Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP – or - Why it is not necessary to "Boldly Go Beyond HAZOP and LOPA"

William G. Bridges, President
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
1321 Waterside Lane, Knoxville, TN 37922
Phone: (865) 675-3458
Fax: (865) 622-6800
e-mail: wbridges@piii.com

A. M. (Art) Dowell, III, PE
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)
2437 Bay Area Blvd PMB 260
Houston TX 77058-1519
phone: 713-865-6135
e-mail: adowell@piii.com

Prepared for Presentation at
12th Global Congress on Process Safety
Houston, TX
April 10-13, 2016

UNPUBLISHED

Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP – or - Why it is not necessary to "Boldly Go Beyond HAZOP and LOPA"

William G. Bridges, President
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)

A. M. (Art) Dowell, III, PE
PROCESS IMPROVEMENT INSTITUTE, INC. (PII)

Keywords: PHA, HAZOP, Hazard and Operability analysis, risk assessment, risk analysis, LOPA, IPL, independent protection layer, layer of protection analysis

Abstract

This paper shows how to apply the qualitative definition of IPLs within the setting of a process hazard analysis (PHA) to get most of the gain from *LOPA* without doing a LOPA (without using numerical values). The paper includes an implementation path to develop PHA leader competencies to guide the qualitative approach. We also show the way we use a PHA team to identify when a SIF is needed and to select the proper target SIL. This portion of the SIL evaluation and the identification and labeling of the IPLs during the PHA/HAZOP does not take any longer than a normal PHA/HAZOP, once the right habits are established. Note that this approach eliminates the need for a separate SIL Evaluation Study to identify the SIFs and select the target SIL. Finally, the paper ties together these two specific topics, along with the topic of making risk judgments, to show there is less than 5% need to go beyond HAZOP, and less than 0.01% need to go beyond LOPA.

Background

Identifying safety instrumented functions (SIFs) and other independent protection layers (IPLs) is important for any organization. Features that are designated as IPLs (including SIFs) are now being treated as "Safety Critical" or "Business Critical" or "Mission Critical" features.[1] These need to be maintained such that the predicted probability of failure on demand of the feature is actually achieved. These can be identified in a simplified risk assessment, such a Layer of Protection Analysis (LOPA).[2] But, these also can be identified with relative ease in a purely qualitative setting of a process hazard analysis (PHA) using hazard and operability analysis (HAZOP) or other PHA methods.

Similarly, a PHA team can usually identify in a qualitative sense if an instrumented safeguard loop meets the restrictions of a SIF. PHA teams can also be taught to assign qualitatively the necessary Safety Integrity Level (SIL) for the SIF. Per ANSI/ISA 84.00.01 Part 3, Section 3.8:

> *A qualitative method may be used as a first pass to determine the required SIL of all SIFs. Those which are assigned a SIL 3 or 4 by this method should then be considered in greater detail using a quantitative method to gain a more rigorous understanding of their required safety integrity*[3]

Many believe that only a quantitative analysis, such as LOPA, can identify the need for an SIF and assignment of the SIL necessary to reach tolerable risk. But, purely qualitative teams are permitted to make the same judgements and have been doing so for more than 50 years.

Once the IPLs (including SIFs) are identified, then the purely qualitative teams can make the final judgment on if the risk is a tolerable level or not. This last step is iterative and leads to the judgments of where additional or improved safeguards and IPLs are needed, including SIFs. The conclusion by the authors and most of our clients who follow this approach, is that once a PHA team is properly calibrated, they will be capable of judging tolerable risk and identify IPLs, including SIFs, without resorting to quantitative methods. Further, hundreds of PHAs have been performed using this approach, which together illustrate that less than 5% extra meeting time is required to identify and label the IPLs/SIFs.

This qualitative approach saves the time that it would take to do multiple LOPAs and yet still provides the comprehensive list of necessary SIFs (and their SILs) and other IPLs. The company can then use this information to assign inspection, test, and preventive maintenance (ITPM) activities and other management systems to ensure the necessary PFD against the accident scenarios are available.

Why is Qualitative Decision Making Normally Better than Quantitative?

As illustrated by the title of this conference session, "Boldly Go Beyond HAZOP and LOPA", many people believe that more quantification is better. But, a comparison of results of qualitative versus quantitative does not support this position. In the past, every quantitative analysis textbook, from *LOPA* (2001) to *Guidelines for Chemical Process Risk Analysis* (CPQRA; 1992), states that it is unrealistic to get an accurate estimate of risk for quantitative methods. Instead, QRA methods are mainly useful to compare risk of alternatives. The same is true of LOPA. Yet, more recently (CPQRA; 2000) most organizations use the risk estimated

from LOPA or QRA as approximations of the actual risk of a scenario and base absolute decisions on such estimates. This is somewhat puzzling given that broad assumptions are built into such estimates about control of human factors, management systems, accuracy of the average failure rates used, and uncertainty (range of data that is used to provide the average) in the failure rates.

The authors are proficient in all of the risk assessment methods, from purely qualitative to full quantitative, and have supervised (and helped perform) more than 7000 PHA/HAZOPs, 3000 LOPA, and about 100 QRAs (and human reliability analyses [HRAs]). Assuming each analysis is performed by highly competent staff, the conclusions are that qualitative analysis is usually (more than 95% of the time) better than quantitative analysis at judging the risk of specific accident scenarios. By "better" we mean the PHA team can use more relevant data (their experiences at the site) which is nearly always more pertinent and more accurate than data from lookup tables provided in CCPS LOPA textbooks and other sources. Some may comment here that "highly competent staff" are difficult to come by on the PHA teams. We certainly understand that challenge. But that does not change the fact that without an excellent PHA, your organization will miss Many process safety scenarios and these scenarios are much more likely to not have sufficient safeguards in place. Having a highly competent PHA team is much more important than any other discussion point in this paper.

Note that CCPS textbooks on QRA and LOPA recognize the value of PHAs. As the newest CPQRA textbook (2000) concedes ***"… where the risks are clearly excessive and the existing safeguards are inadequate, corrective actions can be adequately identified with qualitative methods."*** And the LOPA book (CCPS, 2001)[2] lists and answers myths about LOPA being better than PHA/HAZOP, which it is not.

Based on analyses of these methods and their results, we believe a spectrum of methods is best, with qualitative methods being the first choice, and then other methods being used if the qualitative analysis team (PHA/HAZOP team) is confused on the risk. The summary below (Table 1) compares the three major risk analysis approaches:

Table 1: Comparison of Risk Analysis Approaches vs. Uncertainty and Usefulness

Approach	Assessment Methods	Risk Judgment Method	Estimated Range of the Results	Comments
Qualitative only (no numbers; not even a risk matrix).	What-If HAZOP of parameters HAZOP of steps FMEA	Voting of experts, from the specific site, but including at least one expert from outside of the process under review. **Fully capable of judging risk more than 95% of the time.**	Within one IPL of minimal value (so within about an order of magnitude)	Heavily focused on site-specific experience, with some consideration of general industry data and incidents
Simplified quantitative	LOPA RiskGraph	Multiplication of statistical averages of general failure rate data. **Was necessary to judge risk on about 5% of the scenarios.**	Plus and minus an order of magnitude, since the range of data for some to most inputs data is plus and minus an factor of 10	Typically does not use site-specific data for the PFD and IEF. Broad assumptions made about management systems at the site

Full quantitative	Fault Tree Event Tree Consequence modeling Human reliability event tree Bow Tie	Multiplication of statistical averages of general failure rate data; in some cases modified by expert opinion based on site-specific evidence. **Was needed for less than 0.01% of the scenarios.**	Plus and minus an order of magnitude, since the range of data for some to most inputs data is plus and minus an factor of 10	Typically does not use site-specific data for the PFD and IEF. Broad assumptions made about management systems at the site. See paper from Bridges and Dowell, 2015, for illustration of how QRA underestimated risk by three orders of magnitude in nuclear power PRAs.

General Approach to Qualitative Determination of IPLs and SIFs

One of most valuable outcomes of starting LOPA in the mid-1990s was the crystallization of the qualitative definition of an IPL. If the PHA/HAZOP leader was competent in the definition of an IPL, we found that IPLs could be just as easily identified in a PHA/HAZOP as in a LOPA. This was a significant outcome, since IPLs are what we need to focus on to maintain tolerable risk for each scenario; in other words, we can focus our reliability/maintenance efforts and operational efforts on IPLs to conserve resources while maximizing control of risk. SIFs are just one type of IPL and we found the same was true for identifying SIFs and setting their SILs. Also, as mentioned earlier, ANSI/ISA 84.00.01-2004 allows SIL to be set qualitatively.[3] The following sections explain the steps to achieve the competency necessary in the PHA/HAZOP team leader, scribe, and/or members to allow these qualitative judgments. COMPETENCY, as always, is King; the path to competency includes learning the rules for using this approach, so the rules are explained first in this paper. After a review of rules, the steps for **intentional competency development** are explained in more detail.

Review of Rules for an IPL

Below are the set of rules for each IPL. These rules can each be applied "qualitatively" to each candidate IPL. (These are similar to those found in Guidelines to Initiating Events and Independent Protection Layers.[1])

1. **Each protection layer must be truly independent of the other protection layers and independent from the initiating event (IE). That is, there must be no failure that can deactivate two or more IPLs and the IE cannot deactivate an IPL.**

   An IPL (or an IE) includes the ENTIRE sub-system, including any root valves, impulse lines, and bypasses. The other IPLs (nor IE) cannot share any of these (except for the mother board when using approach B for BPCS loops), and describe the textbook on LOPA.[2]

   A device, system, or action is **not** independent of the initiating event and cannot be credited as an IPL for either approach if either of the following is true:

   - Operator error is the initiating event and the candidate IPL assumes that the same operator must act to mitigate the situation. Human error is equivalent to the failure of a system and once a human has committed an error it is not reasonable to expect the same operator to act correctly later in the sequence of events. This approach is justified because the error may be due to fatigue, illness, incapacity (drugs or alcohol), distraction,

work overload, inexperience, faulty operating instructions, lack of knowledge, etc., that are still present later when the action is required.

- Loss of a utility (electricity, air, cooling water, nitrogen, etc.) is the initiating event and a candidate IPL is a system that depends on that utility.

Other examples where the IPL is not independent include:

- Multiple flow meters, analyzers, etc., with a calibration error or other error during testing, due to human error, faulty calibration instruments, etc.
- Multiple units or SIF systems with a single source of power or a common circuit breaker unless it can be determined that fail safe action will always be initiated in the event of power loss—this is true for any other utility required for an IPL to reach a safe state;

2. A control loop in the BPCS whose normal action would compensate for the initiating event can be considered as an IPL.

For example, an initiating cause for high reactor pressure could be failure of a local upstream pressure regulator; the normal action of the reactor pressure controller would be to close the inlet PV, thus providing protection against the impact event.

NOTE: Under specific conditions, a BPCS can be used twice in the same LOPA scenario, as described later in detail in the LOPA book[2] and IPL book[1]. But, under no circumstance can a BPCS be used more than twice in the same scenario. So:

a) a BPCS loop failure can be an initiating event

b) a BPCS loop (the entire loop) can be an IPL

c) a BPCS loop can give an alarm and then a human respond as part of a human IPL

…but in LOPA, the maximum use of a BPCS is one case of a and b, or two cases of b, or one case of a and c, or one case of b and c.

3. The frequency reduction for an IPL is at least one order of magnitude, i.e., 10^{-1} PFD (that is, the availability is 90%).

- ***Example:*** If the operator has sufficient time to react, then the risk reduction for Operator Response to an Alarm is one order of magnitude, i.e., 10^{-1}

4. The IPL is capable to prevent or mitigate the consequences of a potentially hazardous event. To make this judgment, the evaluator (such as the PHA team) must ask:

- Is the IPL valid for the mode of operation for the scenario (startup, shutdown, normal, batch, etc.)
- Is the IPL applicable to the scenario under consideration? For instance: Is the PSV even designed for this scenario?
- What are the maintenance/reliability practices and plant/company history? How much likelihood reduction credit will you take for a relief valve?
- How good are the procedures and related training practices? Were the operators trained in specifics of how to respond to this alarm/indication?
- Consideration of standards and certifications (PSV code stamp; IEC 61508 classification,

etc.) can help ensure safeguards qualify as IPLs.

5. **The IPL must be *Maintained* and *Validated* periodically; it must be proven that the IPL can be counted on to do what it was intended to do.**

   The IPL must be periodically maintained and it must be proven or validated. The site must have data that supports the reliability factor. The frequency and test method must comply with best industry practices for such IPLs. Also, the site must maintain a database for each IPL that statistically supports the PFD stated. For a component or instrumentation IPL, this requires maintaining a statistical failure rate database that justifies the PFD listed for each IPL. For a human IPL, the site must maintain data from "drills" of the action of the worker that statistically demonstrates that the worker(s) can indeed implement the required action (of the IPL) with the time specified in the IPL. For a PFD of 10^{-1}, the statistical data must support that 90% of the recorded data demonstrates the necessary speed and reliability. For a PFD of 10^{-2} the statistical data must support that 99% of the recorded data demonstrates the necessary speed and reliability.

6. **The IPL maintenance and validation must be *Audited*.** Auditing is required to ensure the validation, procedures, training, and resulting data are adequate. This is an administrative check. This auditing cycle is set frequent enough (typically 1 year for the first audit and then 5 year frequency after that) to ensure that validation is being carried out as planned and is sufficient to justify the IPL and its PFD.

7. **Specific errors (such as leaving an IPL bypassed) and systemic failures (such as the instrument tap plugging) that would impact the performance of the IPL (also applies to IEs) must be considered in the PFD (or IEF).**

   Example: When considering a PSV as an IPL; if there is a block valve (B/V) upstream or downstream of the PSV then the probability of leaving this closed (and perhaps even car-sealed-closed) must be included. Currently, site data indicates this probability is between 0.01 and 0.04, which means a PSV valve of 0.01 is Not valid.

   Example: When considering a SIL 2 or 3, systemic errors and failures can obviate the redundancy and increase the PFD (increasing the risk) since some of these errors and failures can themselves be 0.01 or higher. The SIL Verification for SIL 2 and 3 must account for these systemic errors and failures or else the assigned SIL is not valid; they may be no better than a SIL 1 in actual performance. (See later comments of SIS for LOPA).

8. **Related to 7, the boundary for the IPL (or IE) must include all relevant components upstream and downstream that could affect the performance of the IPL (or IE).** For example, for a PSV, the IPL includes the PSV as well as any inlet and outlet piping and any isolation valves upstream or downstream. Similarly, as shown on the Boundary B of Figure 1, an SIF boundary includes the root valves, impulse lines, and any bypasses associated with the SIF.

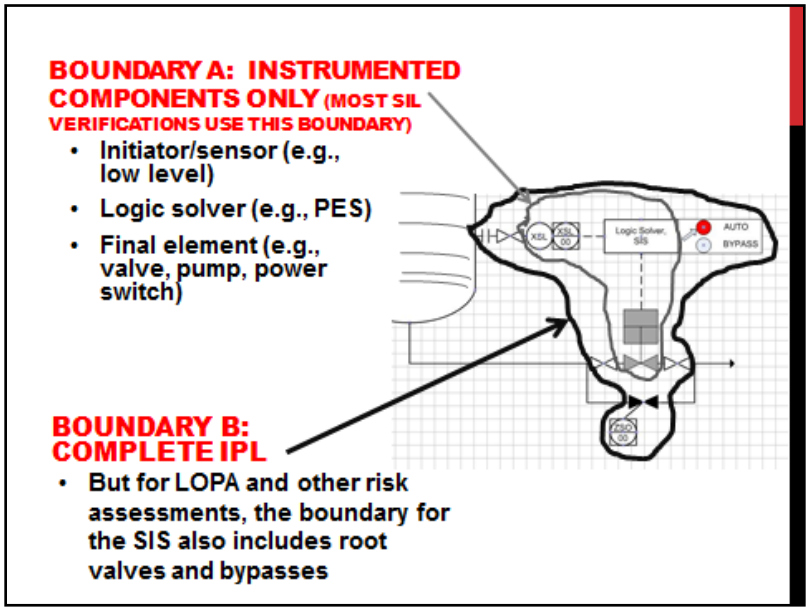


Figure 1. The True Boundary for an IPL includes all associated connections, isolations, and bypasses. Note how the traditional SIL Verification calculation boundary is much different that the true IPL boundary

Review of Specific Rules and Example Architectures of SIFs of Various SIL

The design of SIFs to meet a required SIL can be complex in certain applications, but in general a **SIL 1** SIF is a single loop that uses devices rated for use in a SIF of the appropriate SIL, including a safety PLC that is independent of the BPCS (control system), and that is rated for use in an SIF of the appropriate SIL. Figure 2 shows a typical example of a SIL 1 SIF configuration. These are tyically one sensor or switch, going to one fast acting final element (like a shutdown valve). These typically have a calculated PFD in the range of 0.03, depending on the proof test interval.

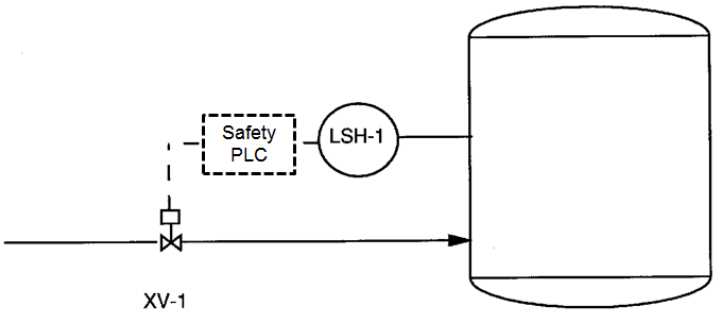


Figure 2. Typical configuration of a SIL 1 SIF

It should be noted that the achieved safety integrity level for an SIF is a function of the architectural constraints requirements for the particular SIL in addition to the PFD requirements for the SIL. The architectural constraints depend on the safe failure fraction of the devices, the voting architecture, and the diagnostics for the device.

The PFD of the SIF depends on the voting architecture, the failure rate of each device, the diagnostics to detect failures, and the proof test interval for the SIF.

In general a **SIL 2** SIF is a safety loop similar to a SIL 1, but which uses one or more redundant devices, that are voted one-out-of-two (1oo2) or better, for the safety functions. Depending on the architectural constraints requirement, the failure rate and diagnostics of the devices, the voting architecture, and the proof test interval, redundant devices may be required for the sensors and for the logic solver and/or for the final element. Figure 3 shows two typical configurations for SIL 2 SIFs – when redundancy is either be in the sensor/ switch/ transmitter devices (so, in the example shown here, two level swiches) or in the final element (such as two shutdown valves, where at least one needs to close for safety purposes). The calculated PFD for such systems, if the specific human erorrs of leaving the SIF in bypass or of miscalbrating of two devices is ignored, will be about 0.009, depending on the proof test interval.

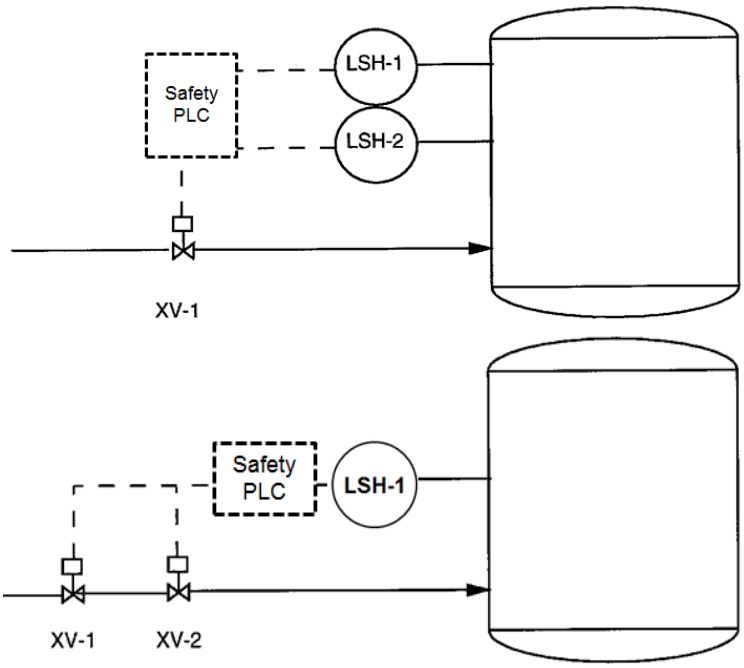


Figure 3. Typical configurations of SIL 2 SIFs

The required PFD for a **SIL 3** SIF is likely not possible to achieve in practice, as the human errors for maintaining such systems is greater than the target PFD of 0.001 to 0.0001. But, if such a system is designed to compensate for all such errors, then SIL 3 usually have both redundancy in the sensors and in the final elements. Figure 4 shows a typical example of a SIL 3 SIF configuration.

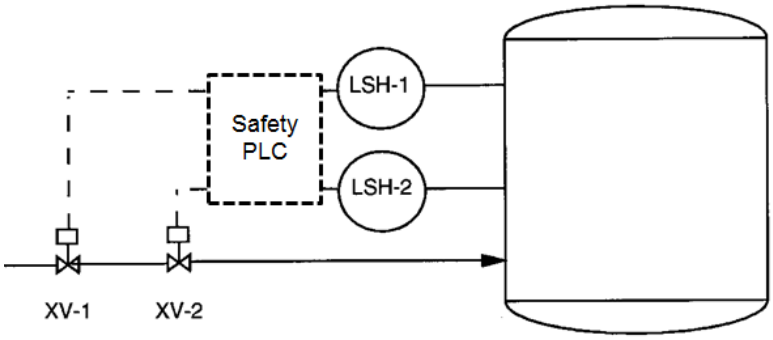


Figure 4. Typical configuration of a SIL 3 SIF

Note that there are architectural constraints and common mode issues for SIL 2 and SIL 3 that are beyond the scope of this paper. And of course there are more complex configurations for SIFs, but typically, they follow the patterns above.

Once the PHA leader and scribe understands the typical configurations of SIFs for the various SILs then they must learn the basic rules of SIS (which are listed in detail in IEC 61508 and 61511[ANSI/ISA 84.0 0.01-2004])[4], which are simplified below:

- Devices rated for use in a SIF of a particular SIL must be used (or "proven in use" devices must be used)

- All of the rules of an IPL must be followed for any SIF (e.g., the SIF cannot share any components with the BPCS)
- Only one SIF is allowed for a scenario per SIS (That is, all the safety instrumented functionality for a given scenario should be evaluated as one SIF, if contained within the same SIS.)
- The ITPM stated in the Safety Requirements Specification (SRS) must be followed and documented.

The PHA leader or scribe can now begin to judge qualitatively if a loop shown on a P&ID is intended to be a SIF or not, and if so, if it meets the basic rules of a SIF.

If the PHA team feels that a SIF is the best way to reach tolerable risk (given that the risk of the scenario is judged to be intolerable), and a SIF is not present or is not of a high enough rating, then the PHA team can recommend a SIL 1, 2, or 3 SIF (though at PII we do not typically go along with recommendations for a SIL 3 SIF, for the reasons mentioned earlier).

Implementation Path – Intentionally Achieving COMPETENCY in the Qualitative Definition of an IPL and SIF

Now that the rules and descriptions of SIFs (of various SILs) and other IPLs are defined, the next requirement for adequately using these in a qualitative PHA is for the **PHA team leader to understand fully these rules and definitions and to be competent in their application.** Many PHA leaders are not competent in even how to conduct a PHA; in fact, about 90% of the PHAs reports that we have reviewed around the world are woefully deficient, especially with respect to finding scenarios during startup, shutdown, and online maintenance. Per the authors experience, the path to the necessary competency is typically:

- Already be an experienced PHA leader, trained in all PHA methods, and capable of applying these methods to all modes of operation and capable to make sound qualitative judgments, along with the PHA team members, on when the number and type of IPLs is sufficent to control the risk. Achieving full competency as a PHA leader may require some remedial training on how to lead PHAs of startup, shutdown, and online modes of operation; or remedial training on how to uncover and discuss all plausible damage mechanisms. This assumes the PHA leader has the correct technical background, including many years in operations. *A poster from the classroom training from 2003 is shown in Figure 5.*

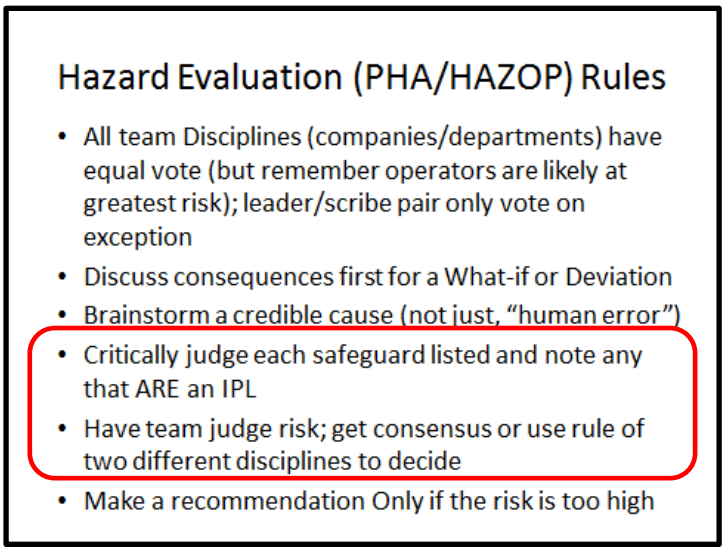


Figure 5. Wall Poster of PHA Rules; PII, 2003-2016 ©

- Attend a LOPA course to learn the basics of IPLs (including SIFs) as described in the previous sections. Or, attend a more progressive training course for PHA/HAZOP leadership that covers the definitions of IPLs and provides exercise time on how these determinations are made. The key on qualitative risk judgment is to know when there are enough IPLs for the accident scenario under review. *Another poster from the PHA Leadership classroom training from PII since 2003 is shown on the right* ➔

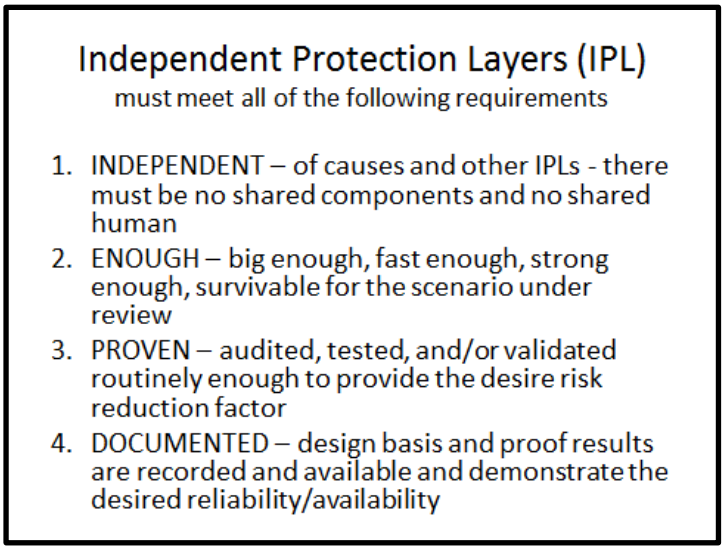


Figure 6. Wall Poster of IPL Rules; PII, 2003-2016 ©

- Get coaching (by someone already competent) during actual PHAs to learn how to help a team make judgments if safeguards meet the definition of an IPL (or SIF) or not and also on if there are enough IPls for the accident scenario (risk judgment). The PHA team leader must have either seen (or done) enough LOPA of similar nature to make such judgments or the PHA team must be able to judge when to go to LOPA or not. We know from thousands of PHAs over the past decades that a PHA team can make excellent risk judgments > 95% of the time, which also means that the IPLs and SIFs can be clearly identified > 95% of the time.
- Achieve competency, in the opinion of the competent coach on the skills above.
- In addition to the PHA team leader competency, the PHA team has enough understanding of either qualitatively risk judgment or LOPA risk judgment– just in time training by the PHA leader (we tend to accomplish this training across the first 5-10 accident scenarios we discuss):
  - IPL requirements – difference between just a safeguard and a safeguard that is an IPL
  - Initiating cause frequency
  - Consequence severity
  - Required mitigated consequence frequency to meet risk criteria for that consequence severity; or the Required IPLs qualitatively necessary to reach tolerable risk.
  - Risk reduction provided by existing IPLs

Implementation Path – Using the Qualitative Definition of an IPL and SIF

The competent PHA/HAZOP leader can now guide the PHA/HAZOP team through the following thought processes:

- IF (1) the safeguard meets the definition of an IPL and (2) if the team believes (qualitatively) this safeguard is critical to control risk to tolerable level (qualitatively),then add the designator " – IPL" to the right of the safeguard text (or else,

turn on the "IPL Type" column in HazardReview LEADER [by ABS Consulting] and select the IPL type from that pulldown menu). If the safeguard is not going to be labeled an IPL, then it can be run to failure; unless the safeguard supports an IPL, such as when a sight glass support an LAH used in an Human Response IPL, in which case the sight glass will have some ITPM (such a periodic cleaning of the sight glass).

- IF an instrument is already in the ESD system or SIS and qualitatively meets the archetecture of an SIL 1, or SIL 2, or SIL 3, and also meets the definitions/rules for an IPL, then add the "- SIL-1" (or SIL-2, or SIL-3) to the right of the text (or else, turn on the "IPL Type" column in HazardReview LEADER and select SIL-1, 2, or 3 from that pulldown menu). *See the screen shot of a LEADER window of a PHA/HAZOP table in Figure 7.*

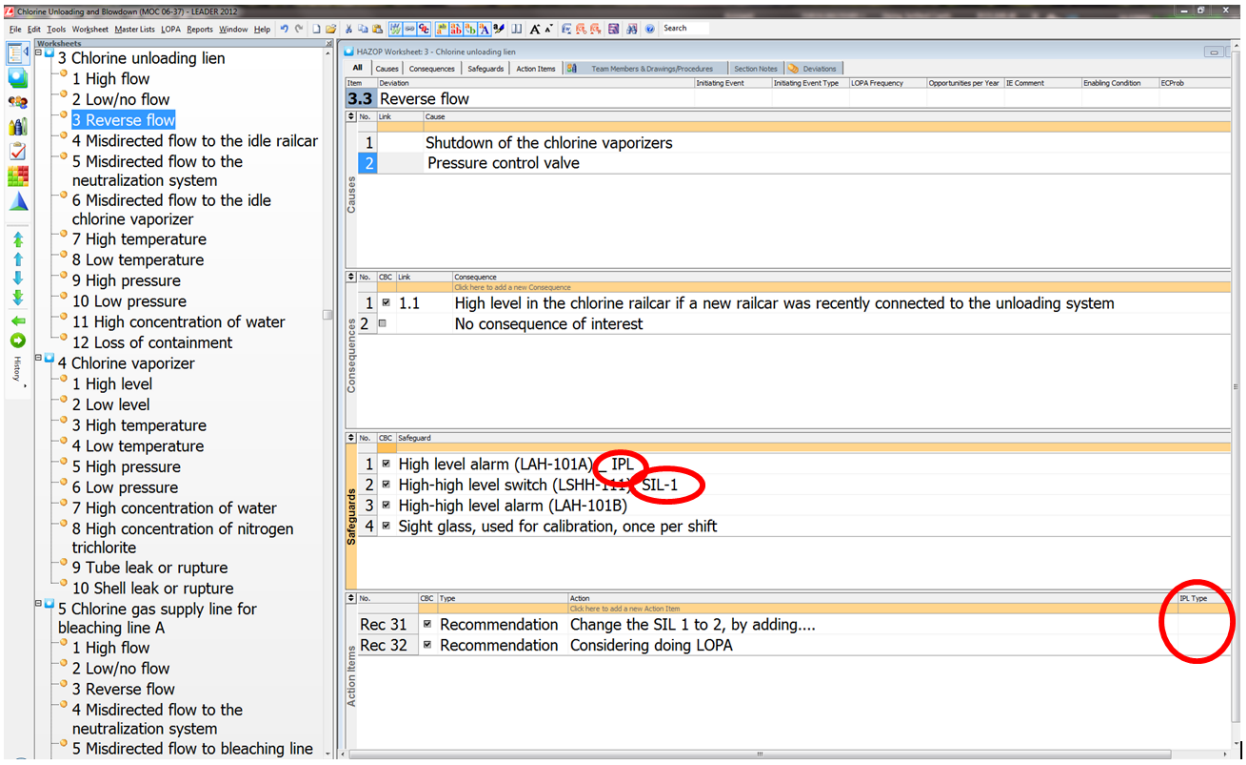


Figure 7. Screen Shot of LEADER software showing designation of IPL and SIL in the HAZOP Record

The non-human IPLs identified can be maintained as critical features in reliability/maintenance systems. For SIFs, the facility should have the SILs verified by calculations and have the SRSs developed. The human IPLs can be tested/drilled once a year. All of these activities are to ensure the IPLs/SIFs deliver the PFD anticipated, while still ensuring reliable operation/control by not cause too many spurious trips.

CASE STUDIES

Case Study 1 – Sinopec-SABIC Tianjin Petrochemical Company (SSTPC)[5]

PHAs of 9 full petrochemical plants were led and documented in 2013 - 2015 (see complete paper from 2015 GCPS).[5] The results were documented in English into *HazardReview LEADER*™ software; a Word report was generated for each unit's PHA. This report contains the typical entries, with considerable detail developed for each scenario. Excerpts from the report are shown in Table 1.

Table 2: Excerpts from Petrochemical Process PHA at SS-TPC[5]

No.: 2 XXXX storage spheres xxx-T-XX A/B/C/D/E/F/G/H/I/J/K/L (1 of 12)					
#	**Dev.**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
2.1	High level	Too much flow to one sphere from XX Plant (through their pump; about 40 bar MDH)	High pressure (see 2.5)	High level SIF with level sensors voted 2oo2, to close inlet valve - **SIL 1** Overflow thru pressure equalization line to other spheres (through normally open [NO] valve) - **IPL**	
		Misdirected flow - Liquid from xxx Plant(s) to spheres (see 1.4)	Overpressure of sphere not credible from high level, for normal operating pressure of the column (which is 1.75 MPa), unless all spheres are liquid filled and then thermal expansion of the liquid could overpressure the spheres	High level SIF with level sensors voted 2oo2, to close inlet valve - **SIL 1** Overflow thru pressure equalization line to other spheres (through normally open [NO] valve) - **IPL** Spheres rated for 1.95MPa (19.5 Bar, approx) and the highest pressure possible from the column feeding the spheres is 1.75 MPa Level indication and high level alarm in DCS, used by operators to manually select which tank to fill - **IPL**	
			Overflow into the equalization line will interfere with withdrawal from the column, but this is an operational upset only		
			Excessive pressure on inlet of high pressure liquid pumps, leading to excess load on pumps and trip of pumps on high pumps, causing trips of xxx, xxx, etc. - significant operability issue		
2.2	Low level	Failing to switch from the sphere with low level in time (based on level indication)	Low/no flow - Liquid from spheres through high pressure product pumps to the vaporizer (see 4.2)	Level indication and low level alarm, inspected each year, per government regulation **(not IPL; part of the cause)** 9 other spheres with possibly enough level to switch to Feeding from two spheres at all times, so unlikely for BOTH spheres to have low level at the same time - **IPL** Two level indication from SIS level transmitter, with low level alarm, with more than 60 min available to switch tanks (SIF driven alarm and	Rec 4. Make sure the Human IPL of response to low level in all spheres and tanks is described in a trouble-shooting guide (like an SOP) and practiced once per year per unit operator. This will make this response a valid IPL.
			Low/no flow - Unqualified liquid from spheres back		

No.: 2 XXXX storage spheres xxx-T-XX A/B/C/D/E/F/G/H/I/J/K/L (1 of 12)					
#	**Dev.**	**Causes**	**Consequences**	**Safeguards**	**Recommendations**
			to Plant (see 6.2)	response) - **possible IPL, if action of the operator is quick enough**	
2.3	High temp.	Large area of damaged insulation Loss of cooling. when the tank is isolated from column	High pressure - vapor from spheres through condenser and return to liquid pump out line (only used when plant is shutdown) (see 3.7)		
2.4	Low temperature	Deviation during startup (see 2.9)	Loss of containment - due to sudden flashing to -100 °C; if there is also a sudden vibration (such as by the flashing from liquid to gas) (see 2.8)	Temperature indication	Rec 5. Consider adding an IPL, such as an interlock, to prevent opening of the isolation valves for liquid into a sphere (following maintenance or an outage), until the sphere has been pressurized with vapor, to prevent brittle fracture of the sphere and to prevent thermal shock of the sphere.
2.5	High pressure	Liquid filled and left blocked in	Loss of containment (see 2.8)	Pressure indication and high pressure alarm in DCS (1 on each of the 12 spheres); with operator response (with practice/drills) - **IPL** (Note: The pressure control valve to the flare is normally blocked in; and is only used when the standby cooling system is used)	
		High pressure in the gas equalization line from column	Loss of containment (see 2.8) More losses to flare from sphere - economic consequence	(Note: The pressure control valve to the flare is normally blocked in; and is only used when the standby cooling system is used)	

To help the teams make consistently good judgments on risk, each safeguard was judged to determine if it met the definition of an IPL or not. The team then qualitatively judged the risk (voted; sometimes with pressure from the team leader) and decided if the risk was controlled well enough; if not, then recommendations were made to reduce the risk to tolerable levels. As a cross-check of these judgments, SS-TPC required the PHA team also to score (using a calibrated risk matrix or LOPA) any scenario that had catastrophic consequences. The results turned out the same as purely qualitative risk judgment. The team also determined if a safety instrumented function (SIF) was needed (if a SIF was the best way to achieve tolerable risk) or if a SIF was intended in the design (based on the configuration of the dedicated safety instrumentation). If there was a SIF, the PHA team assigned the SIL based on either the risk reduction needed from the SIF or again by evaluation of the existing instrument configuration.

It was noted in some cases that the SIF that was installed for protection against scenarios during continuous mode of operation did not protect against even more catastrophic and much more likely consequences during startup or online maintenance. For such situations, additional IPLs, including SIFs specific to startup or online maintenance, were recommended by the PHA team.

The PHA covered all modes of operation for the units; besides a HAZOP or What-if of continuous modes of operation, the PHA team also used the Two Guideword or What-if approach to complete a PHA of startup, shutdown, and online modes of operation. The PHA of the non-routine modes of operation took about 25% of the total meeting time and was done at the end of the unit PHAs. This portion of the analysis followed the requirements in Chapter 9 of Guidelines for Hazard Evaluation Procedures[6], as improved in Bridges[7].

Many Other Case Studies

PII has led hundreds of PHA/HAZOP of entire process units over the past 13 years using the approach described above. In these cases, the PHA/HAZOP team, by itself, was able to make the determination of risk and the determination of IPLs and SIFs using only qualitative judgment about 97% of the time (95 to 100% of the time). In about 3% of the cases, a LOPA was recommended by the PHA/HAZOP team to help clarify the risk of a scenario. A full QRA (FTA, ETA, Consequence modeling, and/or HRA) was necessary and recommended for less than 0.01% of the scenarios. Clients for which qualitative judgment and qualitative identification of IPL and SIF/SIL were performed include:

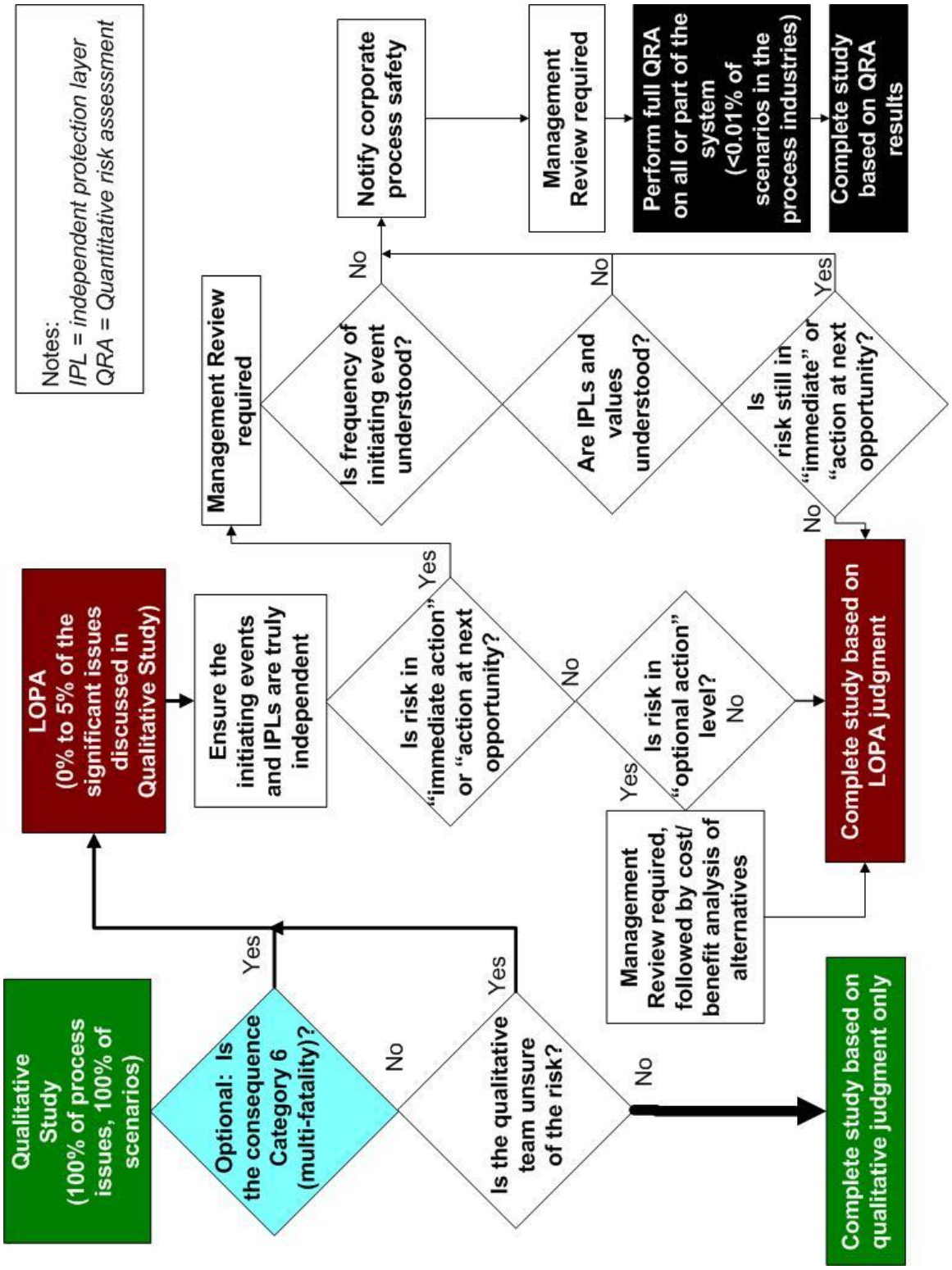
- Advanced Turbine (ATTSSA; Saudi Arabia)
- CABOT (EU)
- ECOLAB (USA)
- Elementis (USA)
- Gulf Petrochemical (GPIC; Bahrain): 4 plants
- Irving Oil (Canada): 2 units
- MIDREX (USA)
- MOL Pakistan (Gas plant in Pakistan)
- PlusPetrol (Peru): 5 gas/oil well clusters, 5 gas processing trains
- Peru LNG
- QAFCO (Qatar): multiple ammonia, urea, and other plants; 7 process plants in all
- Roquette (USA)
- SABIC (Saudi Arabia): several affiliates; about 15 plant-size PHAs)
- SS-TPC (China, see Case Study 1): 9 petrochemical plants
- SUNCOR
- WISON (China)
- Many others – anonymous

In addition, we have trained hundreds of PHA/HAZOP leaders how to do the same, though we have only provided the follow-on coaching for about 20.

Summary

Based on the data above, the choice of methods for risk judgment is shown in Figure 8.

Figure 8: Flowchart for Risk Judgment Methods



So, PHAs using qualitative methods has been shown to work effectively for making >95% of the risk judgments and for also judging which safeguards qualify as IPLs, including which qualify as SIFs and what SIL is warranted. And, others can learn to do the same with reasonable investment of time.

Further, adding these assignments to the task list of the PHA team leader/scribe increases the time required for the PHA by only about 0 to 5% (all of the increase, if any, is in extra documentation load).

Finally, our experience indicates that when companies want to over-use quantitative methods (starting with LOPA as the next step) for risk judgments and identification of IPLs and SIFs/SILs, they describe their needs in one of the following ways:

- "The PHA team leaders we use, coupled with the less-than-expert team members we provide them, are not competent to make good risk judgments." *Our suggestion is to work on this problem as a HIGH PRIORITY, since no amount of additional LOPA can fix this problem, and no other activity (other than near miss reporting) can find the accident scenarios you are missing.*
- "We want to get a Better estimate of the risk; HAZOP and other qualitative methods simply can't do that." *This is a myth; LOPA and QRA do NOT provide better risk estimates. In fact, the PHA methods likely have the lower error band on the risk estimate, because at most, we have found the qualitative teams off by 1 IPL (PFD = 1E-1) on their judgment of tolerability of risk.*
- "The PHA team leaders, and the teams we give them, do not make consistent risk judgments." *Our suggestion is to work on this problem by coaching of the PHA team leaders. Adding requirements for more quantification within the PHA meetings will lead less productive brainstorming, and therefore more accident scenarios being missed. And adding more LOPA outside of the meetings will result in a significant waste of time. The alternative of bolstering the skills of the PHA team leaders is much more productive.*

Conclusions

So, there is no need to **"Go Boldly Beyond HAZOP and LOPA."** The opposite is true. Organizations should instead **"Bring Hazard Identification and Risk Assessments Back to Earth".** There is plenty of practical evidence presented in this paper and available elsewhere than shows qualitative voting by a group of experts (the PHA team) does a better job >95% of the time than artificially defining the same scenario to fit within the bounds of LOPA or QRA and using "other people's data" as inputs.

It is critical that the PHA leader:

- Be trained and coached in LOPA and/ or in qualitative IPL definitions and in judging if there are sufficient IPLs.
- Be trained, coached, and confirmed to be able to guide the PHA/HAZOP team in the identification of true IPLs and the sufficiency of the IPLs (including SIFs) for the scenario; this can only be done by someone who is already fully competent already.

Acronyms Used

AIChE– American Institute of Chemical Engineers
BPCS – Basic Process Control System (such as a distributed control system [DCS])
CCPS – Center for Chemical Process Safety (of AIChE)
EHS – Environment, Health, and Safety (includes process safety)
ESD – Emergency Shut Down
ETA – Event Tree Analysis
FTA – Fault Tree Analysis
HAZOP – Hazard and Operability Analysis
HRA – Human Reliability Analysis
IE – Initiating Event
IEF – Initiating Event Frequency
IPL - Independent Protection Layer
LOPA – Layer of Protection Analysis
LSH – Level Switch High
MOC – Management of Change
PFD – Probability of Failure on Demand
P&ID – Piping & Instrumentation Diagram
PHA – Process Hazard Analysis
PLC – Programmable Logic Controller
PSI – Process Safety Information
PSM – Process Safety Management
PSV – Pressure relief valve or pressure relief valve
QRA – Quantitative Risk Analysis
SIF - Safety Instrumented Function
SIL - Safety Integrity Level
SIS - Safety Instrumented System
SS-TPC – Sinopec SABIC Tianjin Petrochemical Company

References

1. *Guidelines for Initiating Events and Independent Protection Layers*, 2015, CCPS/AIChE.
2. *Layer of Protection Analysis: Simplified Process Risk Assessment,* 2001, CCPS/AIChE.
3. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels*; ANSI/ISA 84.00.01 Part 3, 2004.
4. IEC 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements,* International Electrotechnical Commission.
5. "Implementation of Process Hazard Analysis at SINOPEC-SABIC Tianjin Petrochemical Company Ltd, China**",** Homoud Al-Maymouni, Yunzhong Gao (both from SS-TPC), and W. Bridges, *11th Global Congress on Process Safety*, Austin, TX, AIChE, April 2015.
6. *Guidelines for Hazard Evaluation Procedures,* 3rd Edition, 2008, CCPS/AIChE.

7. Bridges, W. and Clark, T., "How to Efficiently Perform the Hazard Evaluation (PHA) Required for Non-Routine Modes of Operation (Startup, Shutdown, Online Maintenance)," *7th Global Congress on Process Safety*, Chicago, AIChE, March 2011.