International Association Of Certified Practicing Engineers	IACPE INTERNATIONAL ASSOCIATION OF CERTIFIED PRACTICING ENGINEERS www.iacpe.com Knowledge, Certification, Networking	Rev: 01 Rev 01 – Sept 2016
IACPE No 19, Jalan Bilal Mahmood 80100 Johor Bahru Malaysia	**LAYERS OF PROTECTION ANALYSIS** **CERTIFIED PRACTICING SAFETY PROFESSIONAL TRAINING MODULE**	

The International Association of Certified Practicing Engineers is providing the introduction to the Training Module for your review.

We believe you should consider joining our Association and becoming a Certified Practicing Engineer. This would be a great option for engineering improvement, certification and networking.

This would help your career by

1. **Providing a standard of professional competence in the practicing engineering and management field**
2. **Identify and recognize those individuals who, by studying and passing an examination, meets the standards of the organization**
3. **Encourage practicing engineers and management professionals to participate in a continuing program of personal and professional development**

www.IACPE.com

TABLE OF CONTENT

LIST OF PICTURS

LIST OF TABLES

INTRODUCTION

Scope

Safety is improved through inherently safer design and various safeguards, such as instrumented systems, procedures, and training. Oil and Gas accidents may result in causalities and economic losses. Determining specific safety requirements of safety systems is an important part in ensuring that accidents are prevented. In chemical processes, several protection layers are used,

Safety instrumented systems like HIPPS (High Integrity Pressure Protection Systems) are increasingly becoming a preferred risk mitigation solution based on their cost effectiveness and ease of implementation. On processing plants, HIPPS can eliminate the need to upsize the flare system and potentially replace it. At the wellhead or pressure source, a HIPPS system allows the downstream piping to be lower pressure rated. Further safeguarding analysis using the LOPA (Layer of Protection Analysis) method identified a HIPPS system as a technically viable risk reduction solution to protect against overpressure.

Process designers use a variety of protection layers, or safeguards, to provide a defense in depth against catastrophic accidents. They are devices, systems or actions that can prevent a scenario from proceeding to an undesired consequence. Ideally such protection layers should be independent from one another so that any one will perform its function regardless of the action or failure of any other protection layer or the initiating event. When they meet this criterion, they are called Independent Protection Layers (IPL). Not all safeguards meet the independence requirements to be classified as an IPL. LOPA addresses safeguards that are IPLs.

General Design Consideration

The process industry is obligated to provide and maintain a safe, working environment for their employees. Safety is provided through inherently safe design and various safeguards, such as instrumented systems, procedures, and training. Oil and Gas accidents may result in causalities and economic loss. Determining specific safety requirements of safety systems is an important part in ensuring that accidents are prevented. In chemical processes, several protection layers are used.

A. Safety Instrumented System (SIS)

A safety instrumented system (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 such as set points for pressure, temperature, level, etc. in other words, they trip the process when they are in an out of limit condition. SIS are also called emergency shutdown (ESD) systems, safety shutdown (SSD) systems, and safety interlock systems. Safety Instrumented System (SIS) is an alternative for conventional relief device to eliminate the source of overpressure, thereby making relief capacity unnecessary. They are typically used where the provision of relief capacity is inappropriate. This is typically (but not always) due to one of the following factors:

- the fluid which would be discharged via a relieving device is toxic or extremely hazardous.
- realistic evaluation of the overpressure scenario and quantification of the relief load is difficult or impossible (e.g. explosive reaction).
- the cost of providing the necessary capacity in the disposal system or the relief valves is prohibitive.

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. SIS provides a layer of protection to help protect the process against accidents.

The basic SIS layout comprises:

1. Sensor(s) for signal input and power

2. Input signal interfacing and processing
3. Logic solver with associated communications and power. The safety firmware constitutes the basic logic solver equipment from which the safety applications are built:
    a. Framework, racks, cabinets;
    b. Processor/memory boards;
    c. Communication boards;
    d. I/O boards;
    e. Termination units;
    f. Power supplies;
    g. System software;
    h. Application software libraries;
    i. Application programming tools;
    j. Communication protocols;
    k. Human/system interfaces.

    When designing the logic solver hardware, the following should be considered:

    a. A safety user design manual should exist which describes how non-certified equipment shall be used in safety critical applications. For certified equipment, this is normally available as part of the certification;
    b. Appropriate designated architecture must be selected for the central processing unit. As a minimum, the selected architecture shall meet the highest SIL level of the relevant safety functions;
    c. If possible, the architecture of the I/O and interface modules should be selected individually for each safety function;
    d. When working with certified equipment, the difference between certified components and components certified for non-interference should be noted:
    e. Certified components: for use in safety critical functions;
    f. Components certified for non-interference: may be used but not in safety critical functions.

g. For non-certified equipment PFD calculations shall be performed to show that the contribution from the logic solver is within acceptable limits;

h. For certified equipment, the maximum contribution to the PFD figure is normally part of the certification report and is therefore available as pre-calculated and verified parameters;

i. For non-certified equipment, the maximum time in degraded mode should be calculated;

j. For certified equipment, the maximum time in degraded mode is normally part of the certification report and is therefore available as pre-calculated and verified parameters.

4. Output signal processing, interfacing and power
5. Actuators and valve(s) or switching devices to provide the final control element function.

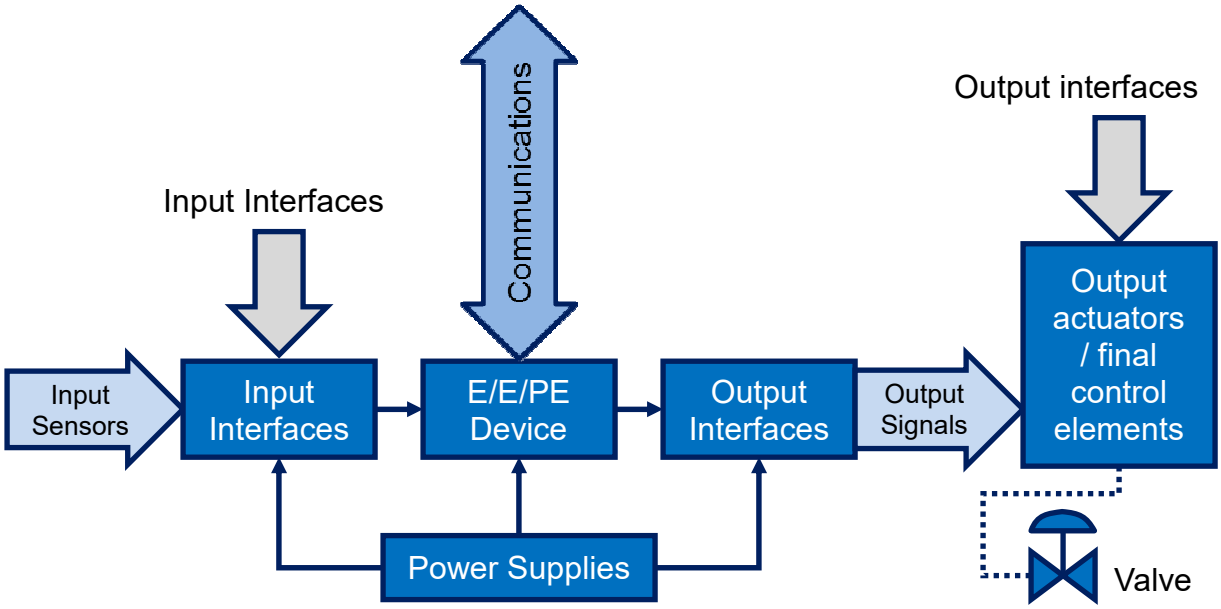

Figure 1: Basic SIS layout

Safety Instrumented System (SIS) is an alternative for conventional relief device to eliminate the source of overpressure, thereby making relief capacity unnecessary. They

are typically used where the provision of relief capacity is inappropriate. This is typically (but not always) due to one of the following factors:

1. The fluid which would be discharged via a relieving device is toxic or extremely hazardous
2. Realistic evaluation of the overpressure scenario and quantification of the relief load is difficult or impossible (e.g. explosive reaction)
3. The cost of providing the necessary capacity in the disposal system or the relief valves is prohibitive.
4. The vessel is not exclusively in air, water, or steam service.
5. The user must ensure the MAWP of the vessel is higher than the highest pressure that can reasonably be achieved by the system.
6. A quantitative or qualitative risk analysis of the proposed system must be made addressing: credible overpressure scenarios, demonstrating the proposed system is independent of the potential causes for overpressure; is as reliable as the pressure relief device it replaces; and is capable of completely mitigating the overpressure event.

Lifecycle of SIS is based on industry standards and these standards cover a wide range of chemical process operations. Due to its broad scope, the standard has many general requirements addressing the complete lifecycle of the SIS, starting with the identification of SIS requirements in the risk assessment and ending when the SIS is decommissioned. While there are many ways of representing the lifecycle, a simple four step approach can be followed:

1. Define a risk-management strategy - establish a facility management system for how SISs are identified, designed, inspected, maintained, tested, and operated to achieve safe operation and perform a hazard and risk analysis to identify where SISs are needed and their target SIL
2. Implement the strategy - develop a design basis to achieve the target SIL and execute the detailed design to meet the requirements. The SIS design basis should address the following:

    a. Detection of and response to potential hazardous events
    b. Selection of equipment based on prior history
    c. Fault detection, such as diagnostics and proof testing

d. Fault tolerance against dangerous failures
e. Procedures for maintenance and test, including the use of bypasses
f. Operation and maintenance procedures required when SIS equipment is out of service
g. Emergency shutdown capability if the SIS fails to take action as expected
h. Start-up and shutdown of the process equipment

3. Validate, start-up, operate and maintain the strategy - implement the SIS following the design basis and detailed design documentation and define what is required of operation and maintenance personnel to sustain the SIL
4. Manage changes to the strategy - ensure the SIS meets the target SIL by monitoring operation, inspection, test, and maintenance records and making changes as necessary to improve its performance

Validation planning of the SIS should define all activities required for validation. The following items shall be included:

1. The validation activities, including validation of the SIS with respect to the safety requirements specification and implementation and resolution of resulting recommendations;
2. Validation of all relevant modes of operation of the process and its associated equipment including:
    a. Preparation for use including setting and adjustment;
    b. Start-up, teach, automatic, manual, semi-automatic and steady state of operation;
    c. Re-setting, shut down and maintenance;
    d. Reasonably foreseeable abnormal conditions.
3. The procedures, measures and techniques to be used for validation;
4. Reference to information against which the validation shall be carried out (e.g., cause and effect chart, system control diagrams).
5. When the activities shall take place;
6. The persons, departments and organizations responsible for the activities and levels of independence for validation activities;

SIS safety validation shall mean all necessary activities to validate that the installed and mechanical completed SIS and its associated instrumented functions, meets the requirements as stated in the Safety Requirement Specification (SRS). The validation of the safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning. Validation activities shall as a minimum confirm that:

1. The safety instrumented system performs under normal and abnormal operating modes (e.g., start-up, shutdown, etc.) as identified in the Safety Requirement Specification;
2. Adverse interaction of the basic process control system and other connected systems do not affect the proper operation of the safety instrumented system;
3. The safety instrumented system properly communicates (where required) with the basic process control system or any other system or network;
4. Sensors, logic solver, and final elements perform in accordance with the safety requirement specification, including all redundant channels;
5. Safety instrumented system documentation reflects the installed system;
6. The safety instrumented function performs as specified on bad (e.g., out of range) process variables;
7. The proper shutdown sequence is activated;
8. The safety instrumented system provides the proper annunciation and proper operation display;
9. Computations that are included in the safety instrumented system are correct;
10. The safety instrumented system reset functions perform as defined in the safety requirement specification;
11. Bypass functions operate correctly;
12. Manual shutdown systems operate correctly;
13. The proof test intervals are documented in the maintenance procedures;
14. Diagnostic alarm functions perform as required;
15. The safety instrumented system performs as required on loss of power or a failure of a power supply and confirm that when power is restored, the safety instrumented system returns to the desired state.

The safety lifecycle is a management system that strives to ensure a functionally safe system if all steps are implemented properly. Figure 2 illustrates the safety lifecycle. The SIS lifecycle approach is an engineering process to optimize SIS design and preserve its risk reduction properties. It means that engineers should stay involved the whole life of the safety system so that all activities affecting the SIS function is carried out in the right time and in a correct way. The SIS lifecycle includes seven phases, specification, design, integration, operation, maintenance, modification and decommissioning, as described in figure and listed below.

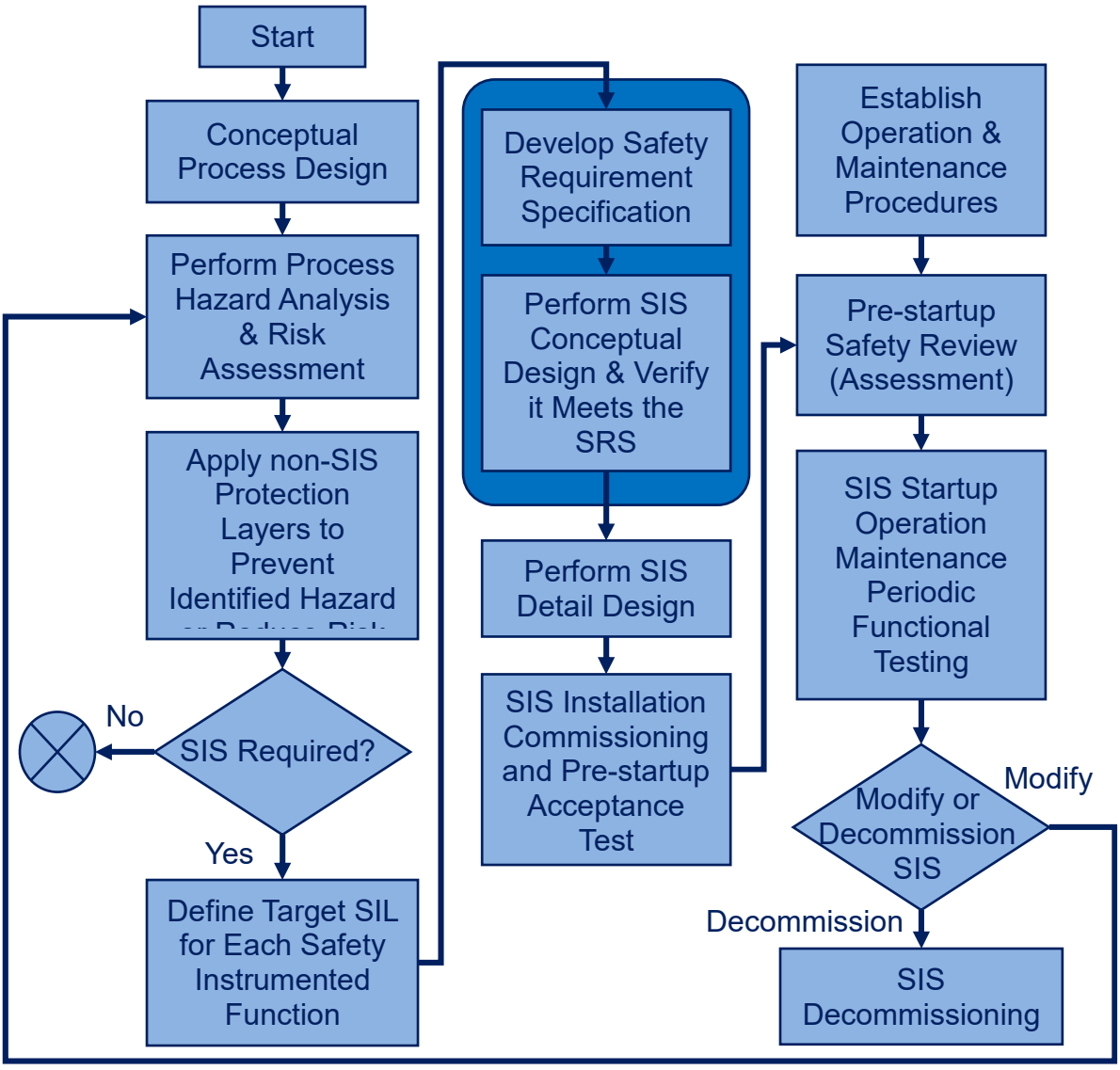

Figure 2: SIS safety life-cycle phases

1. When using a SIS lifecycle approach a hazard and risk assessment has to be made. All events and sequences leading to a hazardous consequence shall be identified. This step also includes risk reduction requirements and which SIF that are needed.
2. The next step includes further description of each SIF and the associated safety integrity level. For determination of SIL the LOPA method can advantageously be used.
3. Step three provides a Safety Requirement Specification (SRS), which specify the requirement of each SIS, i.e. the software safety requirements and the reliability data for each part of the loop. The SRS report shall provide a basis for the safety loop design.
4. The fourth step handles design of a specific SIS, which includes taking safety requirements and software requirements into account. It also includes planning for the SIS integration tests which shall be performed in the following step of the lifecycle process.
5. The fifth step includes installation, commissioning and validation of the SIS. It is made in order to validate that the SIS meets all requirements, with respect to the required SIL. The step results in a fully functioning SIS in conformance with specified SIS design results.
6. SIS operation and maintenance is performed in order to ensure that the SIS safety requirements are provided over time. The reliability and effectiveness of all layers of protection needs to be monitored so that the SIL rating from the original assessment can be adjusted to the reality.
7. Any change to any of the layers of protection affect the reliability demands that rests upon the SIL rated functions. Therefore, the safety instrumented systems needs to be reassessed so that the total risk reduction requirement is met over time.
8. Finally, when it is time decommissioning, it is important to ensure that proper review, sector organization and the total system risk remains at an appropriate level.

There are a number of ways of configuring and testing a Safety Instrumented System (SIS) to achieve specified Safety Integrity Level. In order to define the method for arriving at a configuration for the safety instrumented system, typical example of High Integrity Pressure Protection Systems (HIPPS) implemented on pipelines and other process streams is considered.

B. LOPA Overview

Determining specific safety requirements of safety systems is an important part in ensuring that accidents are prevented. In the 1990s the industry standards emerged, and the need for documenting compliance with these in a consistent manner led to the introduction of the layer of protection analysis (LOPA).

Layer of Protection Analysis (LOPA) is an analytical tool to determine if there are sufficient layers of protection against a hazardous scenario. Usually many types of protection layers can be applied, but only one protection layer has to work successfully to prevent the consequence. However, no protection layer can be 100 % reliable and an analysis has to be made to ensure system tolerable risk level. If the risk is not tolerable, additional safety measures have to be added. LOPA only judge whether there are sufficient protection or not and does not suggest which type of protection to be added. LOPA simply help the analyst to decide how much the system risk has to be reduced in order to reach tolerable risk level.

The protection layer (PL) should be:

- effective in preventing the consequence when it functions as designed,
- independent of the initiating event and the components of any other PL already claimed for the same scenario,
- auditable, i.e. its effectiveness in terms of consequence prevention and probability of failure on demand (PFD) has to be capable of validation (by documentation, review, testing, etc.).

In chemical processes, several protection layers are used, and in LOPA the number and the strength of these protection layers are analyzed. LOPA can be considered as a simplified form of a quantitative risk assessment. It can be used after a hazard and operability analysis (HAZOP), and before a quantitative risk analysis (QRA). A difference between LOPA and other tools is that LOPA analyzes the different protection layers individually, and the mitigation they lead to. LOPA is especially used to determine

the safety integrity level (SIL) of safety instrumented functions in conjunction with IEC 61511, but also as a general risk assessment tool to evaluate if the protection layers in a system are satisfactory.

LOPA can be used at any point in the lifecycle of a project or process, but it is most cost effective when implemented during front-end loading when process flow diagrams are complete and the P&IDs are under development. For existing processes, LOPA should be used during or after the HAZOP review or revalidation. LOPA is typically applied after a qualitative hazards analysis has been completed, which provides the LOPA team with a listing of hazard scenarios with associated consequence description and potential safeguards for consideration.

LOPA can be divided into different steps. LOPA performance can be divided into following steps.

1. Step 1. Identify the consequences. The first step is to screen scenarios and to decide which consequences to avoid. Some companies stop at the magnitude of an unwanted release, while others explicitly estimate the risks by addressing the consequences.
2. Step 2. Select an accident scenario. LOPA is applied at one scenario at a time. Scenarios are identified during an identification procedure where all events leading to a specific consequence are determined. The analysis describes the identified events as single cause-consequence happening. The scenarios are usually identified by qualitative risk assessment methods such as HAZOP or HAZID.
3. Step 3. Identify the initiating event of the scenario and determine the event frequency. In this step the frequency of a consequence, given failure of all IPLs/Safeguards, is determined. The frequency has to be based on the background of the scenario, like how often an operation causing an event is actually exercised.
4. Step 4, Identify IPLs and estimate its probability of failure on demand. Depending on the scenario and the system properties there can be different kinds of IPLs. Some accident scenarios need many IPLs while other needs one or none. An IPL can be high rated or low rated depending on its effectiveness to prevent an event to develop into an unwanted consequence or to mitigate the consequence. The effectiveness of the IPL or safeguard is quantified as probability of failure on demand (PFD).

   Protection layers that perform their function with a high degree of reliability may qualify as Independent Protection Layers (IPL). The criteria to qualify a Protection Layer (PL) as an IPL are:

- The protection provided reduces the identified risk by a large amount, that is, a minimum of a 10-fold reduction.
- The protective function is provided with a high degree of availability (90% or greater).
- It has the following important characteristics:
  a) Specificity: An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (e.g., a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event; and, therefore, multiple event scenarios may initiate action of one IPL.
  b) Independence: An IPL is independent of the other protection layers associated with the identified danger.
  c) Dependability: It can be counted on to do what it was designed to do. Both random and systematic failures modes are addressed in the design.
  d) Auditability: It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary.

5. Step 5. Estimate the risk of the scenario. In LOPA, the risk of a scenario is defined as the consequence multiplied by the frequency. All IPL data lowering the risk should be taken into account. In other words, the total risk is a combination of the consequence and the frequency of an event and the IPLs affecting these factors. The risk is not allowed to exceed specific tolerable risk criteria, e.g. TMEL.
6. Step 6. Evaluate the risk to reach a decision concerning the scenario. The final step includes comparison between the acceptable risk criteria and the total risk of the scenario. The results can be used to identify which safety measure to focus on. If the residual risk is low, simple design enhancement may be enough. Otherwise, extra SIL rated safety function can be added.

LOPA can be extended to many situations involving risk-informed decision making including:

- Design
- Capital improvement planning
- Management of change
- Evaluating facility siting risk
- Mechanical integrity programs
- Identifying operator roles
- Incident investigation
- Emergency response planning
- Bypassing a safety system
- Determining the design basis for over-pressure protection
- Determining the need for emergency isolation valves
- Screening tool for QRA

Figure 3 shows typical layers of protection of in a hazardous industrial plant. An interesting methodology for preliminary risk analysis and safety-related decision-making is the layer of protection analysis (LOPA) methodology

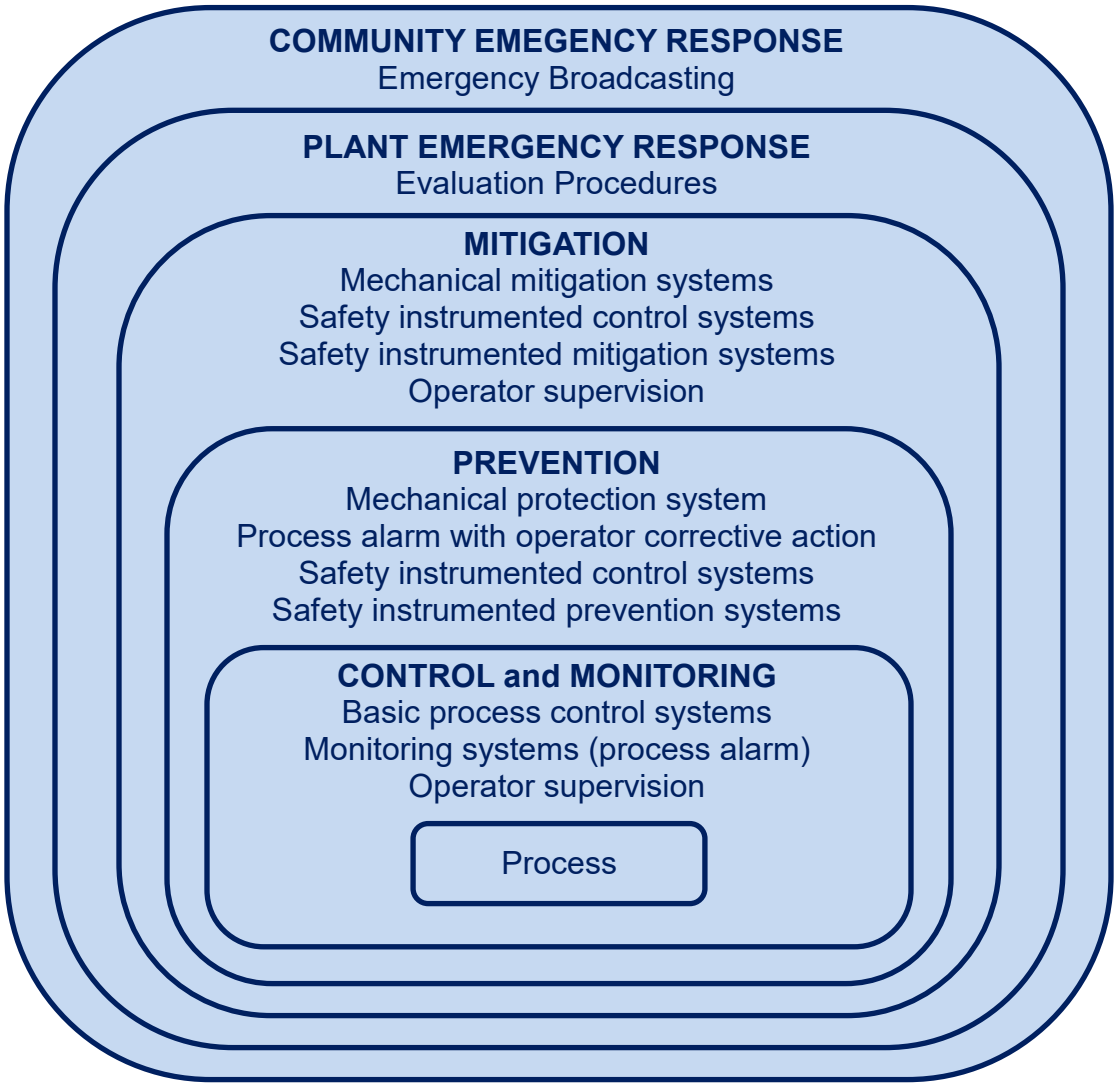

Figure 3: Typical protection layers in hazardous industrial installation

Often, an "onion" as the one in Figure 4 is used as an illustration of the protection layers in LOPA. The system or process design has protection layers including basic process control system (BPCS), critical alarms and human intervention, SIFs, physical protection and emergency response.

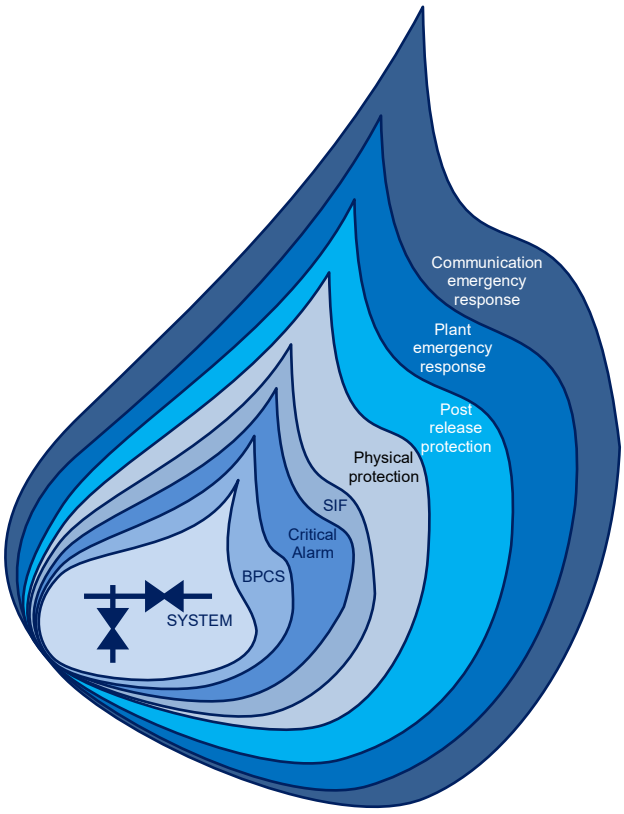

Figure 4: Anion LOPA

- BPCS is the control system used during normal operation and sometimes denoted as the process control system (PCS). Input signals from the process and / or from the operator are generated into output which make the process operate in a desired manner. If the control system discovers that the process is out of control (e.g. high pressure) it may initiate actions to stabilize the temperature (e.g. choking the flow) (CCPS, 2001).
- Alarms monitoring certain parameters (e.g. pressure and temperature) are considered another protection layer. When the alarm is tripped, the operator may intervene to stop the hazardous development. Note that the alarm system has to be wired to another loop than the BPCS in order to be independent (CCPS, 2001).
- A SIS implements the wanted safety function SIF. In LOPA, SIFs are considered as protection layers.
- Physical protection include equipment like pressure relief devices. In a separator this may be a rupture disc which blows-off pressure if the pressure is too high.
- Post release protection is physical protection as dikes, blast walls etc. These have their function after the release or explosion has occurred.
- Plant and community emergency response, and are considered the final protection layer. If an accident occurs, procedures, evacuation plans, equipment and medical treatment help the exposed personnel to escape, or to mitigate damage / injury. Such measures are classified as plant and community emergency response (CCPS, 2001)

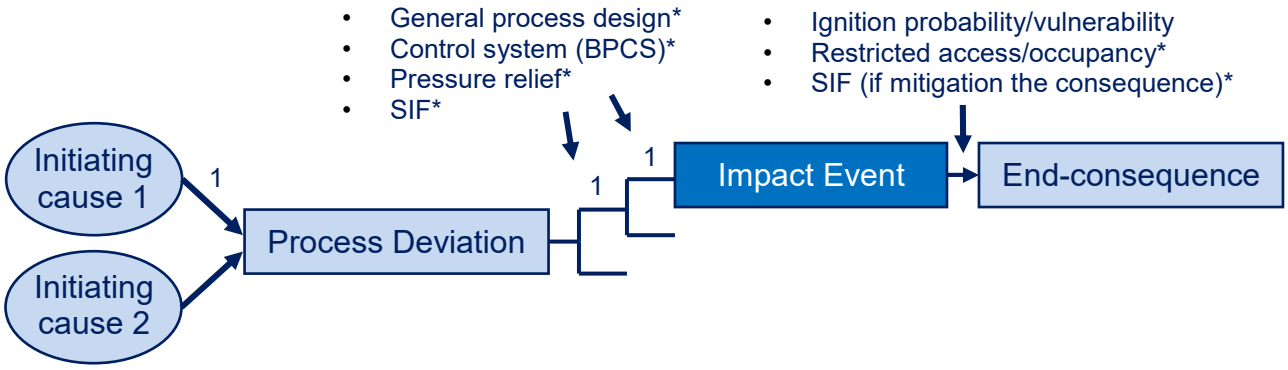

Figure 5: Relation between initiating causes, impact event, process deviation and IPLs

Figure 5 shows the relation between the initiating causes, impact event, process deviation and the PLs. It shows how all the terms fit together and the figure and the definitions given found the basis of the understanding of LOPA. Initiating causes may be the sources of a process deviation which may lead to an impact event. The impact event may result in an end-consequence. In order to prevent the end-consequence PLs are introduced. Most of these have the objective of limiting the frequency of the impact event, but PLs to minimize the extent of damage may also be put in place.

There are four primary benefits to implementing LOPA over other SIL assignment methodologies procedures.

- Due to its scenario-related focus on the process risk, LOPA often reveals process safety issues that were not identified in previous qualitative hazards analysis.
- Process hazards are directly connected to the safety actions that must take place, providing clear identification of the safety instrumented systems and associated SIL.
- It has been proven effective in resolving disagreements related to qualitative hazards analysis findings.
- LOPA often identifies acceptable alternatives to the SIS, such as adding other layers of protection, modifying the process, or changing procedures. This provides options for the project team to evaluate using cost/benefit analysis, allowing the most cost effective means of risk reduction to be selected.

C. Introduction to HIPPS

Overpressure protection is required where a process, system or equipment failure can cause the pressure in an item of equipment or pressure system to exceed the maximum pressure allowed by the pressure design code. The following initiating causes for overpressure events:

- loss of utilities, such as electric power, steam, water, etc.,
- runaway reactions,
- fire exposure,
- operating errors,
- maintenance errors,
- block outlet,

- equipment failures, and
- instrumentation malfunctions.

In traditional systems over-pressure is dealt with through relief of venting systems. These systems have obvious disadvantages such as release of (flammable and toxic) process fluids in the environment and often a large footprint of the installation. With the increasing environmental awareness relief systems are no longer an acceptable solution.

Recently, ASME has accepted the use of alternative methods of protection and in particular the use of instrumented protective systems (ASME Code Case 2211). Such systems often provide a more feasible and cost-effective approach in situations where discharge of the process fluid may be undesirable or where the design of pressure relieving facilities would be impractical or very expensive. In some applications, the use of pressure relief devices is impractical. Typical cases include (SIS-Tech, 2000):

- Chemical reactions so fast the pressure propagation rate could result in loss of containment prior to the relief device opening. Examples are “hot spots,” decompositions, and internal detonation/fires;
- Chemical reactions so fast the lowest possible relieving rate yields impractically large vent areas;
- Exothermic reactions occurring at uncontrollable rates, resulting in a very high propagation rate for the process pressure. (The pressure propagation rate for these reactions is often poorly understood.);
- Plugging, polymerization, or deposition formed during normal operation, which have historically partially or completely blocked pressure relief devices;
- Reactive process chemicals relieved into lateral headers with polymerization and thus plugging, rendering the relief device useless;
- Multi-phase venting, where actual vent rate is difficult to predict; and
- Pressure relief device installation creates additional hazards, due to its vent location.

The industry has established standards that govern the design of pressure relieving systems to protect vessels from hazardous overpressure. The applicability of these standards is illustrated in Figure 6. Starting in 1996, these codes were amended to

allow for examining the reduction in relief system load due to well-designed Safety Instrumented Systems (SIS). When the primary purpose of a SIS is to safeguard against equipment overpressure in lieu of conventional relief design, then such a system is referred to as a “High Integrity Pressure Protection System”, or HIPPS.

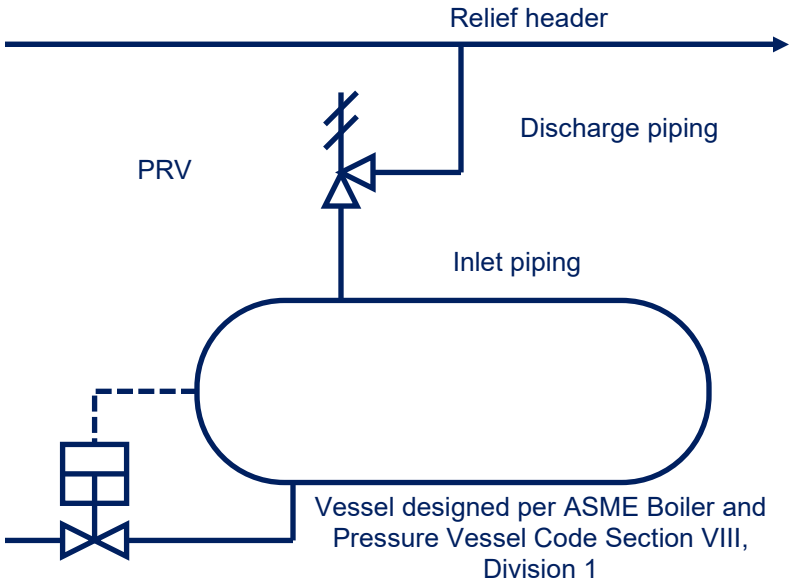

Figure 6: Applicability of codes and standards for pressure protection

There is the potential for upset conditions at chemical plants and refineries that may require equipment to relieve excess pressure at a rate that exceeds the design of flare systems, vent systems, or other disposal systems. Due to this concern, many chemical plants and refineries are now proposing a HIPPS be used to mitigate that potentially hazardous situation.

HIPPS systems are a series of components, specifically engineered to isolate the source of dangerous high pressure instead of relieving the excess flow, in the case of

an overpressure event. HIPPS, an abbreviation for high integrity pressure protection system, is a specific application of a SIS designed in accordance with industry standards. With HIPPS, the protection against overpressure is achieved by quickly isolating the source causing the overpressure, as compared to conventional relief systems where the overpressure is relieved to atmosphere. The purpose of the HIPPS is to safeguard against over-pressuring equipment and, often, consequently overloading the flare or disposal system.

In general terms, the following overriding considerations apply to analysis and design of a HIPPS system. The overpressure protection system:

- Must ensure safe equipment operation from overpressure
- Must comply with applicable laws and ASME Codes
- Should be consistent with applicable industry recommended practices

HIPPS provides a solution to protect equipment in cases where:

- high-pressures and / or flow rates are processed
- the environment is to be protected
- the economic viability of a development needs improvement
- the risk profile of the plant must be reduced

A typical HIPPS system includes

- a SIL rated logic solver (PES - programmable electronic system), which processes the input from the sensors to an output to the final element
- input sensors (typically three pressure sensors (PIT) on the same process variable), that detect the high pressure
- final elements (typically at least two actuators/safety shut-off valves). that actually perform the corrective action in the field by bringing the process to a safe state. In case of a HIPPS this means shutting off the source of overpressure. The final element consists of a valve, actuator and solenoids.

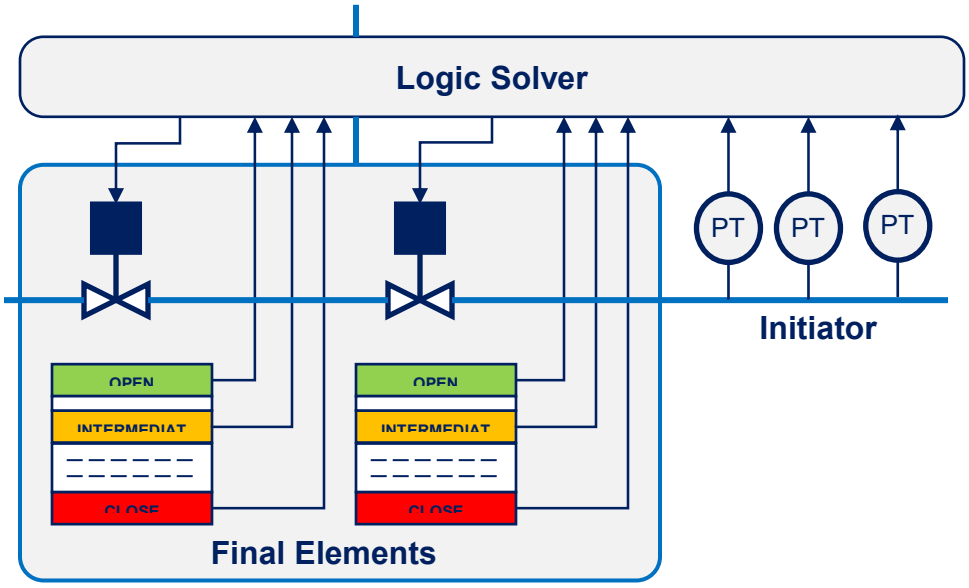

Figure 7: A typical HIPPS system

Advantages

- They are becoming the option of choice to help alleviate the need to replace major portions of the flare system in existing facilities when adding new equipment or units.
- If the header and flare system must be enlarged, significant downtime is incurred for all of the units that discharge to that header.
- The capital and installation cost associated with HIPPS is attractive when compared to the downtime or equipment cost of flare modification.
- The process unit will not flare as much as a process unit designed for full flare loading. In some areas of the world, this is becoming important as regulatory agencies place greater restrictions on flaring of process gases.

Disadvantages

- The ability of the HIPPS to adequately address overpressure is limited by the knowledge and skill applied in the identification and definition of overpressure scenarios.
- HIPPS systems are more complex, requiring the successful functioning of multiple devices to achieve the performance of a single pressure relief device.
- The user must verify that HIPPS will work from a process standpoint and that the HIPPS design results in an installation as safe or safer than a conventional design.
- The effectiveness of the system is highly dependent on the field design, device testing, and maintenance program. Consequently, the user must understand the importance of application-specific design aspects, as well as the associated costs of the intensive testing and maintenance program whenever a HIPPS is utilized.
- When a pressure relief device is not installed or is undersized based on conventional design, the HIPPS becomes the “last line of defense,”

DEFINITIONS

BPCS - the control system used during normal operation and sometimes denoted as the process control system (PCS).

Commissioning - The functional verification of equipment and facilities that are grouped together in systems

Hazard - a physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these.

Impact event - the unwanted consequence of the hazardous event or accidental event which is referred to as a process deviation. Impact event is closely related to the unwanted consequence, and the question which remains is what degree of consequence an impact event represents, e.g. end-consequence or intermediate consequence.

Independent protection layers (IPL) - a PL that is capable of preventing a process deviation from proceeding to the end consequence, regardless of other PLs associated with the same impact event - initiating cause pair, and of the initiating event".

Initiating causes - the reasons why the process deviation occur, not the most basic underlying root-causes. The initiating causes are the results of the root causes

Intermediate event - the occurrence of the end-consequence with the existing / planned protection layers in place, but without the SIF under consideration.

Layer of Protection Analysis (LOPA) - an analytical tool to determine if there are sufficient layers of protection against a hazardous scenario.

Maximum Allowable Working Pressure (MAWP) - the maximum (gauge) pressure permissible at the top of a vessel in its normal operating position at the designated coincident temperature and liquid level specified for that pressure.

Mechanical Completion - The checking and testing of equipment and construction to confirm that the installation is in accordance with drawings and specifications and ready for commissioning in a safe manner and in compliance with project requirements.

Mitigated event likelihood - the occurrence of the end consequence with all protection layers in place, including the proposed SIF. The mitigated event likelihood is the frequency per year of the occurrence the this event

Overpressure - The pressure increase over the set pressure of the relieving device during discharge. It is also used as a generic term to describe an emergency which may cause the pressure to exceed the maximum allowable working pressure.

PHA (Process Hazards Analysis) - 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.

Process deviation (accidental event) - event or chain of events that may cause loss of life, or damage to health, the environment or assets

Pressure Relief Device - A device actuated by inlet static pressure and designed to open during an emergency or abnormal condition to prevent the rise of internal fluid pressure in excess of a specified value. The device may also be designed to prevent excessive vacuum. The device may be a pressure relief valve, a non-reclosing pressure relief device or a vacuum relief valve.

Protection layers (PL) - device, system or action that is capable of preventing a process deviation from proceeding to the end consequence".

PFD_{avg} - The average PFD used in calculating safety system reliability

PFD Probability of Failure on Demand - The probability of a system failing to respond to a demand for action arising from a potentially hazardous condition

Risk - The likelihood of a specified undesired event occurring within a specified period or in specified circumstances. It may be either a frequency (the number of specified events occurring in unit time) or a probability, (the probability of a specified event following a prior event), depending on circumstances.

Safety - The state in which the risk of harm to persons or of property damage is reduced to, and maintained at or below an acceptable level through a continuing process of hazard identification and risk management.

Safety Instrumented Function (SIF) - safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function.

Safety Instrumented System (SIS) - instrumented system used to implement one or more safety instrumented functions. A safety Instrumented System is composed of any combination of sensor (s), logic solver (s), and final elements(s).

SIS safety validation - all necessary activities to validate that the installed and mechanical completed SIS and its associated instrumented functions, meets the requirements as stated in the Safety Requirement Specification (SRS).

SIS lifecycle - Both standards chose to rely on the establishment of a design process, throughout which the performance of the instrumented systems must be maintained.

Safety Integrity Level (SIL) - discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

Safety layer matrix - a risk matrix which in addition to frequency and consequence takes the number of protection layers (PL) into account

Safety Requirements Specification - specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems.

Scenario - extended to describing ”the development from a process deviation to an impact event, including the causes leading to the process deviation”.

Validation - Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

ACRONYMS

BPCS	Basic Process Control System
CCPS	Center of Chemical Process Safety
ESD	Emergency Shutdown System
HAZOP	Hazard and Operability Study
HIPPS	High Integrity Pressure Protection System
I/O	Input/Output
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
PFD	Probability of Failure on Demand
PHA	Process Hazards Analysis
QRA	Quantitative Risk analysis
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLC	Safety Life Cycle
SLM	Safety Life Cycle Manual
SRS	Safety Requirement Specification
SSD	Safety shutdown systems