LOPA in Action: Making Sure Initiating Events (IEs) and Independent Protection Layers (IPLs) are Included in Integrated Management Systems

William Bridges
President
Process Improvement Institute, Inc. (PII)
1321 Waterside Lane,
Knoxville, TN 37922 USA
wbridges@piii.com

Paul Casarez
Principal Engineer
Process Improvement Institute, Inc. (PII)
1321 Waterside Lane,
Knoxville, TN 37922 USA
pcasarez@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2020 Spring Meeting and 16th Global Congress on Process Safety
Houston, TX
March 30 – April 1, 2020

LOPA in Action: Making Sure Initiating Events (IEs) and Independent Protection Layers (IPLs) are Included in Integrated Management Systems

Paul Casarez
Process Improvement Institute, Inc. (PII)

Presenter:
William Bridges
Process Improvement Institute, Inc. (PII)

Keywords: Process Hazard Analysis, PHA, HAZOP, Risk Assessment, Hazard Identification, Independent Protection Layers, IPLs, Initiating Events, IEs, Layer of Protection Analysis, LOPA, Mechanical Integrity, Asset Integrity, Risk Based Process Safety, RBPS

Abstract

This paper focuses on ensuring that risk is effectively maintained by ensuring that each Initiating Event (IE) and each Independent Protection Layer (IPL) is included within integrated management systems. Topics covered include:

- Extracting IEs and IPLs from Process Hazard Analyses (PHAs) for inclusion in mechanical integrity, asset integrity, and operational discipline programs to ensure the reliability factors targeted for each is achieved in practice.
- Auditing techniques for checking if IEs and IPLs listed in PHAs are being maintained. The paper will share an auditing protocol that has proven valuable for this step.
- Measuring the Initiating Event Frequency (IEF) for IEs and Probability of Failure on Demand (PFD) for IPLs. This includes ensuring the effectiveness of human IPLs per the approach described in earlier papers on this topic; these approaches will be summarized here. (Another paper in this conference, *People as Safeguards – When are Human IPLs Valid, and How are their PFDs Assured in Practice*, describes Human IPL validation in more detail.)
- Examples are shared for each step above.

Every organization spends a lot of effort conducting Process Hazard Analyses (PHA), Hazard and Operability Studies (HAZOPs), Layer of Protection Analysis (LOPA), and perhaps other risk assessments. However, the usefulness of these studies is significantly reduced if the likelihood of the causes (initiating events, IEs) and the probability of failure on demand (PFD) of the safeguards (particularly the independent protection layers, IPLs) are not maintained. Yet, many companies (1) do not have a defined program for ensuring that each IE and each IPL is included in the mechanical integrity (MI) and/or reliability program and (2) do not effectively audit to ensure the IEs and IPLs are included and that the needed Inspection, Testing and Preventative Maintenance (ITPM) is performed, documented and managed. This paper provides guidance and examples of how to do both.

1 Review of the Users and Uses of results from PHA/HAZOPs & LOPA

As stated in an earlier paper [1], there are many users of the results of the PHA/HAZOP and LOPA studies. Table 1 is a partial listing of the users and uses, in relative order of importance (the ordering is based on the combined experience of PII, who have helped more than 50 organizations implement process safety and who have led and documented thousands of PHAs of entire units or plants.)

Table 1. Uses and Users of IE and IPL Information Derived in PHA/HAZOP and LOPA Studies [1]

Engineering

Identifying the IPLs needed *(including SIFs)*

Identifying the target SIL *(if SIF used)*

Finding limiting case for PSV & flare sizing

Determining fire protection needs

Facility Siting

Error proofing designs

Mech. Integrity

List of IEs and IPLs *(all safety critical equipment; SCE)*

Unique Corrosion/ Erosion Issues

Bypassing plans and time limits, and therefore critical spares

SCE that may require staggering of maintenance

Operations/Training

List of Human IEs and Human IPLs *(all safety critical actions)*

Alarm rationalization *(all safety critical alarms)*

Provides Input to Trouble-shooting Guides *(the procedures for responding to critical deviations)*

Remote Isolations and emergency response

Error-reduction needs

This paper will focus on ensuring the IEs and IPLs are first identified, and then that they are correctly identified, and finally that they are properly included in the MI and reliability programs so that the Initiating Event Frequency (IEF) and PFDs of the IPLs can be relied upon. Note from Table 1 above that this goes beyond identifying the IEs and IPLs in the PHA/HAZOP and LOPA, but includes details from the same analyses, or additionally from outside of these analyses, on how to maintain each.

2 Review of Definition of IPLs

Below are the set of rules for each IPL. These rules can each be applied "qualitatively" to each candidate IPL. Note that much of this section is summarized from an earlier paper [2]. (These rules are similar to those found in Guidelines for Initiating Events and Independent Protection Layers. [3])

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 (block valves on pressure taps or level bridles), impulse lines, and bypasses. The other IPLs (or IEs) cannot share any of these components except for the mother board when using approach B for Basic Process Control System (BPCS) loops as described in the textbook on LOPA [4]).

   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.
   - 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.

2. **A control loop in the Basic Process Control System (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 pressure valve (PV), thus providing protection against the impact event.

   NOTE: Under specific conditions, a BPCS can be used up to twice in the same LOPA scenario, as described later in detail in the LOPA book [4] and IPL book [3].

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 Pressure Safety Valve (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; International Electrotechnical Commission (IEC) 61508 classification, etc.) can help ensure safeguards qualify as IPLs.

5. **The IPL and IE 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 and it must be proven that the IE has the stated IEF.**

   Each IPL and IE 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 IE and IPL that statistically supports the IEF and PFD that are used in PHA/HAZOP and LOPA. 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) within 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. (Another paper in this conference describes Human IPL validation in more detail. [7])

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 PFD value of 0.01 is not valid.

Example: When considering a Safety Integrity Level (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.

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, a Safety Instrumented Function (SIF) boundary includes the root valves, impulse lines, and any bypasses associated with the SIF.

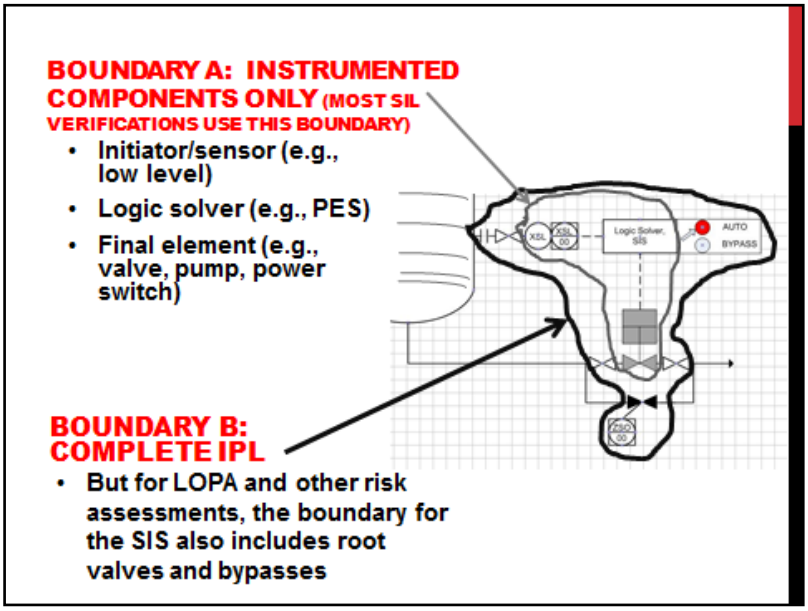

Figure 1. The True Boundary for an IPL includes all associated connections, isolations, and bypasses. Note how the traditional SIL Verification calculation boundary is much different than the true IPL boundary

3 Why each IE, in addition to each IPL, is Safety/Business Critical

Many companies neglect to extract the critical causes (initiating events, IEs) from the PHA/HAZOP tables and LOPA worksheets. But, if the frequency of the cause (i.e., IEF) increases, then the risk of the entire scenario increases. Allowing the IEF to drift upward, uncontrolled, is no different than allowing an IPL to fail as either failure increases the frequency of the consequence occurring. Therefore, it is critical to identify the IEs during

the PHA/HAZOP and any follow-on LOPA, and it is critical to include these IEs in the Inspection, Testing and Preventative Maintenance (ITPM) program to ensure the IEF is controlled as low as claimed in these risk assessments.

4 Review of How to Identify IEs and IPLs during HAZOP or during LOPA

4.1 Identifying IEs and IPLs during HAZOP

This section is an update to a prior paper [2].

The PHA team leader must understand fully the rules and definitions for IPLs and IEs and be competent in application of them. Many PHA leaders are not competent in even how to conduct a PHA; in fact, about 90% of the PHA reports that we have reviewed around the world are woefully deficient, especially with respect to finding scenarios during startup, shutdown, and online maintenance.

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.

The PHA Leader should attend a LOPA course to learn the basics of IPLs (including SIFs) as described in the previous sections, or attend a training course for PHA/HAZOP leadership that covers the definitions of IPLs and provides exercise time on how these determinations are made. In qualitative risk judgment, the key is to know when there are enough IPLs for the accident scenario under review.

The PHA/HAZOP leaders should receive 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 if there are enough IPLs for the accident scenario (risk judgment). The PHA team leader must have either participated in or led enough LOPAs of similar nature to make such judgments, or the PHA team must be able to judge when to use 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 more than 95% of the time.

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 a tolerable level (qualitatively), then add the designator " – IPL" to the right of the safeguard text. 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 supports a level alarm high (LAH) used in a Human Response IPL, in which case the sight glass will have some ITPM (such a periodic cleaning of the sight glass).

Table 2 illustrates how the IEs and IPLs (along with their likelihood values) are documented in a PHA/HAZOP report – for studies with LOPA combined within the PHA/HAZOP. The items highlighted in yellow must be included in the ITPM program.

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**	**Recs**
2.1	High level	Too much flow to one sphere from XX Plant (through their pump; about 40 bar MDH) **IEF Type: Mech** **IEF = 0.1/yr**	High pressure (see 2.5)	High level SIF with level sensors voted 2oo2, to close inlet valve **IPL Type: SIL 1** **PFD = 0.1** Overflow thru normally open pressure equalization line to other spheres **IPL Type: Process Vent** **PFD = 0.01**	
		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 **IPL Type: SIL 1** **PFD = 0.1** Overflow thru normally open pressure equalization line to other spheres **IPL Type: Process Vent** **PFD = 0.01**	
			Excessive pressure on inlet of high-pressure liquid pumps, leading to excess load on pumps and trip of pumps on high pressure, causing trips of xxx, xxx, etc. - significant operability issue	Level indication and high level alarm in DCS, used by operators to manually select which tank to fill **Type: BPCS** **PFD = 0.1**	
2.2	Low level	Failing to switch from the sphere with low level in time (based on level indication) **IEF Type: Hum** **IEF = 0.01/yr**	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)** Feeding from two spheres at all times, so unlikely for BOTH spheres to have low level at the same time **(not IPL; part of the cause)** Two level indication from SIS level transmitter, with low level alarm, with more than 60 min available to switch tanks (SIF driven alarm and response) - **possible IPL, if operator action quick enough**	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 to Plant (see 6.2)		

- IF an instrument is already in the Emergency Shut Down (ESD) system or Safety Instrumented System (SIS) and qualitatively meets the architecture of a SIL 1, 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.

4.2 Identifying IEs and IPLs during LOPA

Of course, IEs and IPLs are inherently captured in each LOPA. But these need to be documented with enough details and notes to understand any unique aspects of the IE or IPL. Below is a typical LOPA worksheet showing the IEF and IPLs with the proper level of detail for subsequent use in the MI or reliability program. The items highlighted in yellow must be included in the ITPM program.

Scenario Number: 5	**Equipment Number**: 26-1201	**Scenario Title:** Rupture of Feed Surge Drum due to reverse flow from the DHDS reactor	
Date:	**Description**	**Probability**	**Frequency (per year)**
Consequence Description / Category	*Rupture of the Feed Surge Drum due to reverse flow from 1200 psig hot liquid from the DHDS reactor. Category 5 based on likely fatality (target ≤ 10^{-4})*		
Initiating Event (Typically a Frequency)	*Spurious trip of the feed pumps due to false low level in the feed surge drum (but two false lows required)*		*10^{-1} (spurious SIF trip)*
Enabling Event or Condition	*NA*		*NA*
Independent Protection Layers			
BPCS	*BPCS action not in the correct direction; will open the minimum flow return line on low flow to DHDS*	*NA*	
Human Intervention	*Not fast enough - rupture can occur within seconds*	*NA*	
SIF	*SIL-1 closure of one safety valve that closes to prevent reverse flow, with 2oo2 low flow readings needed to cause a trip of the one XV in the main flow line*	*10^{-1}*	
Pressure relief device	*1oo2 PSVs must open – standard value since there are no blocks valves in the relief paths*	*10^{-3}*	
Other protection layers	*NA*	*NA*	
Safeguards (non-IPLs)	*2 check valves in the main line, but no ITPM on either*		
Total PFD for all IPLs		*10^{-4}*	
Frequency of Mitigated Consequence (current situation)			*10^{-5}*
Suggested Actions: *None. Risk is acceptable as is*			
Modified Frequency after Actions (final frequency):			*10^{-5}*
Comments on Residual Risk (after actions are implemented): *Risk is acceptable as is (optional action zone on risk matrix)*			

5 Extracting IEs and IPLs

How to extract the IE and IPL data from the PHA and LOPA depends on the native software used. Below are the general steps:

- For Word or Excel outputs, the IE text, IEF Type, target IEFs, IPL text, IPL type, and PFD must be manually extracted.
- For LEADER™ software (ABS Consulting) it is possible to use the standard queries for PHA analysis worksheets such as HAZOP or What-if, to extract Causes, (along with some customization of the queries using MS Access) to get all of the information for specific Initiating Events in the proper format. Extracting IPL information from the PHA analysis worksheets is straightforward using standard queries that come with the software. Regardless, these queries make extracting the Initiating Event and IPL data nearly painless.
- It is best to associate each item with the PHA deviation or the LOPA worksheet that it originates from, so that it is easy to track back to the source to get questions answered.
- It is also best to associate each item with the PFD, P&ID, and/or Operating Procedure that the IE or IPL relates to.
- Finally, for each item or action it is necessary to include a full component tag number or if a procedure step, then step number and operating procedure number, along with any associated alarm tag number or the tag of the component that the operator will manipulate.

This can be a lot of work, especially if the items (IE and IPL, and associated data) must be extracted manually from the PHA record.

6 Implementing the ITPM of each IE and IPL

Once the IEs and IPLs are extracted from the PHA/HAZOP and LOPA and included in the ITPM program, then the frequency or trigger of each ITPM task must be set. The task and frequency must be chosen, and over time perhaps adjusted, in order to achieve the stated IEF for each IE and the PFD for each IPL. The general approach is as follows:

- If the cause is an IE, then it must be inspected and maintained proactively and proven to provide the stated IEF.
- If the safeguard meets the definition of an IPL then it must be properly maintained and proven to provide the PFD claimed by the company.
- Each organization should either adopt or uniquely develop standards for the installation and care of each IE, to ensure the IEF. And each should either adopt or uniquely develop standards for the installation and care of each IPL, to ensure the PFD.

  On the following two pages are examples of standards (for ITPM) for one IE and for one IPL. These standards are similar to those found in the CCPS book on IEs and IPLs [3].

- 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 supports a 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).

IE Description: **Catastrophic pump seal failure (designed to ANSI or API) in normal operating range of temperature and pressure**
Generic IEF for Use in LOPA: **0.001/yr**
Special Consideration for Use of Generic IEF for this IE: The failure frequency may differ, depending on service and the robustness of the bearing/bearing lube system. Guidance from a pump specialist is recommended. There are multiple possible causes, and this may require additional hazard analysis techniques such as FMEA or FTA, using seal failure as a top event.
Initial Quality Assurance: API pumps receive PMI, hydrotesting, and appropriate X-ray inspection of welds based on the hazard associated with the service. Cartridge seals are leak-tested prior to installation.
Generic Validation Method: Visual surveillance (e.g., by site staff during weekly rounds) and fugitive emissions monitoring for detection of small seal leaks prior to propagation of failure to the point of a hazardous consequence. Detection of leakage of one of the seals in a double mechanical seal can be detected by online monitoring of the pressure of the barrier fluid, or the level in the tank supplying barrier fluid to the seal.
Generic Validation Frequency, Criteria, and Documentation: Varies depending on application, but typically weekly for visual inspection and monthly for fugitive emissions monitoring. Visual inspections are documented by inspection checklists. Fugitive emissions monitoring is typically conducted for environmental regulatory compliance, and documentation of testing is maintained for the life of the application, or as specified by the applicable regulation.
Site-Specific Validation Method Criteria and Documentation: Same as for Generic, but also recording and data analysis of seal failures for each type of pump, and adjustment of IEF as necessary.
Audit of Validation: For materials regulated by environmental regulation, audit frequency is dictated by compliance at a minimum. Otherwise, independent audits of documentation are recommended on a 5-year basis.
Starting Source of Guidance: API and company data.

IPL Description and Purpose: **Single** Spring-Operated Pressure Relief Valve in clean service with no history of blockage or fouling and with **no block valve upstream or downstream**

Generic PFD for Use in LOPA: **0.01** for failure to open enough at set pressure (100% of rating), if inspected and tested every 4 yrs or less. Note: Use this number if your organization requires you to control overpressure to Code limits (e.g., 10% accumulation over MAWP). Note: If interval between inspections is greater than 4 years, then the case is beyond Basic LOPA.

If there is an isolation valve (block valve) upstream or downstream of the relief device, then the PFD is taken as 0.1, unless the site has auditable documentation that demonstrates the probability of a human leaving a block valve inadvertently closed is much less than 1 chance in 100.

Special Consideration for Use of Generic PFD for this IPL: The PSV is confirmed to be sized for the scenario being considered, and the datasheet to prove this is available on demand. The inlet and outlet piping are sized correctly and mechanically adequate for relief flow. There is no block valve upstream or downstream of the PSV (except for the allowable case of a 3-way valve **either** upstream or downstream but not both when an online spare relief valve is provided, and that cannot impede flow irrespective of position, **or** mechanically linked 3-way valves upstream and downstream of the in-service and online standby relief valves, **or** use of captive-key system on valves that ensures one relief path is always open).

The relief valve is in clean service. Service does not have the potential for freezing of the process fluid before or during relief; if freezing is possible, then adequate heat tracing (of the relief valve and piping) is installed and maintained, with inspection for performance for heat tracing at the start of each cold season or every 3 months when in cold environments.

Note: Use of multiple relief devices, each sized for a portion of the required relief flow, opening at different set points, requires more rigorous likelihood [probability] techniques such as FTA to account for common-cause errors leading to a lower reliability of the combined set of PSVs.

Generic Validation Method: Relief valve to undergo periodic removal and pop testing by certified person (in the USA, normally a state certified inspector is required). Inspection to include inlet and discharge piping to ensure they are free and clear, as well as checking for any evidence of corrosion that would impede proper functioning prior to the next validation check/test. The pressure at initial opening is recorded. Internal inspection is performed to detect onset of failure (corrosion, damaged internals, fouling/plugging). Relief valve returned to like-new condition prior to return to service.

Generic Validation Frequency, Criteria, and Documentation: Inspection frequency is every 4 years or less. Chemical and Petrochemical industries (ICI, Olin, etc.,) use frequencies of 1-2 years. 2-3 years appears most common in literature. Inspection shows no history of blockage or corrosion and no onset of blockage. API RP-576 and NFPA standards allow up to 5 years between inspections, but current industry data does not support a PFD of 0.01 at inspection periods greater than 4 years. Inspections and tests are documented for each device and for the life of the process. Credentials of the inspector and test entity are noted.

Site-Specific Validation Method Criteria and Documentation: In addition to the Generic approach, testing shows that each pressure relief valve opens at no more than 21% above set pressure, with less than 0.5% failure rate. Test results and data analysis of failures are kept for the life of the process.

Basis for PFD and for Generic and Site-Specific Data and Validation Methods and Frequency:
Based in general on CCPS "Guidelines for Pressure Relief and Effluent Handling Systems," Chapter 2, and recent published data (Bukowski, 2009, etc.[7])

7 Auditing Protocol to Ensure Proper Care of each IE and IPL

An organization that ensures that PHAs meet the needs of all users within the company is one that understands how to control process safety. PII tests for this linkage during PSM audits. One way we do this is to extract several dozen causes and safeguards (those that either are or appear to be IPLs) and then check to see if these are in the list of Safety Critical Elements (SCE) and check to make sure that the site is inspecting, testing, and maintaining each of these components. If not, then the site has a gap or perhaps the site fails to understand the relationship between the PHA and the rest of process safety.

- Review each PHA, identifying at least 3 separate High Consequence Severity scenarios. (Note: These may not be high risk scenarios after the safeguards have been applied; the intent of this step is to identify high consequence severity scenarios before any safeguards are considered.)
- Choose a mixture of causes and safeguards associated with these High Consequence Scenarios. When selection is complete, there should be approximately 5 causes and 10 safeguards for each PHA. There should be a good mix of mechanical and operator response items.
- Repeat this selection process for each PHA at the site. For example: if there are 5 PHAs then there should be approximately 70-80 items (5x15=75) to track down (approximately 50 MI and 25 OP RESPONSE).
- DO NOT list all of these at once; instead begin with an initial list of 45 (from 3 PHAs) and begin tracking those down to develop a workable process for researching causes and safeguards.
- For equipment-based (MI) items, go to the respective ITPM system and ensure the items are included, are being inspected, tested and the required preventative maintenance is being done and on the right approximate frequency, and the last scheduled ITPM matched the assigned frequency. If possible, identify the basis and rationale for determining the frequency for inspections and tests.
- For human action-based items, and if triggered by an alarm (so if it says "xx alarm in PIxxx" in the safeguard column of the HAZOP or What-If tables, that is what this means), then do the same tracking as above for the ITPM, but also use the following as an example of what to track down on "response to critical alarms":
  - How does an operator know a process deviation has occurred?
  - Are the required operator actions in response to an alarm clear and documented? If so, where?

Items for Horizontal Audit of MI & OP Response (IEs and IPLs) extracted from PHA report

Project: Client:	PSM Audit – ABC Chemical Company	Lead Auditor:	Joe Auditor
Elements:	PHA→ MI → OP → TNG	Date:	09/21/2019
PHA Base Document:	PHA of PBA	Date PHA was Completed:	8/2017

Node: Description:		2.3 Reverse flow	Consequence: Severity Rating	S C2
Cause or Safeguard?		Description	Mechanical or Human?	How maintained? Evidence? (ITPM/Schedule or OP/TRG/HF)
1	C (IE)	Loss of mother liquor flow 1. Pump Failure causing loss of line pressure leading to reverse flow	Mech	
2	SG (IPL)	Double check valve on the ML line	Mech	
3	SG (IPL)	Human action to respond to close the acetone feed valves (for case of loss of acetone)	Human	
4	C (IE)	Loss of flow of acetone 1. Pump Failure causing loss of line pressure leading to reverse flow	Mech	

Node: Description:		4.5 High pressure in dehydration column	Consequence: Severity Rating	S C2
Cause or Safeguard?		Description	Mechanical or Human?	How maintained? Evidence? (ITPM/Schedule or OP/TRG/HF)
1	C (IE)	Vacuum pump (to prevent failure)	Mech	
2	SG (IPL)	PSVs 531012 A/B/C (credited for 10-2)	Mech	
3	SG (IPL)	Operator response to PAH, 531PIC002A	Human	
4	C (IE)	Heat exchanger tubes: E-53102 & 53103	Mech	

- What is the Process Safety Time (PST, see definition in LOPA text [4]) for that scenario? This sets the time limit for the operator response; the operator response is actually a "portion" of that PST. Is adequate time available to perform the actions required? Note: 10-20 minutes is the minimum PST for a field-based action; 5 minutes for a control room action. However, individual site or company data trumps these minimums.
- Are drills and/or simulations performed on that alarm trigger each year by each operator in that specific unit? (This is not an industry standard, at least not yet; just ask for now how they ensure the operator can indeed respond in time.)
- Is there a record of these drills and the time it took to fully respond?
- How would an operator know they have made a mistake or that a component has failed?

- What feedback does the process give?
- Does the operator have the right information at the right time to respond to the process upset/ or to recover from the mistake?
- Can the operator hear/see it in the field, and/or in the control room?

This will evaluate part of the PHA as well as part of the MI and OP elements: Are the PHA results being used to prioritize the ITPM activities and are the safeguards listed really being maintained, or are they not?

8 Closing

Doing risk assessments such as PHA/HAZOP and LOPA is worthless unless the identified IEs and IPLs truly provide the risk reduction stated. Industry knows how to maintain these critical features and actions. Proven approaches now exist for extracting the IE and IPL data from PHA/HAZOP and LOPA studies and for ensuring these items are included in the ITPM program and other management systems.

9 References

References Cited

[1] W.G. Bridges, J. Thomas, P. Casarez, "The Uses and Users of PHA/HAZOP Results", 14th Global Congress on Process Safety, Orlando, FL, April 22-25, 2018, American Institute of Chemical Engineers.

[2] W.G. Bridges and A. Dowell, "Identify SIF and Specify Necessary SIL, and other IPLs, as part of PHA/HAZOP", 12th Global Congress on Process Safety, Houston, TX, April 10-13, 2016, American Institute of Chemical Engineers.

[3] CCPS, *Guidelines for Initiating Events and Independent Protection Layers*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2015.

[4] CCPS, *Layer of Protection Analysis: Simplified Process Risk Assessment*, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, NY, 2001.

[5] Homoud Al-Maymouni, Yunzhong Gao (both from SS-TPC), and W. Bridges, "Implementation of Process Hazard Analysis at SINOPEC-SABIC Tianjin Petrochemical Company Ltd, China**",** *11th Global Congress on Process Safety*, Austin, TX, AIChE, April 2015.

[6] J.V. Bukowski and W.M. Goble, Villanova University, *Analysis of Pressure Relief Valve Proof Test Data*, Process Safety Progress, American Institute of Chemical Engineers, March 2009.

[7] W.G. Bridges and W. Chastain, *People as Safeguards – When are Human IPLs Valid, and How are their PFDs Assured in Practice*, 16th Global Congress on Process Safety, Houston, TX, March 30 - April 1, 2020, American Institute of Chemical Engineers.

Additional Reference

[8] A.M. Dowell, III, "Understanding IPL Boundaries", Process Safety Progress, March 2018. (Originally prepared for presentation at the American Institute of Chemical Engineers 2018 Spring Meeting, 14th Global Congress on Process Safety, Orlando, Florida, April 23–25, 2018).