Safety Instrumented Systems

The Need for Safety Instrumentation

- Safety Systems Engineering(SSE) describes a disciplined, systematic approach, which encompasses hazard identification, safety requirements specification, safety systems design and build, and systems operation and maintenance over the entire lifetime of plant.

Risk and Risk Reduction Methods

- Safety can be defined as “freedom from unacceptable risk”.

Risk = Hazard Frequency X **Hazard Consequence**

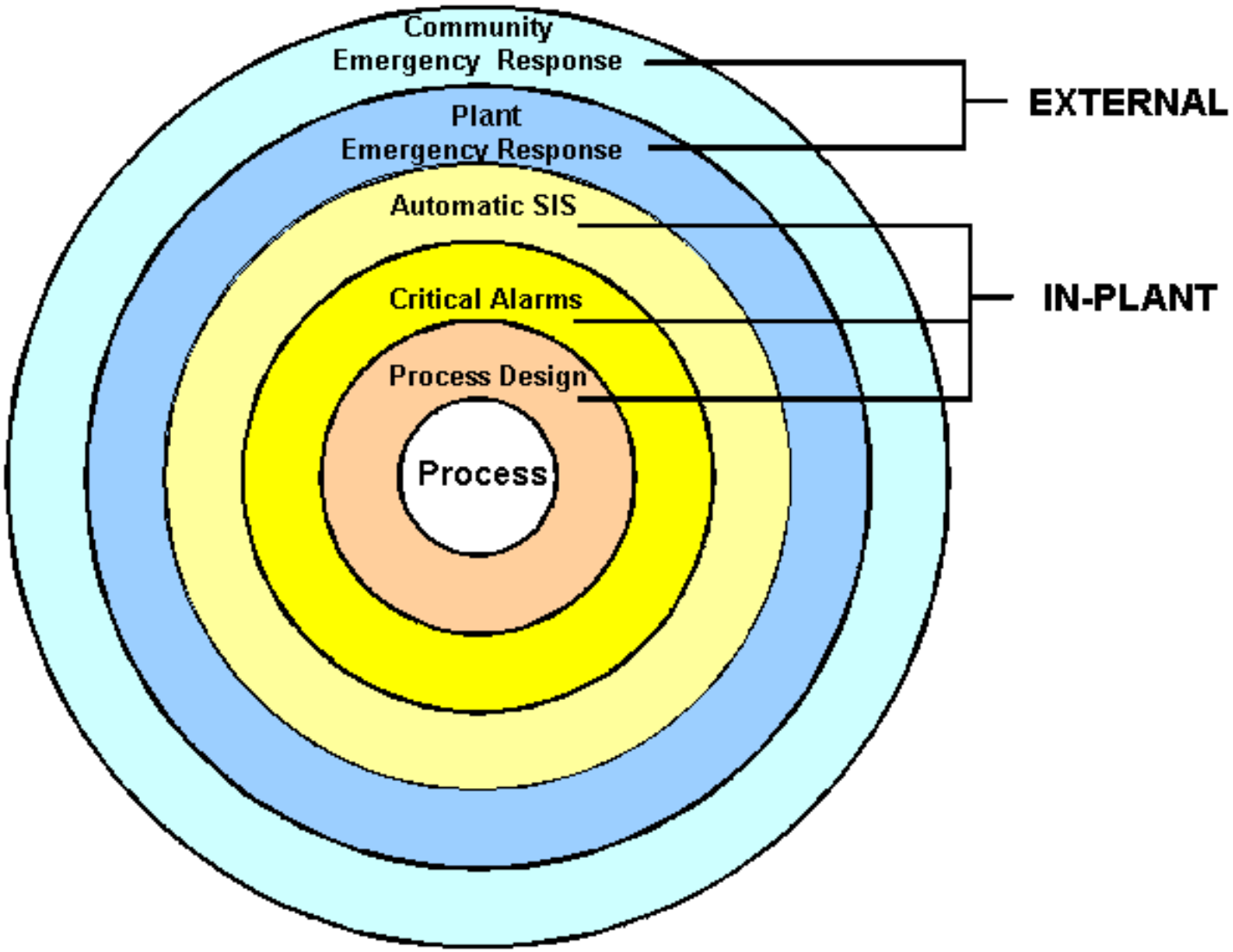
- Absolute safety, where risk is completely eliminated, can never be achieved; risk can only be reduced to an acceptable level.

- Therefore all risks should be dealt with on the ALARP basis, i.e. the target is to ensure that risk is reduced to As Low As Reasonably Practicable.
- Risk can be minimized initially by inherently safe process design, by the **Basic Process Control System** (**BPCS**), and finally by a safety shutdown system.

Safety Methods

- Changing the process or engineering design
- Increasing mechanical integrity of the system
- Improving the Basic Process Control System (BPCS)
- Developing detailed training and operational procedures
- Increasing the frequency of testing of critical system components
- Using a safety Instrumented System (SIS)
- Installing mitigating equipment

Safety Protective layers



Hazards Analysis

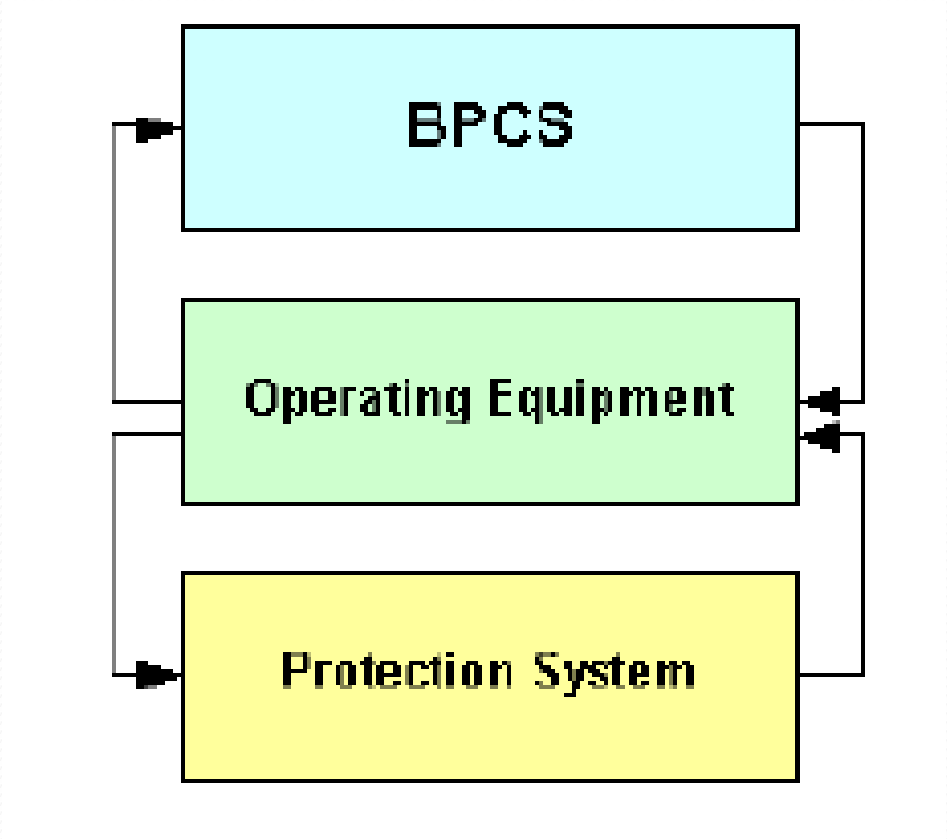
- The levels of protective layers required is determined by conducting an analysis of a process's hazards and risks known as a **Process Hazards Analysis** (**PHA**).
- Depending upon the complexity of the process operations and the severity of its inherent risks, such an analysis may range from a simplified screening to a rigorous **Hazard and Operability** (**HAZOP**) engineering study, including reviewing process, electrical, mechanical, safety, instrumental and managerial factors.

- Once risks and hazards have been assessed, it can be determined whether they are below acceptable levels. If the study concludes that existing protection is insufficient, a **Safety Instrumented System** (**SIS**) will be required.

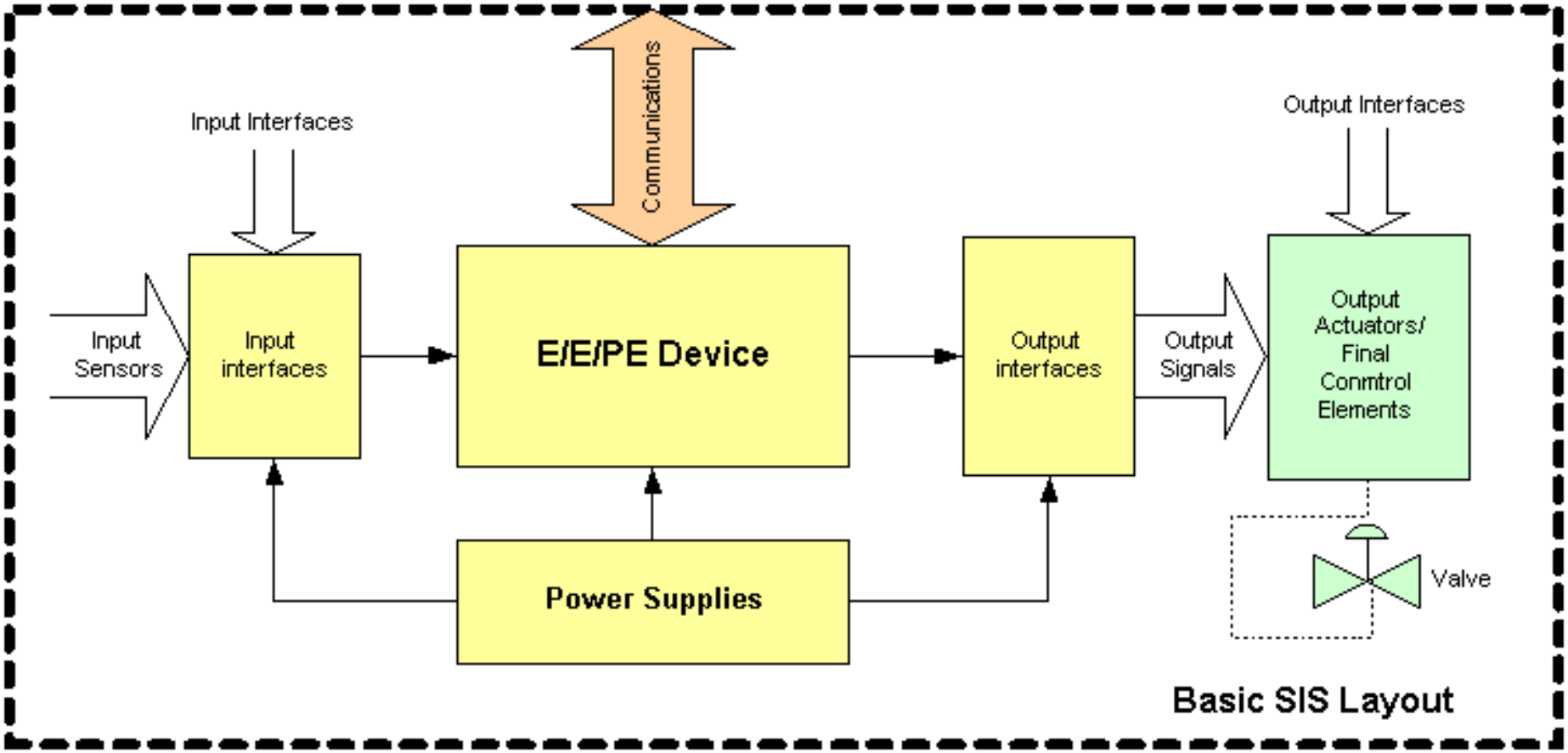
Safety Instrumented Systems

- A SIS is a system comprising sensors, logic solvers and actuators for the purposes of taking a process to a safe state when normal predetermined set points are exceeded, or safe operating conditions are violated.
- SISs are also called emergency shutdown (ESD) systems, safety shutdown (SSD) systems, and safety interlock systems.

Separation of BPCS and Protection System



Basic SIS Layout



- The basic SIS layout comprises

• Sensor(s) for signal input and power

• Input signal interfacing and processing

• Logic solver with associated communications and power

• Output signal processing, interfacing and power

• Actuators and valve(s) or switching devices to provide the final control element Function.

- The scope of a SIS encompasses all instrumentation and controls that are responsible for bringing a process to a safe state in the event of an unacceptable deviation or failure.

Standards – IEC 61508, IEC 61511 and ANSI/ISA S84

- IEC 61508:Functional Safety of Electrical, Electronic and Programmable Electronic Safety related Systems is a generic standard on which sector specific safety standards are to be based.

- Can apply to a range of Electrical /Electronic/ Programmable Electronic (E/E/PES)safety-related systems including:
- Emergency Shut-Down (ESD) systems,
- Fire and gas systems,
- Turbine control,
- Gas burner management,
- Dynamic positioning
- Railway signaling systems,
- Machinery guarding & interlock systems.

IEC 61508: Parts and Headings	
Part 1, December 1998	General requirements
Part 2, May 2000	Requirements for E/E/PE Safety Related Systems
Part 3, December 1998	Software requirements
Part 4, December 1998	Definitions and abbreviations
Part 5, December 1998	Examples of methods for determination of SIL
Part 6, April 2000	Guidelines on the application of IEC 61508-2 and 61508-3
Part 7, March 2000	Overview of techniques and measures

Table 1 – IEC 61508 Standard Parts and Headings

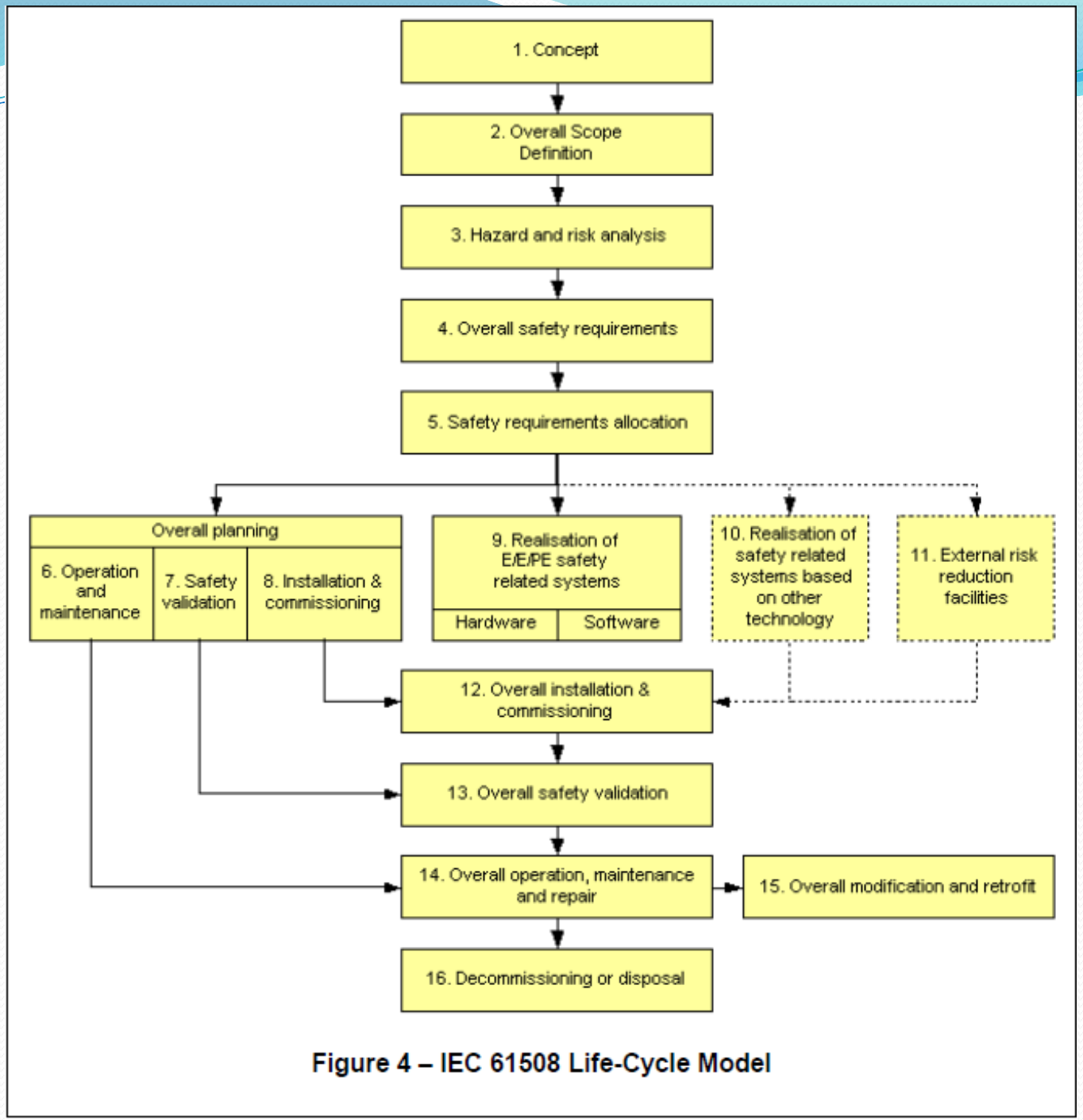


Figure 4 – IEC 61508 Life-Cycle Model

Safety Integrity Level (SIL)

- A statistical representation of the safety availability of an SIS at the time of process demand. It is at the heart of acceptable SIS design and includes the following factors:

- Device integrity
- Diagnostics
- Systematic and common cause failures
- Testing
- Operation
- Maintenance

Safety Availability

- The safety availability (i.e. proportion of time that the system is operational) of a SIS depends on
- Failure rates and Failure modes of components
- Redundancy
- Voting scheme(s) adopted
- Testing frequency

Safety Instrumented Functions **SIF**

- **SIF** is a safety function with a specified Safety Integrity Level which is implemented by a SIS in order to achieve or maintain a safe state.
- A SIF's sensors, logic solver, and final elements act in concert to detect a hazard and bring the process to a safe state.

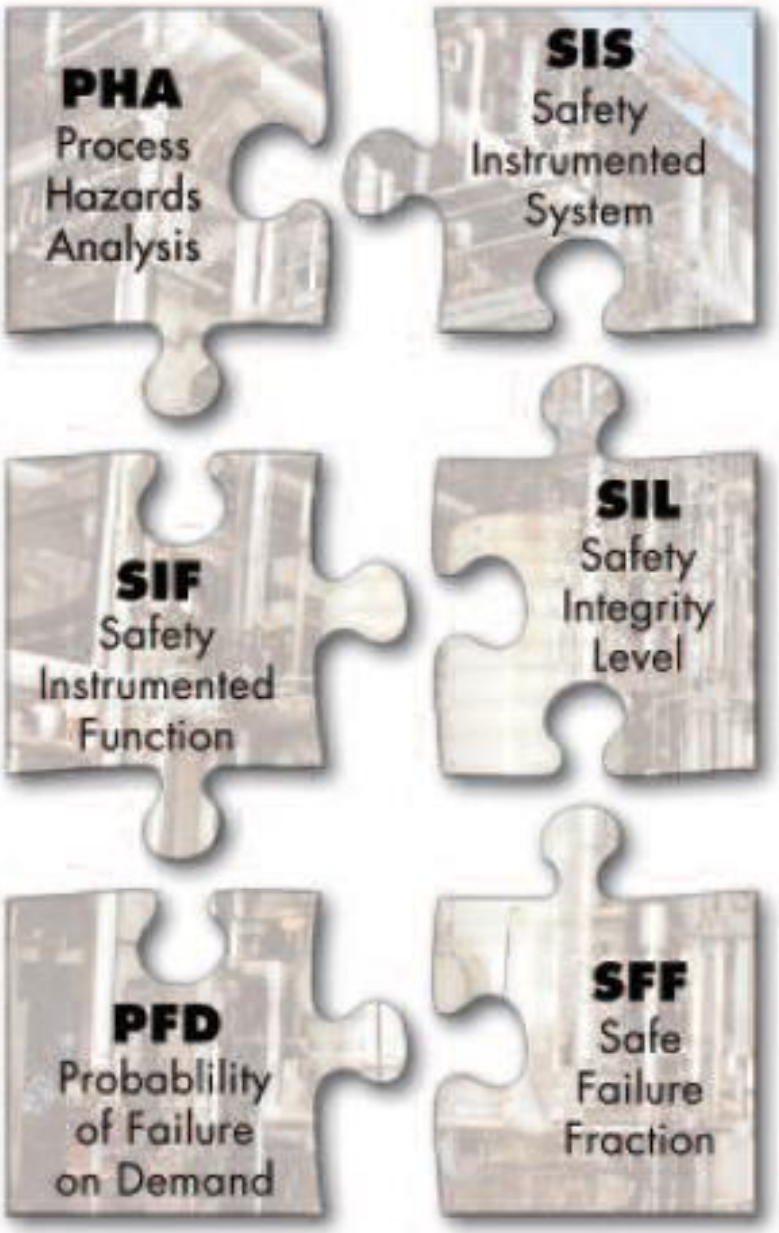
Process Hazards Analysis **PHA**

- It is an analysis of the process that may range from a simplified screening to a rigorous Hazard and Operability (HAZOP) engineering study.
- PHA will determine the need for a SIS.

Safety Instrumented System **SIS**

- Its purpose is to take process to a “safe state” when pre-determined set points have been exceeded or when safe operating conditions have been transgressed. It does so by utilizing SIFs.

IEC 61508/61511



Safety Instrumented Function **SIF**

- One loop within the SIS which is designed to achieve or maintain a safe state.
- A SIF's sensors, logic solver, and final control elements act in concert to detect a hazard and bring the process to a safe state.
- What devices are used in the SIF are based on their required SIL.

Probability of Failure on Demand **PFD**

- The probability a device will fail to perform its required function when it is called upon to do so.
- The average PFD (PFDavg- failure rate of all elements within a Safety Instrumented Function) is used for SIL evaluation.

Safe Failure Fraction **SFF**

- A number that shows the percentage of possible failures that are self-identified by the device or are safe and have no effect.
- The key number in this calculation is Dangerous
- Undetected failures—those that are not identified and do have an effect.