Process Plant Safety:- Instrumented Protective (Safety) Systems for Process Plants

Introduction:-

Instrumentation in an industrial process plant can be classified into three main categories depending on their functional scope: regulatory control systems, monitoring systems and protective systems. Regulatory control systems or basic process control systems or a DCS continuously monitor the parameters to control the process by maintaining critical parameters within their operating region. Monitoring system provides alarms and alerts to the operator, whenever a process variable deviates beyond its desired operating level. Operator action in response to alarms returns the process parameters back in their operating ranges. While control and monitoring functions try to maintain the availability and productivity of a plant, the task of safety instrumented system is to prevent an undesirable hazardous situation in the plant, by initiating a safe shutdown of the facility or machinery.

Hence Safety Instrumented Systems play an active role in protecting a process plant or machinery from consequences that may lead to personnel injury or loss of life, environmental or financial losses. Unavailability of Safety Instrumented Systems may directly lead to loss of life, injuries, release of hazardous materials to the environment or damage to a piece of equipment. This makes the design, manufacture, installation and maintenance of safety systems critical.

The safety instrumented systems have undergone evolutionary changes through the past 40 to 50 years of their existence in the industry. Development in the process/ equipment safety concepts is major contributor to this, in addition to the technology development which has affected the overall automation scenario of this period. This paper presents a brief introduction to the safety instrumented systems in a process plant, concepts used in designing these systems and the evolution of the safety instrumented systems (SIS).

The role of Safety Systems

Safety systems are installed to prevent unsafe conditions existing in any operating scenario.

How do we define ‘Safety’?

Safety is a “state of being free from risk or danger’. A more accurate and comprehensive definition of Safety is “freedom from unacceptable risk”. The latter definition is important because it highlights the fact that all living processes involve risk, it only differs whether the risk is tolerable or not.

How safe is a chemical process plant? A nuclear power plant? How safe are you when you are travelling in a train or an airplane?

In reality there is no activity which is completely safe. Each action involves a certain measure of risk or ‘un-safety’ and depending on the scenario, necessity and benefits of the activity we accept the level of the risk and move forward in our actions. Some actions are relatively more safe than others hence we undertake them without much thinking; some actions require precautions, protections and planning to address the risks involved. Thus we consciously calculate the risks all the time and evaluate them against acceptance to continue the process of living, and this is the same with any larger industrial process or machinery operation.

Hence, absolute safety, where risk is completely eliminated, can never be achieved; risk can only be reduced to an acceptable level. Mathematically, Risk = Probability (likelihood) of the even * magnitude of the consequence. Risk can be reduced by either reducing its likelihood (frequency) or by reducing the magnitude of its impact.

Instrumented Protective (Safety) Systems for Process Plants

Risks prevail in process or manufacturing industry mainly as it involves storage, processing or handling of hazardous or toxic materials. Initial risk is minimized by using various layers of protection, which include mechanical and process design, basic process control systems, and safety shutdown systems.

Safety Instrumented Systems (SIS) are the most important means of achieving safety in a process plant. These are automatic, instrumented safeguards which take the process or machinery to safe shutdown when one or more critical parameters exceed their predetermined safe limits. An SIS reduces the risk by either reducing the likelihood or probability of risk or by reducing the magnitude of the event. Alternative names for an SIS are trip and alarm system, emergency shutdown system, safety shutdown system, safety interlock system or safety-related control system.

Few examples of Safety Instrumented systems:

- Emergency shutdown (ESD) systems in a hazardous chemical process plant
- Automatic train stop (ATS) system in railways
- Interlocking and emergency stopping systems for machinery
- Dynamic positioning systems for ships and semisubmersible platform
- Fly-by-wire operations of aircraft flight control surfaces
- Anti-lock brakes on automobiles
- Air-bag systems in automobiles

In the following sections, two terms are used to imply safety systems interchangeably for simplicity, as these are intended to mean the same functional system which achieves safety, however they differ in their actual meaning, as used in the industrial perspective.

SIS: Safety Instrumented System is the complete functional system in the process plant/ equipment designed to achieve safety

SIF: Safety Instrumented Function is a single functional system, which protects the plant/equipment against a specific hazard.

A SIS is usually a collection of SIFs.

SIS Design: Evolution

Safety or protection systems have been in use since earlier times of the industrial revolution. Around and beginning with the year 1960, process and nuclear industries started building safety instrumented systems with hardwired electromechanical relay based systems.

Later through the 1970's solid state electronic systems were developed and used along with hardwired relay based systems for SIS. Solid state systems became cheaper and slowly started replacing relay based systems.

Development of microprocessors in the late 1970's and early 1980s made electronic systems cost effective and lead to the emergence of modern programmable logic controllers. PLC based safety systems were used for safety shutdown and these systems have been ever evolving since then.

Until into the early 1980s shutdown functions were designed and developed based on perceived need recognized for such functions in a process or equipment operation, based on operating experience of similar plants. This had serious drawbacks, as the designers and operators in a plant considered all trip functions with equal importance, this many times would lead to under design which compromised plant safety or lead to over design with avoidable financial impact. A machinery safety protection function based on high vibration is required to be more dependable than a level overflow protection system for a cooling water tank. Also in spite of the technological advancement, the configurability, flexibility and diagnostic abilities of the PLC's, the designs did not contribute to reliable safety systems in this initial phase. Industrial accidents were increasing partly due to the complexity of systems.

Instrumented Protective (Safety) Systems for Process Plants

Engineers started thinking about process hazards and how hazardous events could be controlled by using reliable safety systems. Safety PLCs were developed in the 1990's. The SIS reliability was assessed during the design and component failure rates and consequences were evaluated. Probabilistic methods were utilised for quantitative and structured failure analysis for components. Hardware and software design was subject to failure analysis and design. Standards for SIS reliability were established and followed for reliable system designs.

Further in this period, process safety management concepts and consequently SIS design have undergone radical changes since mid-1980's, as a result of increased safety awareness of the industrial community, in the wake of grave industrial disasters in the chemical and nuclear industry during the late 1970's and 1980's. The increased global concern on industrial safety beginning with the near melt down of Three Mile Island nuclear power station in 1979, Bhopal gas tragedy in the year 1984, Chernobyl power plant disaster in 1986, Piper Alpha offshore oil platform accident in 1988 to name the major ones, resulted in collective rethinking on and restructuring of the existing safety management methods and safety standards. New International standards were devised by appointed committees which specified a comprehensive functional safety system, and a new risk based management of the Safety Instrumented Systems. Overview of evolution of safety systems and standards are presented in the figure below.

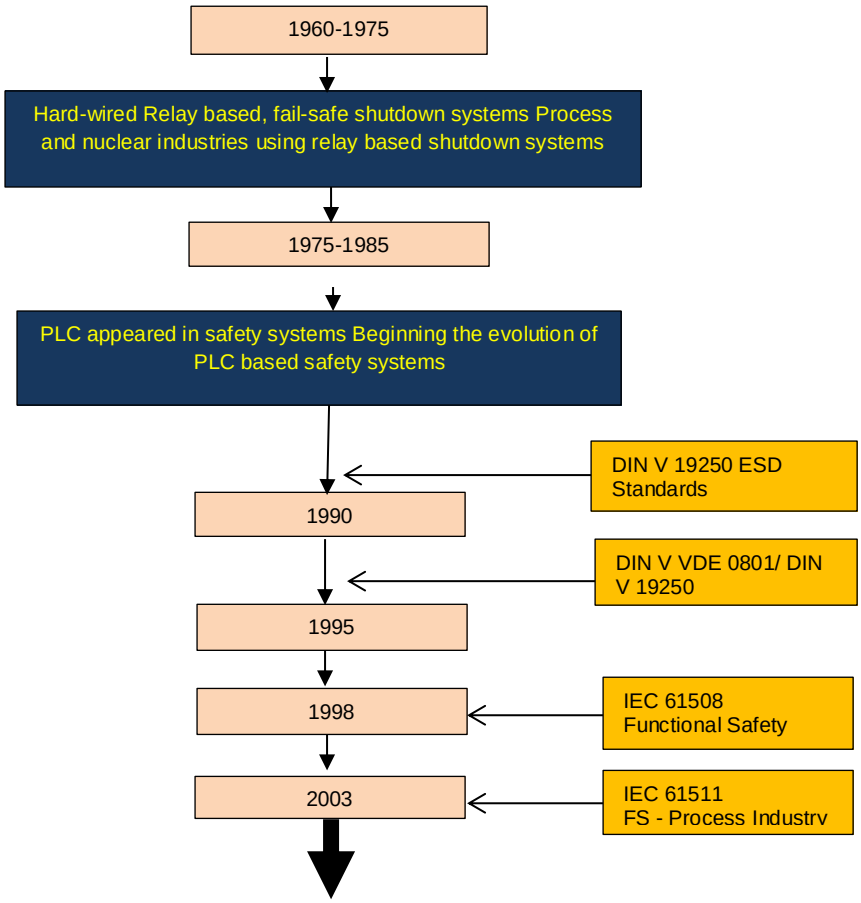

Figure 1: Safety Systems: Evolution

The new standard developed by International Electro-technical commission (IEC- 61508) in 2000 has been accepted as the de facto standard for the design and maintenance of safety instrumented systems, globally.

Safety Instrumented Function – Features

Safety Instrumented Systems are control systems that take the process to a safe state on detection of conditions that may be hazardous or could eventually give rise to a hazard, if no actions were taken. A Safety Instrumented Function (SIF) protects the system by sensing a deviation in process parameter, execute a logic action and actuate a final control element for ensuring a safe sate. SIF consists of three functional elements:

A sensing unit: Sensing device which detects a deviation in the process parameter (ex: high pressure in a vessel) and transmits the signal to a control or logic unit.

Logic Solver: Control Unit which takes an action when the sensing parameter deviates below or above a set limit to initiate a process deviation via a final control element in process.

Final Control Element: Final control actuating element which actually controls the process based on the command received from the logic solver (ex: Shutdown valve).

Figure shows the functional subsystems / elements of a typical safety instrumented function.

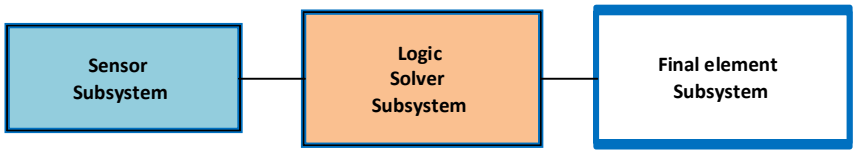

Figure 2: Safety Instrumented Function

Example of a Safety Instrumented Function

Following diagram shows a schematic diagram of pressure and level control system in a vessel, processing hydrocarbon substance. Two instrumented control functions are provided for achieving continuous safe operation of this system. Continuous regulatory control by a DCS loop and a protective safety instrumented function to prevent high pressure inside the vessel. Let us see how this safety function is defined in relation to a process.

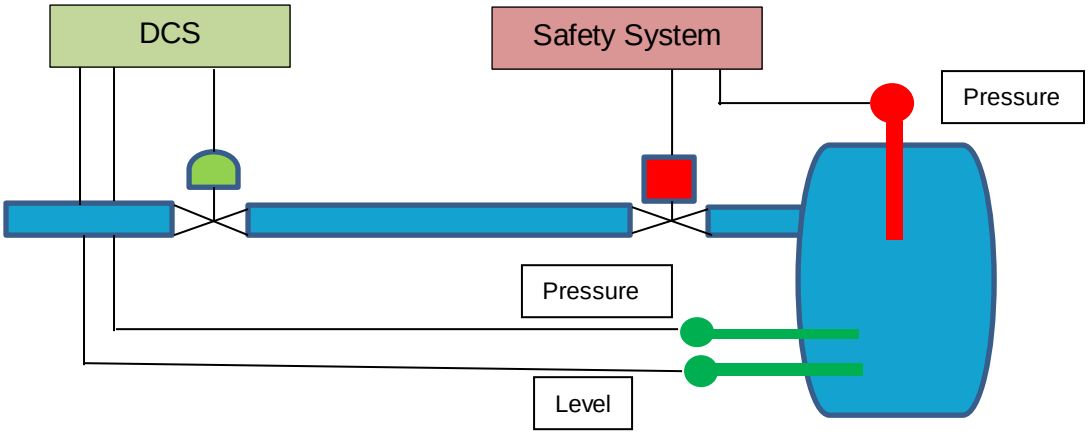

Figure 3: Example Safety Instrumented Function

Pressure inside the vessel is controlled by the DCS control loop using level and pressure measurements within the vessel by controlling the inlet control valve. Any failure in DCS can lead to higher pressure inside the vessel. Assume that the vessel design pressure is 12 barg. The DCS control operates to maintain the pressure within a desirable operating limit, required for the process,

say 6 barg. At higher pressure than 12 barg, the vessel is likely to get ruptured and due to the hydrocarbon inside, there will be a fire or explosion related scenario with major consequence. To prevent this scenario, any higher pressure sensed by the safety instrumented function, set typically below 12 barg, will put a demand on the safety system to initiate a safe shutdown by closing the ESD valve at the inlet piping. Safety Instrumented Function here is designed for protection of the vessel from overpressure and subsequent damage or rupture and related consequences. The SIF includes the entire functional system, the pressure sensor at the vessel, Safety system (SIS) and the shutdown valve at the vessel inlet.

Risk Based Design of Safety Instrumented Systems

The automated SIS being one of the most important functional safety devices in a plant the reliability of the SIS has been given serious attention in the recent past. The new standards focussed on developing a risk based approach to process safety management and recommended that a series of process risk assessments be carried out in the initial design stage to assess the level of risk to be mitigated by the safety functions. This means in case of a failure of the safety function, certain risk is almost imminent and the safety function shall be implemented as reliable as the risk level demands. This means higher the risk level to be mitigated, the related safety function design has to be more robust. SIS implementation based on this risk centred approach includes below activities:-

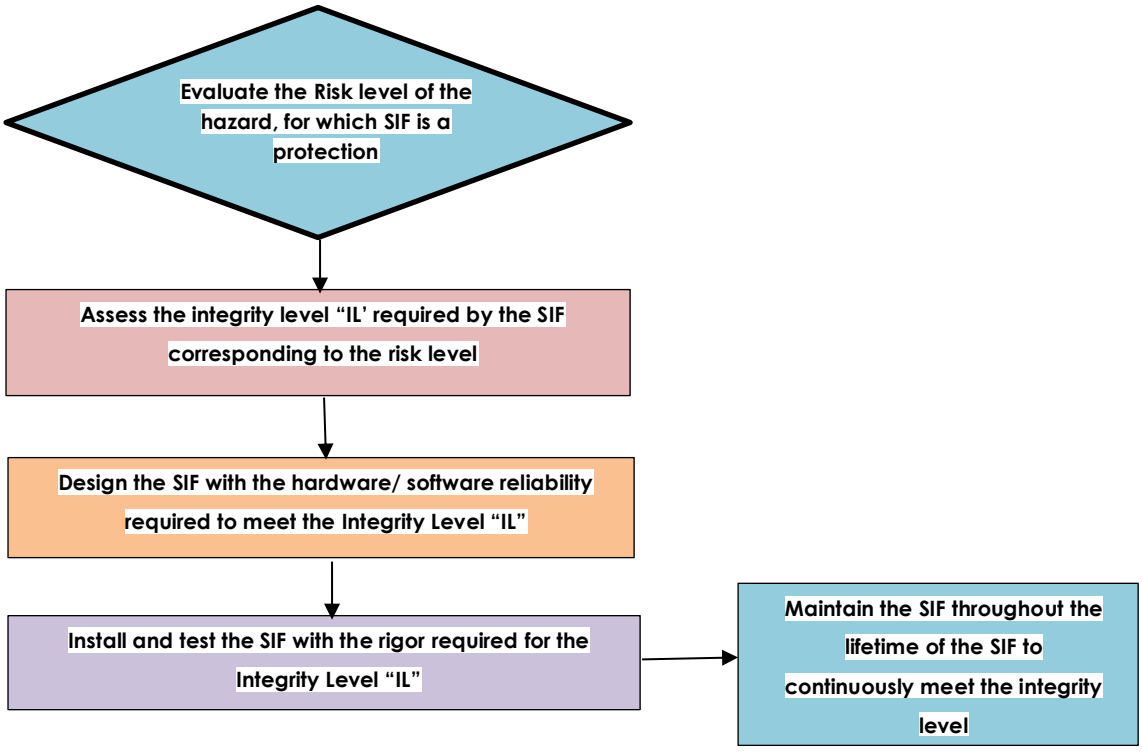

Figure 4: Risk based Design and Management of safety system

Integrity Level or "Safety Integrity Level" (SIL) as it is often referred is the reliability measure of a Safety Instrumented Function, which corresponds to the risk reduction capability or risk reduction factor of a safety function. Hence required integrity level of a SIF is decided based on risk reduction required by this SIF.

IEC Standard assigned 4 different integrity levels for safety instrumented systems:

- SIL-1, minimum integrity associated with a risk reduction factor of 10 to 100
- SIL-2, higher integrity associated with a risk reduction factor of 100 to 1000
- SIL-3, critical integrity level associated with a risk reduction factor of 1000 to 10000
- SIL-4, highest integrity requirement associated with a risk reduction factor of >10000

Safety Integrity Level is a key factor in the design of a safety function and each SIF is required to have a risk assessment.

How the hardware / software design of a SIF is related to its SIL?

SIL level is assigned as a measure of reliability for the entire safety function, higher SIL means a higher risk reduction requirement. Higher SIL level is also a measure of lower failure probability, i.e a reliable device with very low failure rates (number of failures / year etc.) can meet a higher SIL.

A SIL-1 system is not very stringent in terms of its robustness; this can be achieved with good instruments which are proven in specific application for few years. Hence a SIL-1 system is easy to implement and typically has simplex components/elements. For a SIL-2 system, the hardware and software implementing the SIF shall have much lower failures. This means the components used in hardware and software methods shall have more reliability with lesser failures than a SIL-1 system. As an example SIL-2 systems may require redundant components to minimise the system failure probability. SIL-3 systems shall be more reliable with very low failure probability and rigorous software and programming/testing routines. SIL-3 systems will require redundant components and sometimes may require triple redundancy levels.

Conclusion

The process industries often deal with flammable, explosive and hazardous chemicals and complex machinery, and they have a long history of hazardous incidents resulting in loss of lives, lasting injuries and damage to the environment as well as property. Automatic/ instrumented safety systems are used to protect the process against these undesired hazardous events. Operational experiences gained from the process and equipment safety have resulted in continuous improvements in the safety instrumented systems, as the requirement of reliable systems for executing safety functions was more and more recognized.

Evolution of Safety Instrumented Systems in the past decades have been marked mainly in two ways, technological changes based on the developments in the electronic hardware/software platforms in these decades and the changes in the design basis itself for the safety instrumented systems in accordance with the developments in the process safety concepts.

Technologically the hardware used in SIS systems have been developed from the standalone relay based systems through independent PLCs and later into the safety PLCs with fault tolerant architectures and advanced diagnostics.

Design of Safety systems were traditionally based on engineering intuition and thump rules which was later subject to gradual changes to the present day industry practice of risk based safety instrumented systems, where a performance and risk analysis is the basis of SIS selection, design, implementation and maintenance. Process risk analysis plays a pivotal role in the current SIS design, and a reliability matric called ‘SIL’ corresponding to the risk level provides guidance for the design, engineering, procurement, installation, testing and maintenance of the SIS. Hence Safety instrumentation is not exclusively an instrument and control engineering subject. Successful implementation of an SIS depends on knowledge of other disciplines, as well as a well-defined safety management system within a process industry.