Safety Instrumented System

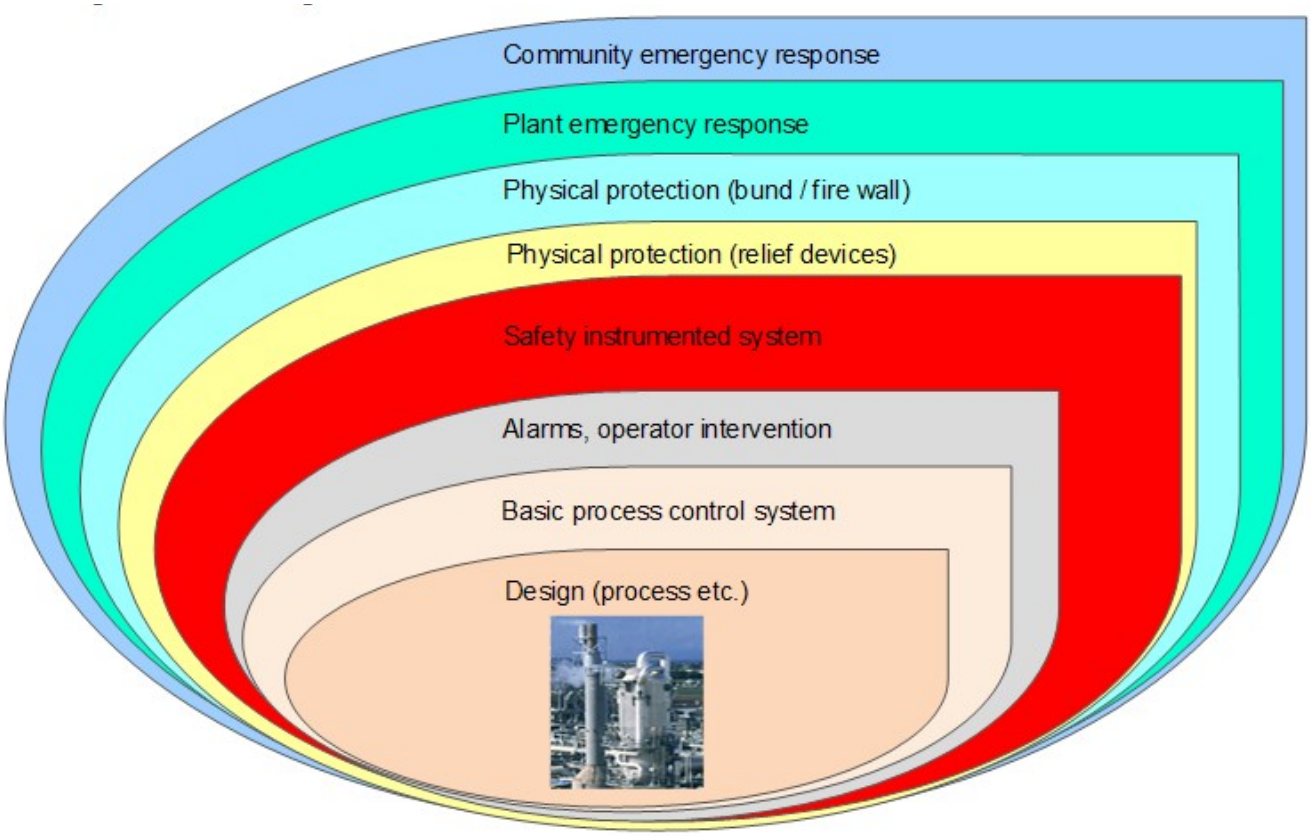
HW 2

Name: Mustafa Essam Ayman Ismail

ID: 5295 5837

INTRODUCTION

Ensuring that a presses or a plant is safe is made up of many layers. Plant design is at the core of plant safety. The Basic Process Control System (BPCS) comes next, followed by operator intervention, alarm systems, and the Safety Instrumented System (SIS). The SIS is an important layer of protection because it can provide the highest level of protection when compared with other layers shown in the figure below.



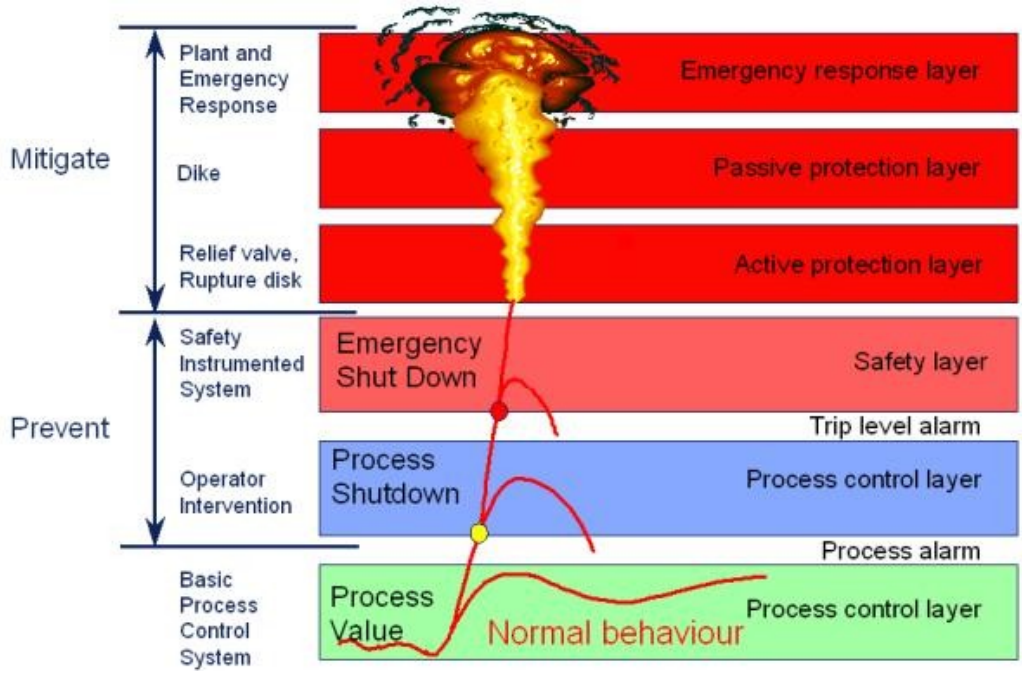
A **Safety Instrumented System (SIS)** consists of an engineered set of hardware and software controls which are especially used on critical process systems. A critical process system can be identified as one which, once running and an operational problem occurs, may need to be put into a "Safe State" to avoid adverse Safety, Health and Environmental(SH&E) consequences. Examples of critical processes have been common since the beginning of the Industrial Age. One of the more well-known critical processes is the operation of a steam boiler. Critical parts of the process would include the lighting of the burners, controlling the level of water in the drum and controlling the steam pressure.

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.

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.

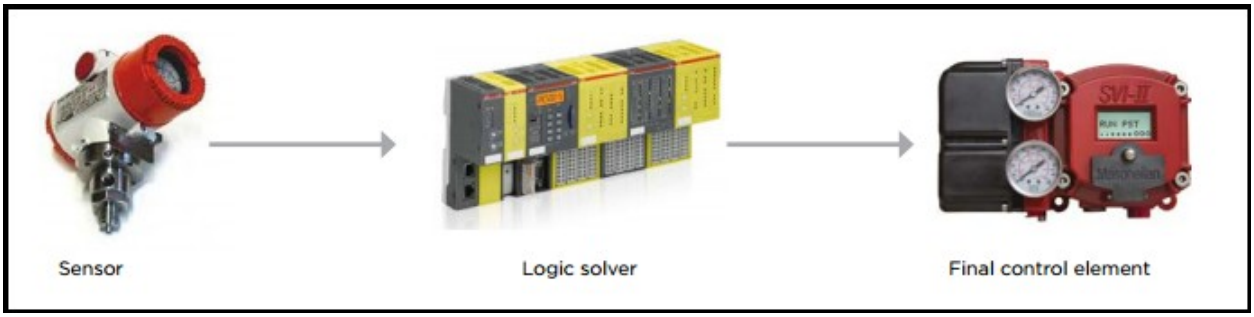
The fifth layer is a passive protection layer. It may consist of a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.

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, firefighting, 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 a 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 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 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.

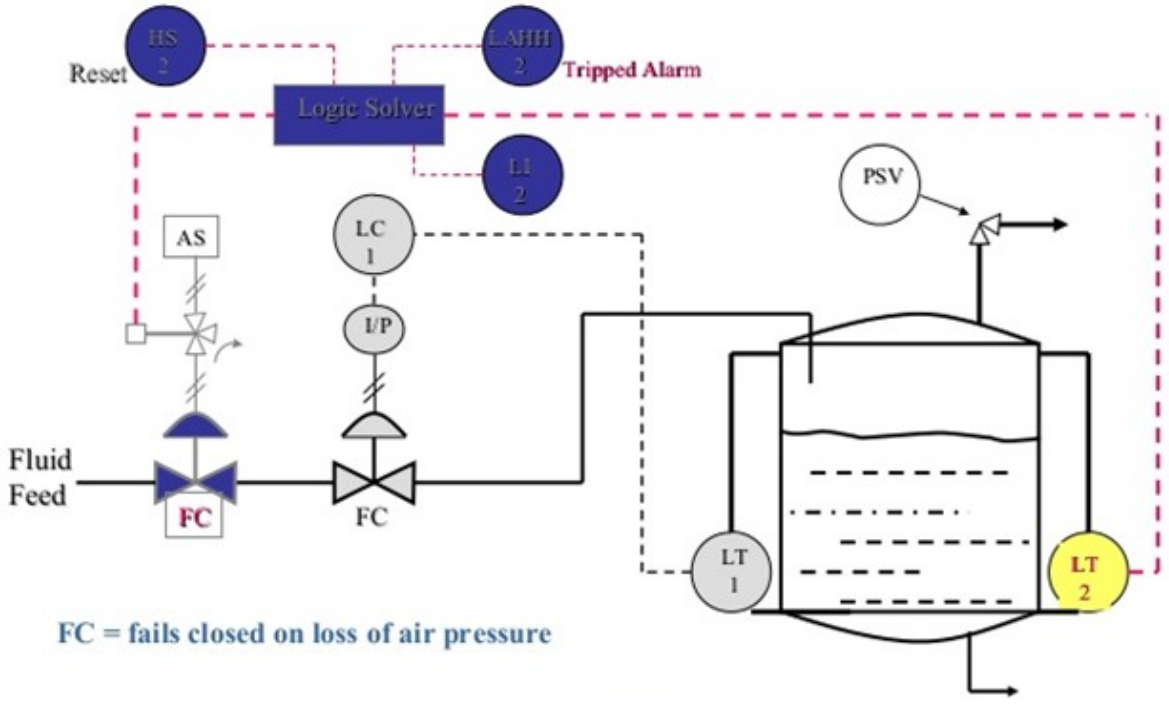
The governing standards for Safety Instrumented Systems SIS state that plant operators must determine and document that equipment is designed, maintained, inspected, tested and operated in a safe manner. Thus, it is imperative that these components of Safety Instrumented Systems be tested frequently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

Example: Typical features of safety instrumented systems

A flammable liquid is pumped into a buffer tank from which it is consumed in a process. A typical level control loop is provided in the process control system to maintain the tank level at 50% full. A hazard will occur if the level control fails for any reason and the tank becomes full. The reasons for level control failure include:

- Jammed open level valve (dirt or seizure)
- Failed level transmitter: false low signal
- Control loop left on manual with valve open
- Leaking control valve

A simple SIS would require the features shown in the Figure bellow: a separate level switch set to detect high level in the tank causes an automatic shut-off valve to close off all liquid feed to the tank. The shut-off valve remains closed until the problem has been rectified.



Questions

1. Explain what safety integrity levels (SIL) are?
   Safety integrity level (SIL) is defined as a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF).
   The requirements for a given SIL are not consistent among all of the functional safety standards. In the European functional safety standards based on the IEC 61508 standard four SILs are defined, with SIL 4 the most dependable and SIL 1 the least. A SIL is determined based on a number of quantitative factors in combination with qualitative factors such as development process and safety life cycle management.

2. Explain why SIS uses different from other process control systems (DCS and PLC) instruments?
   SIS (Safety Instrumented System) is implemented to Safety Critical Function to bring the process to Safe State when Unsafe Condition is detected. Only operation on demand basis. Typically, Safety Instrumented Systems consist of three elements: A Sensor, a Logic Solver and a Final Control Element. A distributed control system (DCS) is a control system for a process or plant, wherein control elements are distributed throughout the system. DCS is implemented for process control with process critical interlock, sequencing, day to day operation and in continuously on demand. A DCS typically uses custom designed processors as controllers and uses both proprietary interconnections and standard communications protocol for communication. Input and output modules form component parts of the DCS. The processor receives information from input modules and sends information to output modules. The input modules receive information from input instruments in the process (or field) and the output modules transmit instructions to the output instruments in the field. The inputs and outputs can be either analog signal which are continuously changing or discrete signals which are 2 state either on or off. Computer buses or electrical buses connect the processor and modules through multiplexer or de-multiplexers. Buses also connect the distributed controllers with the central controller and finally to the Human–machine interface (HMI) or control consoles. The elements of a DCS may connect directly to physical equipment such as switches, pumps and valves and to Human Machine Interface (HMI) via SCADA. The differences between a DCS and SCADA is often subtle, especially with advances in technology allowing the functionality of each to overlap.

3. If reliability of a valve (probability of non-failure within a specified period of time) is 0.9, what is reliability of (a) parallel connection of 2 identical valves; (b) series connection of 2 valves; (c) parallel/series connection of 4 valves?