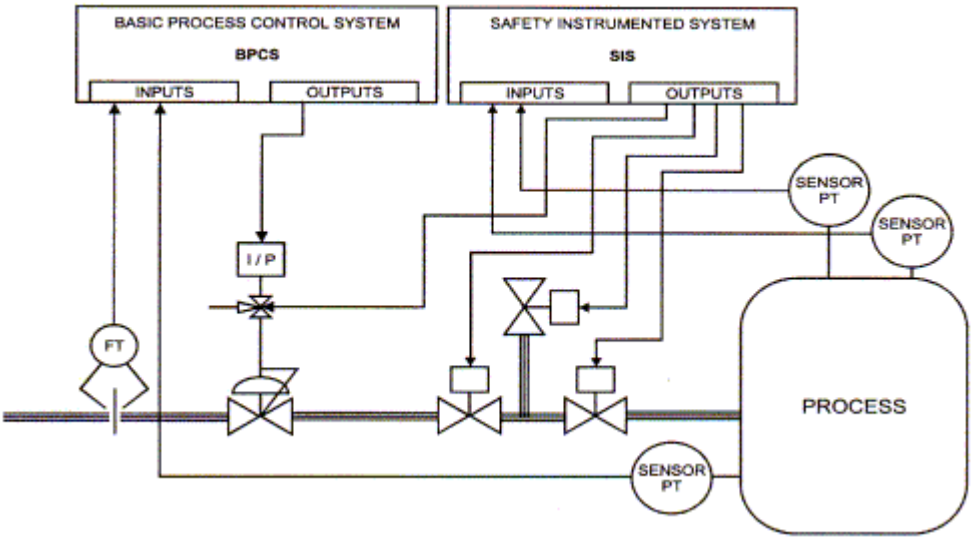
Safety Instrumented Systems

What is a Safety Instrumented System?

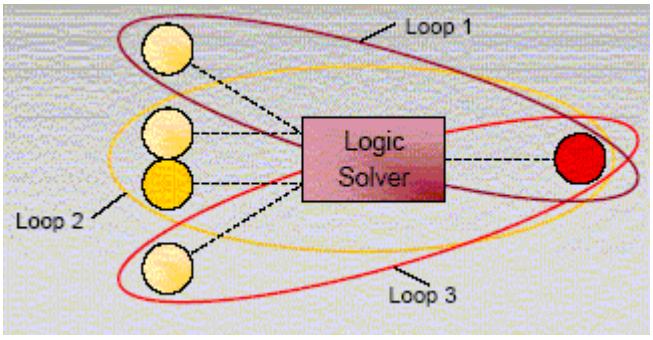
A **Safety Instrumented System SIS** is a new term used in standards like IEC 61511 or IEC 61508 for what used to be called Emergency Shutdown System ESD, Safety Shutdown System, Interlock System, Permissive Systems, etc. ...

A Safety Instrumented System SIS consists of one or more Safety Instrumented Functions SIF.



What is a Safety Instrumented Function SIF?

A **Safety Instrumented Function SIF** is defined as a „Function to be implemented by a SIS, which is intended to achieve or maintain a safety state for the process with respect to a specific hazardous event"



What is a Safety Integrity Level SIL?

Safety Integrity Level SIL is a measure of risk reduction provided by a SIF based on four levels. Each level represents an order of magnitude of risk reduction. Every SIF has a SIL assigned to it, the SIS and equipment does not have a SIL assigned to it.

SIL Safety Integrity Level	**RRF** Risk Reduction Factor	**PFD** Probability of Failure on Demand pro year = 1/RRF
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

Basic Fundamentals of Safety Instrumented Systems SIS

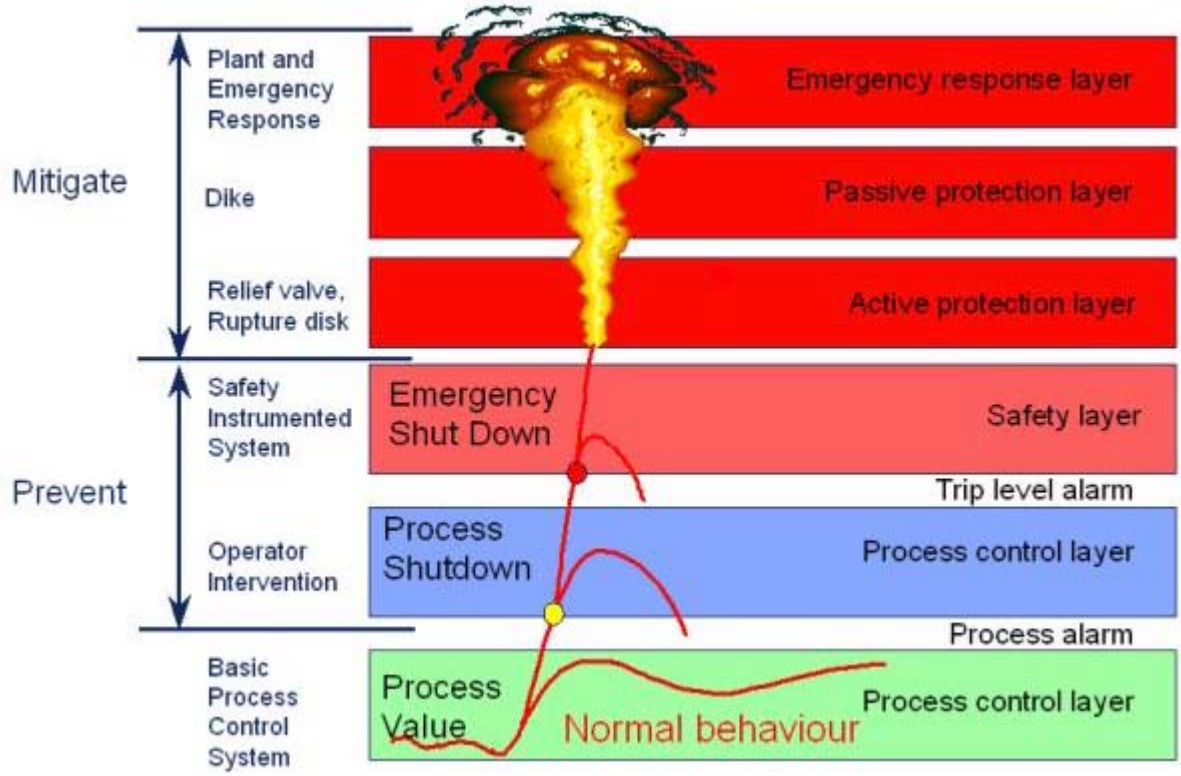
Basic Fundamentals of Safety Instrumented Systems SIS

The operation of many industrial processes involve inherent risks due to the presence of dangerous material like gases and chemicals. Safety Instrumented Systems SIS are specifically designed to protect personnel, equipment and the environment by reducing the likelihood (frequency) or the impact severity of an identified emergency event.

Explosions and fires account for millions of dollars of losses in the chemical or oil and gas industries each year. Since a great potential for loss exists, it is common to employ Safety Instrumented Systems SIS to provide safe isolation of flammable or potentially toxic material in the event of a fire or accidental release of fluids.

This online training tutorial will explain the basic concepts, definitions and commonly used terms in Safety Instrumented Systems SIS and provide a basic understanding of related concepts.

Basics of Safety and Layers of Protection



Safety is provided by layers of protection. These layers start with safe and effective process control, extend to manual and automatic prevention layers, and continue with layers to mitigate the consequences of an event.

The first layer is the Basic Process Control System BPCS. The 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 system operators. Automated shutdown sequences in the process control system combined with operator intervention to shut down the process are the next layer of safety.

The third layer is the Safety Instrumented System SIS. It is a safety system independent of the process control system. It has separate sensors, valves and logic system. No process control is performed in this system, its only role is safety.

These 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.

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

The fifth 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, fire fighting, etc.

Overall safety is determined by how these layers work together.

Basics of Safety Instrumented Systems SIS

Typically, Safety Instrumented Systems consist of three elements: A Sensor, a Logic Solver and a Final Control Element

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 (e.g. temperature, pressure, flow, etc.) used 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 the Safety Instrumented System SIS.

Logic Solver:
The purpose of this component of Safety Instrumented Systems 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 elements.

Final Control Element:
It implements the action determined by the logic system. This final control element is typically a pneumatically actuated On-Off valve operated by solenoid valves.

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

Probability of Failure upon Demand PFD

By understanding how components of an Safety Instrumented System SIS can fail, it is possible to calculate a Probability of Failure on Demand PFD. There are two basic ways for SIS to fail. The first way is commonly called a spurious trip which usually results in an unplanned but safe process shutdown. While there is no danger associated with this type of SIS failure, the operational costs can be very high. The seconf type of failure does not cause a process shutdown or nuisance trip. Instead, the failure remains undetected, permitting continued process operation in an unsafe or dangerous manner. If an emergency demand occurred, the SIS 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 Safety Instrumented System SIS is the sum of PFD's for each element of the system. In order to determine the PFD of each element, the analyst needs documented, historic 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 the test interval TI that accounts for the length of time before a covert fault is discovered through testing. Increases in the test interval directly impact the PFD value in a linear manner; e.g. if you double the interval between tests, you will double the Probability of Failure on Demand, and make it twice as difficult to meet the target Safety Integrity Level SIL.

The governing standards for Safety Instrumented Systems SIS 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 Systems be tested frequently enough to reduce the PFD and meet the target SIL.

****

For more details see the files at “Fieldbus Class Room Safety Lifecycle Management 1.15Mb

****

IEC Safety Standards

IEC 61511

This international standard gives reqirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the processin a safe state.

IEC 61508

The function of an industrial safety instrumented system SIS is to automatically shutdown the process if a dangerous condition is detected. Although different kinds of equipment are used, there is a strong trend towards the use of programmable electronic equipment (processor based logic). For these systems to be certified for use inn certain types of safety applications, they must meet the standards IEC 61508 and ANSI/ISA 84.01 for functional safety.

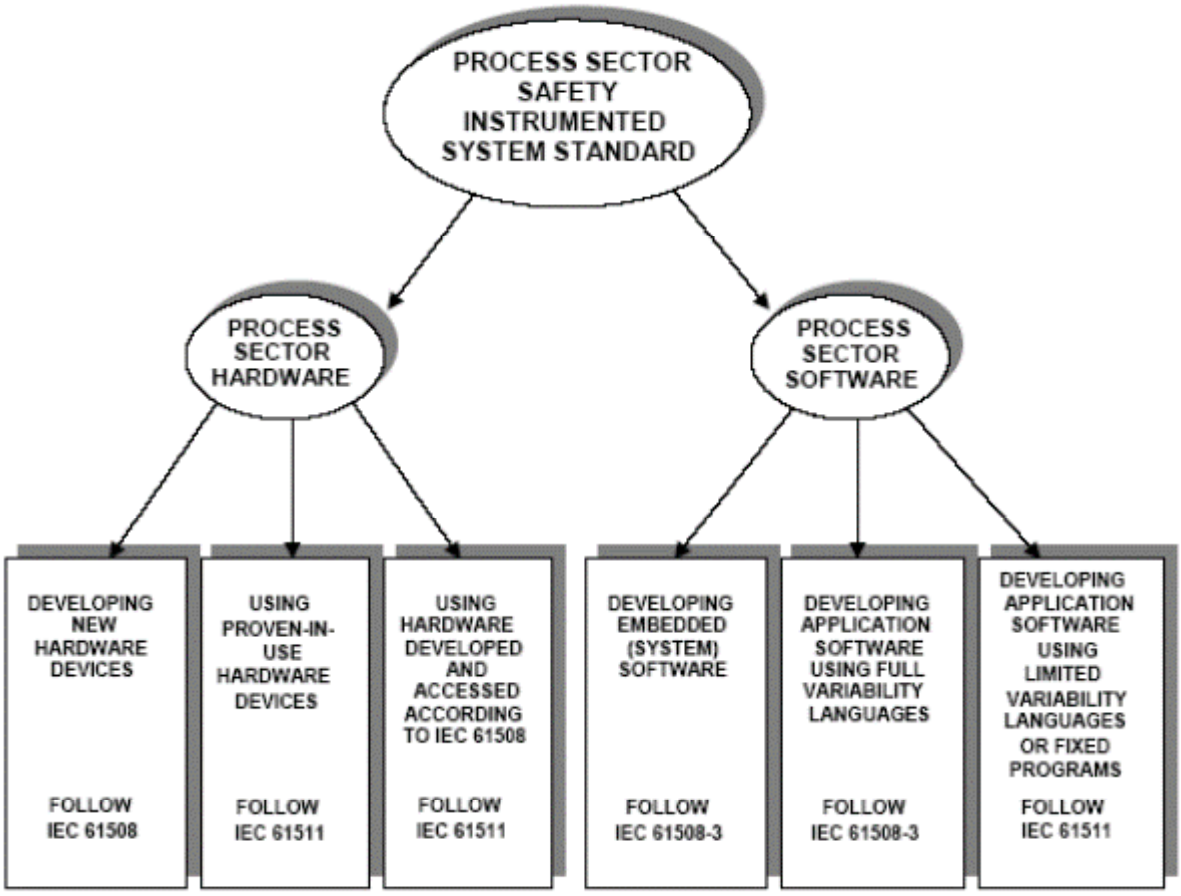


Figure: Relationship between IEC 61511 and IEC 61508

SIS Safety Instrumented Systems

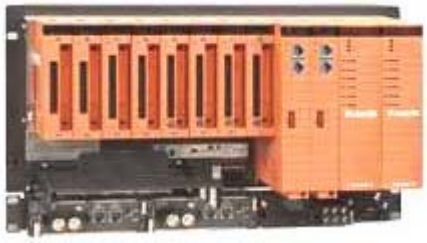
SIS Safety Instrumented Systems

Today SIS Safety Instrumented Systems play an increasingly important role in many process plants. Safety standards such as IEC 61508, IEC61511 and ISA S84.01, are creating more stringent safety requirements for process plants.

Depending on application use, other names used for SIS Safety Instrumented Systems are:
Emergency Shutdown Systems (ESD), Burner Management Systems (BMS), Fire and Gas Systems (F&G), Critical Turbomachinery Control, Railway Switching, Semiconductor Life Safety Systems (SEMI S2), Nuclear 1E Safety Systems, High Integrity Protection Systems (HIPS), High Integrity Pressure Protection System (HIPPS)

|

Yokogawa - ProSafe-RS



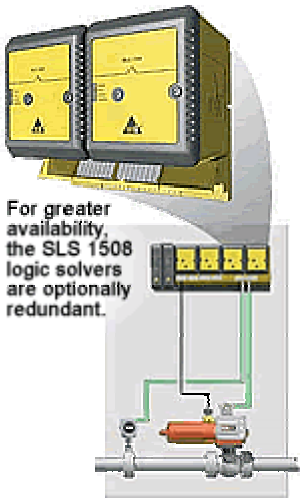
Yokogawa / ProSafe-RS

Achieving absolute integrity between distributed control systems (DCS) and safety instrumented systems (SIS) for plant automation has traditionally raised complex design and integration issues.

Conventionally, two separate monitoring and operating environments were required for a DCS and SIS. Different communications and distinctive hardware architectures had to be set up. Plant managers striving to optimize process operations have taken it as a given that project time and expenses would escalate.

Now Yokogawa puts an end to DCS-SIS incompatibility with the new ProSafe-RS, the world's first truly integrated "safety PLC" for the process industries.

Emerson - DeltaV SLS-1508



Emerson Process Management / DeltaV SLS-1508

Emerson extends the proven innovations of their PlantWeb® architecture to safety applications.

The resulting smart safety instrumented system provides an integrated approach to complete safety loops - from sensor to logic solver to final control element.

It also uses digital intelligence and diagnostics to enable more automated safety loop testing and other features that increase system availability while reducing life-cycle costs and easing regulatory compliance.

As a key component of this smart SIS solution, the DeltaV SIS system takes advantage of the PlantWeb architecture's digital communications and smart diagnostics within field devices to increase the availability of the whole of the Safety Instrumented Function. Scheduled partial-stroke testing of final control elements can improve the safety level, reduce the number of risky personnel trips into the field, and increase the mandatory proof test interval.

Ivensys Triconex - Tricon

Ivensys Triconex / Tricon

The TRICON is a state-of -the-art fault tolerant controller based on a Triple-Modular Redundant (TMR) architecture. TMR employs three isolated, parallel control systems and extensive diagnostics integrated into one system. The system uses two-out-of-three voting to provide high integrity, error-free, uninterrupted process operation with no single point of failure.

Setting up applications is simplified with the TRICON, because the Triplicated TMR system operates as a single control system from the user's point of view. The extensive diagnostics are inherent and transparent to the programmer. All diagnostic information is stored in system variables and annuniciated with Light Emitting Diode (LED) indicators.

The Tricon controller can interface with Modbus masters and slaves, Distributed Control Systems (DCS), external host computers on Ethernet networks and other Tricon on a Peer-to-Peer network.

The TriStation 1131 Developer's Workbench is an integrated tool for developing, testing, and documenting safety and critical process control applications for the Tricon and Trident programmable logic controllers. The programming methodology, user interface, and self-documentation capabilities make the system superior to traditional and competing engineering tools.