected

If SFF exceeds 60%, 90% or 99%, SIL 1, SIL 2 or SIL 3 is obtained respectively. IEC61508 permits self-declaration for SIL 1 but requires the third-party certification for SIL 2 and higher. Safety instrumented systems are increasingly adopted in the oil, gas, and petrochemical industries; there is a growing expectation of higher SIL where risk is lower. For this reason, the demand for field instruments having the certification of SIL 2 or more is increasing, additionally many end users prefer fully assessed devices by third party organizations.

It is always the responsibility of the end user to perform or verify the calculations for the entire safety loop. Since a SIF relies on more than one device, it is imperative that all devices in the loop work together to meet the required SIL levels. The device's SFF and the PFD avg values used for these calculations can be found in a FMEDA/FMEA report.

IEC 61508 requires a quantitative, as well as qualitative, assessment of risk. A Failure Modes and Effects Analysis (FMEA) provides a systematic way to assess the effects of all probable and known failure modes, including on-line monitoring and error checking, of a SIS component.

The detailed circuit and performance evaluation that estimates failure rates, failure modes and diagnostic capability of a device. This data provided is to be used by a competent functional safety practitioner to determine a device's applicability in a specific safety-related application. It is best if the FMEA report is certified by a well-qualified third-party agency that specializes in functional safety approvals.

Third Party Certifications

Today, there are solutions for SIS strategies and numerous possible mixes and configurations. An essential requirement to verify their design is a third-party certification from Exida TÜV or a similarly accredited approval body. This certification provides unbiased, verified evidence that the unit is appropriate for use in specific SIS strategies. For example, the certification may verify that the device is appropriate for SIFs up to SIL3 in a simplex or 1oo1 configuration.

The electro-mechanical switch (Pressure and Temperature switch) family fits into this scenario. They provide an extremely affordable option that delivers simple installation, easier validation and faster start-ups. Perpetual benefits that last for the life of the system include less maintenance, faster testing, easier documentation of the safety management reports and modular replacement strategies.

About ITT

ITT Neo-Dyn® provides standard Industrial Pressure switches, Vacuum switches, Differential switches, Temperature switches, Sanitary switches, Switch Accessories and custom switches for the industrial, chemical process, and energy markets. ITT's global resources, six-sigma and lean manufacturing provide ITT Neo-Dyn® the resources to stay at the forefront of new technologies, research & development as and high quality production for our customers around the world. For more information, visit *www.neodyn.com*.

ITT is a diversified leading manufacturer of highly engineered critical components and customized technology solutions for growing industrial end-markets in energy infrastructure, electronics, aerospace and transportation. Building on its heritage of innovation, ITT partners with its customers to deliver enduring solutions to the key industries that underpin our modern way of life. Founded in 1920, ITT is headquartered in White Plains, N.Y., with employees in more than 30 countries and sales in a total of approximately 125 countries. The company generated 2012 revenues of $2.2 billion.

Author Gaurav Mathur is the Product Line Manager for ITT Neo-Dyn®, if you have questions or comments regarding this article, please contact him via email at Gaurav.Mathur@itt.com or via telephone at 661-295-4166.