Safety Instrumented Systems

Safety Layers and Protections

Safety is provided by layers of protection (see figure 1). These layers of protection start with effective process control, extend to manual and automatic safety prevention layers, and continue with layers to mitigate the consequences of an event.

The first layer is the basic process control system (BPCS). The process control system itself provides significant safety through proper design of process control.

The next layer of protection is also provided by the control system and the control system operators.

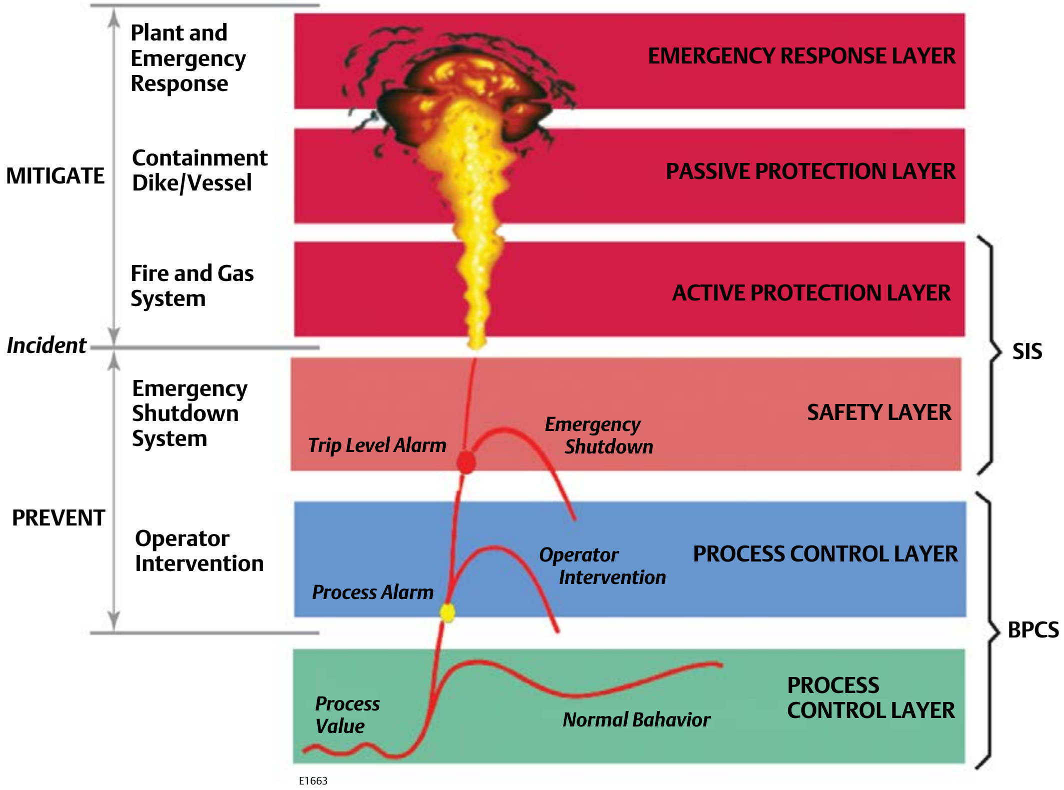
Automated shutdown routines in the process control system combined with operator intervention to shut down the process are the next layer of safety.

Next is the safety instrumented system.

It is a safety system independent of the process control system. It has separate sensors, valves, and a logic solver. Its only role is safety. No process control is performed in this system.

Operator intervention and the safety instrumented system layers are designed to prevent a safety-related event. If a safety-related event occurs, there are additional layers designed to mitigate the impact of the event.

Figure 1. Layers of Protection



The next layer is an active protection layer. This layer may have valves or rupture disks designed to provide a relief point that prevents an uncontrolled release that can cause an explosion or fire.

The next layer is a passive protection layer. It may consist of a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.

The final layer is plant and emergency response. If a large safety event occurs this layer responds in a way that minimizes ongoing damage, injury, or loss of life. It may include evacuation plans, firefighting, etc.

Overall safety is determined by how these layers work together.

Safety Instrumented Systems (SIS)

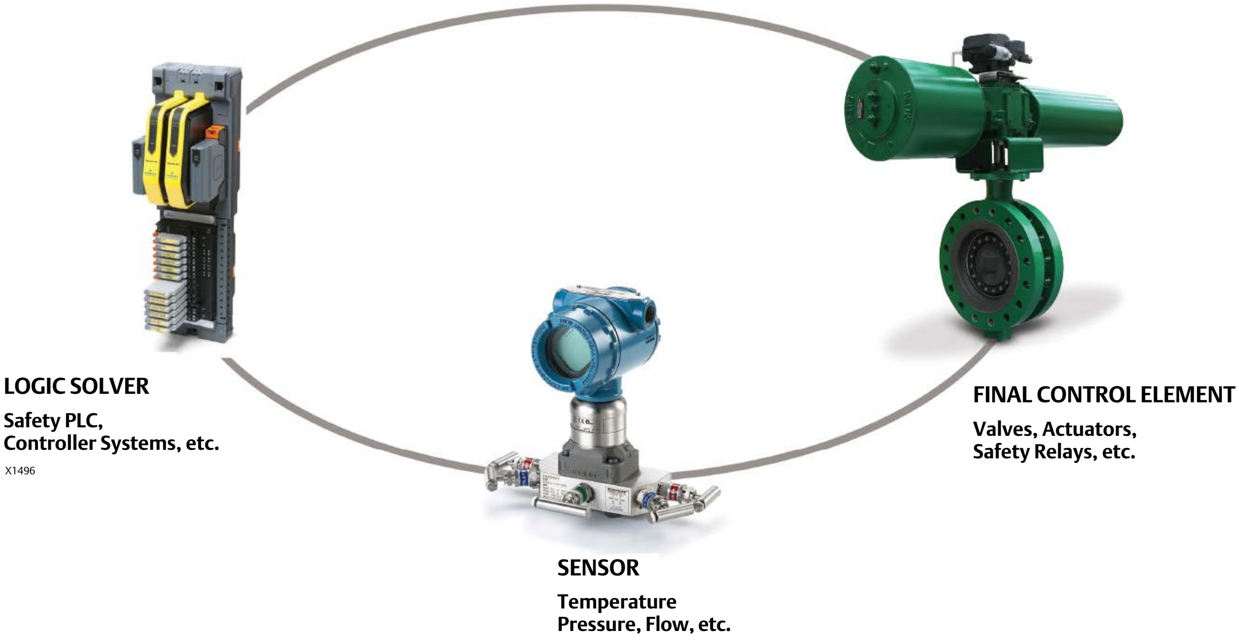
A safety instrumented system (SIS) is considered separate than the basic process control system (BPCS) in that the SIS is dedicated to taking the process to a “safe state” should a critical situation occur.

The SIS consists of several safety instrumented functions (SIF). Each safety instrumented function has a specified safety integrity level (SIL), which is necessary to achieve functional safety. Each SIF is a separate or interlinked loop comprised of sensors, logic solver (LS), and final control element (FE) as shown in figure 2.

Sensors: Field sensors are used to collect information necessary to determine if an emergency situation exists. The purpose of these sensors is to measure process parameters (i.e. temperature, pressure, flow, density etc.) to determine if the equipment or process is in a safe state. Sensor types range from simple pneumatic or electrical switches to smart transmitters with on-board diagnostics. These sensors are dedicated to SIS service and have process taps, which are separate and distinct from the process taps used by normal process information sensors.

Logic Solver: The purpose of this component of SIS is to determine what action is to be taken based on the information gathered. Highly reliable logic solvers are used which provide both fail-safe and fault-tolerant operation. It is typically a controller that reads signals from the sensors and executes pre-programmed actions to prevent a hazard by providing output to final control element(s). Logic solvers are very often programmable or non- programmable devices, but can also be mechanical in form of switched set to trip the safety function.

Figure 2. Components of a Safety Instrumented System



Final Control Element: Final control elements implement the action determined by the logic solver. This final control element is typically an automated on/off valve, with a valve fail- closed or fail-open function.

It is imperative that all three elements of the SIS function as designed in order to safely isolate the process plant in the event of an emergency.

Safety Standards

In a process plant, there is no such thing as risk-free operation or 100% reliability. Therefore, one of the first tasks of the SIS designer is to perform a risk- tolerance analysis to determine what level of safety is needed. IEC Standard 61508 (Functional Safety of Electric, Electronic and Programmable Electronic Systems) is a general standard that covers functional safety related to all kinds of processing and manufacturing plans. IEC Standard 61511 and ISA S84.01 (Replaced by ISA 84.00.01-2004) are standards specific to the process industries. All three standards use a performance-based lifecycle model and specify precise levels of safety, best practices, and quantifiable proof of compliance.

Safety Integrity Level (SIL)

Safety integrity levels (SIL) are quantifiable measurement of risk. Since they were first introduced, safety integrity levels have been used as a quantifiable way to establish safety performance targets for SIS systems. IEC standards specify four possible Safety Integrity Levels (SIL 1, SIL 2, SIL 3, SIL 4) as shown in table 1; however, ISA S84.01 only recognizes up to SIL 3.

A determination of the target Safety Integrity Level requires:

- An identification of the hazards involved.
- Assessment of the risk of each of the identified hazards.
- An assessment of other Independent Protection Layers (IPLs) that may be in place.

Hazards can be identified using a number of different techniques; one common technique is a HAZard and OPerability study (HAZOP).

A risk factor must then be determined for each of the defined hazards, where risk is defined as a function of the probability (likelihood or frequency) and consequences (severity) of each hazardous event.

The HAZOP study is used to identify the risk to personnel or the environment and is carried out by a multi-disciplinary team (HAZOP team).

Once the risk is identified, the HAZOP/ process hazard study (PHA) will set the requirement for risk reduction, thus define the required SIL Level.

Table 1. Safety Integrity Levels and Associated PFD_{avg} and RRF Figures

RRF (Risk Reduction Factor)	PFD_{avg} (Probability of Failure on Demand = 1/RRF)	SIL (Safety Integrity Level)
100000 to 10000	>=10^{-5} to <10^{-4}	4
10000 to 1000	>=10^{-4} to <10^{-3}	3
1000 to 100	>=10^{-3} to <10^{-2}	2
100 to 10	>=10^{-2} to <10^{-1}	1

Additional criteria need to be verified to ensure the SIF meets the required SIL, and they are often divided into the following points:

- Systematic integrity: All elements of the SIF need to be capable being used for the defined SIL level.
- Architectural constraints: Hardware Fault Tolerance (HFT) and redundancy of the architecture need to comply with current functional safety standards.
- Random integrity (PFDavg): The failure rates of the individual devices will be used to calculate the average probability of failure on demand.

Probability of Failure Upon Demand

By understanding how the components of the SIS system can fail, it is possible to calculate a probability of failure on demand (PFD). There are two basic ways for the SIS to fail. The first way is commonly called a nuisance or spurious trip, which usually results in an unplanned but relatively safe process shutdown. While there is minimal danger associated with this type of SIS failure, the operational costs can be enormous. The second type of failure does not cause a process shutdown or nuisance trip. Instead, the failure remains undetected, permitting continued process operation in an unsafe and dangerous manner. If an emergency demand occurred, the SIS system would be unable to respond properly. These failures are known as covert or hidden failures and contribute to the probability (PFD) of the system failing in a dangerous manner on demand.

The PFD for the SIS system is the sum of PFDs for each element of the system:

$$PFD_{total} = PFD_{sensor} + PFD_{logic\ solver} + PFD_{final}$$

In order to determine the PFD of each element, the analyst needs documented failure rate data for each element. This failure rate (dangerous) is used in conjunction with the test interval (TI) term to calculate the PFD. It is this test interval that accounts for the length of time before a covert fault is discovered through testing. Increasing the test interval directly impacts the PFD value in a linear manner; i.e., if you double the interval between tests, you will double the probability for failure on demand, and make it twice as difficult to meet the target SIL.

The governing standards for safety instrumented systems state that plant operators must determine and document that equipment is designed, maintained, inspected, tested, and operated in a safe manner. Thus, it is imperative that these components of safety instrumented system be tested frequently enough to reduce the PFD and meet the target SIL.

Neither Emerson, Emerson Automation Solutions, nor any of their affiliated entities assumes responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use, and maintenance of any product remains solely with the purchaser and end user.

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available upon request. We reserve the right to modify or improve the designs or specifications of such products at any time without notice.

Emerson Automation Solutions
Marshalltown, Iowa 50158 USA
Sorocaba, 18087 Brazil
Cernay, 68700 France
Dubai, United Arab Emirates
Singapore 128461 Singapore

www.Fisher.com

EMERSON.