Understanding IPL Boundaries

A.M. (Art) Dowell, III
Principal Engineer
Process Improvement Institute, Inc.
16430 Locke Haven Dr.
Houston, TX 77059 USA
adowell@piii.com

Prepared for Presentation at
American Institute of Chemical Engineers
2018 Spring Meeting and 14th Global Congress on Process Safety
Orlando, Florida
April 22 – 25, 2018

Understanding IPL Boundaries

A.M. (Art) Dowell, III
Principal Engineer
Process Improvement Institute, Inc.
16430 Locke Haven Dr.
Houston, TX 77059 USA
adowell@piii.com

Keywords: LOPA, IPLs, boundaries, relief valve, dike, alarm, deflagration arrester

Abstract

Layer of protection analysis (LOPA) is a simplified risk assessment tool that has been in use for almost three decades. The technique has improved the focus on independent protection layers (IPLs) that can prevent the progression of an initiating cause to an undesired consequence (a scenario). An IPL must be capable of preventing the scenario from reaching the consequence. To execute the simplified LOPA approach, the IPL must be independent of the initiating cause and other IPLs.

A potential pitfall in LOPA and in the management of IPLs identified in LOPA is misunderstanding the boundary of the IPL.

For example, a pressure relief valve is intended as an IPL to prevent the consequence of catastrophic rupture of the vessel with potential for fatality. In reality, for the pressure relief valve to prevent vessel rupture, the inlet piping from the vessel to the relief valve and the outlet piping from the relief valve to the ultimate destination must provide sufficient flow capability. The IPL boundary must include any block valves in the inlet and outlet piping, and any devices such as flame arrestors or back pressure controllers. The PFD (probability of failure on demand) must include everything in the expanded IPL boundary.

If the IPL boundaries are not correctly understood, the LOPA is not correct and the organization is deluding itself on the risk reduction.

The paper provides examples and illustrations for several types of IPLs: safety instrumented functions, dikes, relief device with fire-resistant insulation and cladding on the vessel, operator response to alarm, and deflagration arrester. The paper includes diagrams to illustrate the concepts.

1 Introduction

In the early 1990s, layer of protection analysis was developed as a simplified risk assessment tool [1]. A LOPA scenario consists of a single cause leading to a single consequence with IPLs (independent protection layers) that can prevent the scenario from reaching the consequence. To execute the simplified LOPA approach, the IPL must be independent of the initiating cause and other IPLs. Therefore, knowing the boundary of the IPL is fundamental to applying LOPA correctly.

IPLs must be capable of detecting the onset of a scenario and must be capable of making a decision (change their state) to take action that is capable of deflecting or preventing the consequence. A memory aid to this rule is that an IPL must "Detect, Decide, Deflect" (even an analog device must decide). (Note that an exception to the Detect and Decide requirements is a dike or other passive IPLs.)

IPLs must also be Big Enough, Strong Enough, Fast Enough, and Smart Enough to prevent the consequence.

Of these issues, perhaps the largest potential pitfall in LOPA and in the management of IPLs identified in LOPA is misunderstanding the boundary of the IPL [2]. The IPL boundary is defined by the answers to these questions:

- Exactly what equipment and human actions are part of an IPL?
- What has to happen from the process-wetted-surface of the detection part of the IPL through the decision-making part of the IPL to the process-wetted-surface of the deflection part of the IPL?

If equipment and human actions are omitted from the IPL boundary, then the PFD calculated for the IPL may be much more optimistic than the PFD that takes consideration of all the elements. Omitted equipment and human actions may not be appropriately designed, tested, verified, validated, or maintained, thereby increasing the risk of the process.

This paper examines these issues for several example IPLs.

2 Understanding IPL boundaries

For each example IPL, there will be a brief description of the IPL. Then a narrow (incorrect) IPL boundary will be discussed. Finally, an expanded (correct) IPL boundary will be demonstrated.

1. Safety instrumented function (SIF)

2.1.1 SIF IPL description

Figure 1 shows a typical safety instrumented function. In this example, the SIF is intended to detect low level in the vessel and to close the outlet valve from the vessel to prevent the high-pressure gas blow-by scenario that overpressures the downstream equipment.

2.1.2 Narrow (incorrect) IPL boundary

Many times, the SIF is visualized as a transmitter input loop to a safety logic solver to an output loop with a block valve. Per IEC 61511 (ISA 84) guidance, the SIL (safety integrity level) verification considers only the transmitter, the logic solver, and the safety valve with its actuator and solenoid valve [3]. IEC 61511 consciously omitted the probability of human error from the PFD calculation of a SIF, including the probability of leaving an SIF in bypass [4]. The calculated PFD is used in the LOPA calculation as a measure of the risk reduction provided by the SIF.

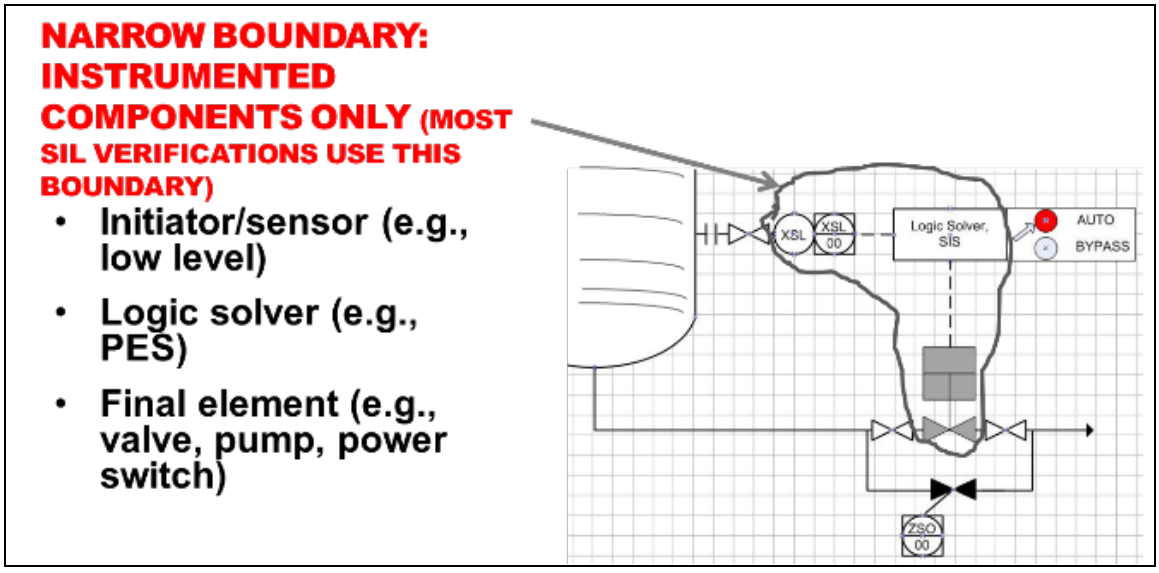

Figure 1: Narrow boundary, instrumented components only
Courtesy Process Improvement Institute, Inc., All Rights Reserved

The problem is that the SIF cannot detect the process upset if the root valve for the transmitter is closed or if the nozzle to the vessel is plugged. The SIF logic solver cannot decide to close the block valve if the auto-bypass switch is in the bypass position. The SIF cannot prevent the gas blow-by consequence if the bypass valve around the safety valve is open.

2.1.3 Expanded (correct) IPL boundary

The issues that can impede the SIF from preventing the consequence should be included in the calculation of the risk reduction from the IPL. Figure 2 shows the expanded IPL boundary, including the vessel nozzle, the transmitter root valve, the auto-bypass switch,

and the block valves and the bypass around the safety valve. Of prime importance, the human actions (and probability of error in these actions) of manipulating the root valve, the auto-bypass switch, and the bypass valve should also be included in the calculation of the risk reduction.

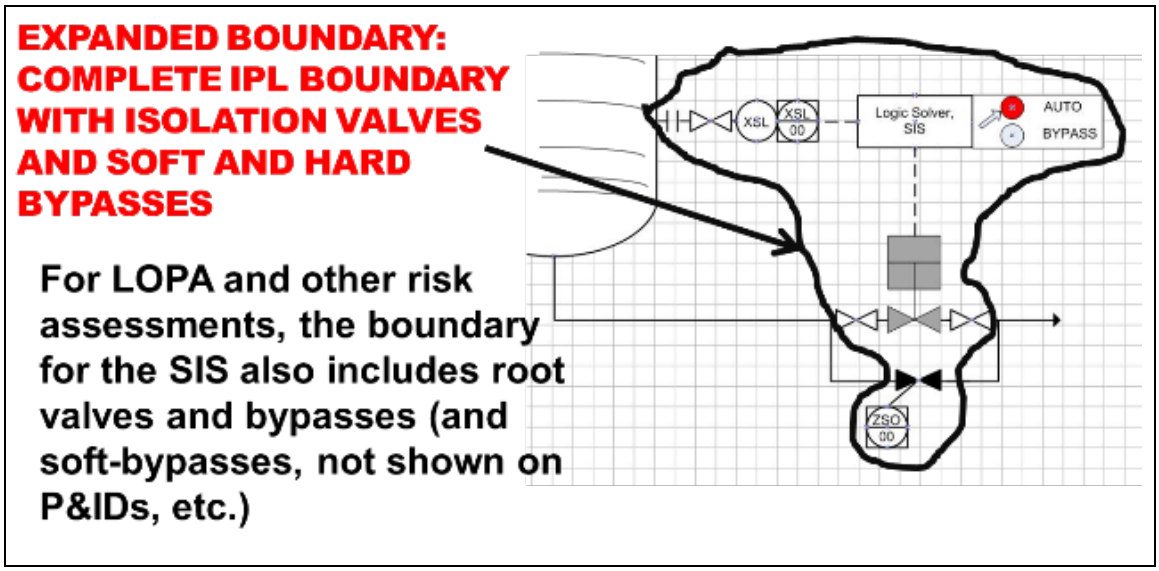

Figure 2: Expanded boundary B, including root valves and bypasses

For the transmitter root valve, the considerations are how often the root valve would be closed for repair, or calibration and testing of the transmitter, the procedures for double checking that the root valve is open, and the ability to detect that the root valve is closed. For example, the process variable from the transmitter could be compared procedurally to other level transmitters with the same range, or a deviation alarm for the level transmitters could be annunciated. The probability of failure on demand for the operator response to the deviation alarm must also be considered.

The PFD for the IPL with the expanded boundaries (Eq. 1) can be significantly higher than that calculated for the narrow boundaries (Eq. 2) [5].

$$\textbf{Eq. 1}\ PFD_{SIF} = PFD_{XSL} + PFD_{LS} + PFD_{SD\_Valve} + \left(PFD_{Root\_Valve} + PFD_{Bypass\_Valve} + PFD_{Auto/Manual}\right)_{Human\_Error}$$

$$\textbf{Eq. 2}\ PFD_{SIF} = PFD_{XSL} + PFD_{LS} + PFD_{SD\_Valve}\ \textbf{INCOMPLETE!}$$

From our experience around the world, very few existing SIL 2 and SIL 3 SIFs can be expected to provide any more than SIL 1 protection, because the human errors listed above are not addressed in the design and maintenance for these SIFs.

2. Dike

2.2.1. Dike IPL description

A typical dike is designed to prevent the spread of a liquid release throughout the facility by confining it to a relatively small area. The dike may be typically sized for 110% of the size of the largest vessel in the dike. Note that the dike does not prevent the spread of vapor; the secondary consequence of vapor dispersion through the facility must be evaluated for its severity. Nor does the dike protect against a wave whose height exceeds the height of the dike wall.

Suppose the scenario is a release from one tank due to a leak (such as a drain valve left open). If the dike is sized correctly, it can prevent liquid release to the facility. Figure 3 shows an appropriate IPL boundary for this scenario.

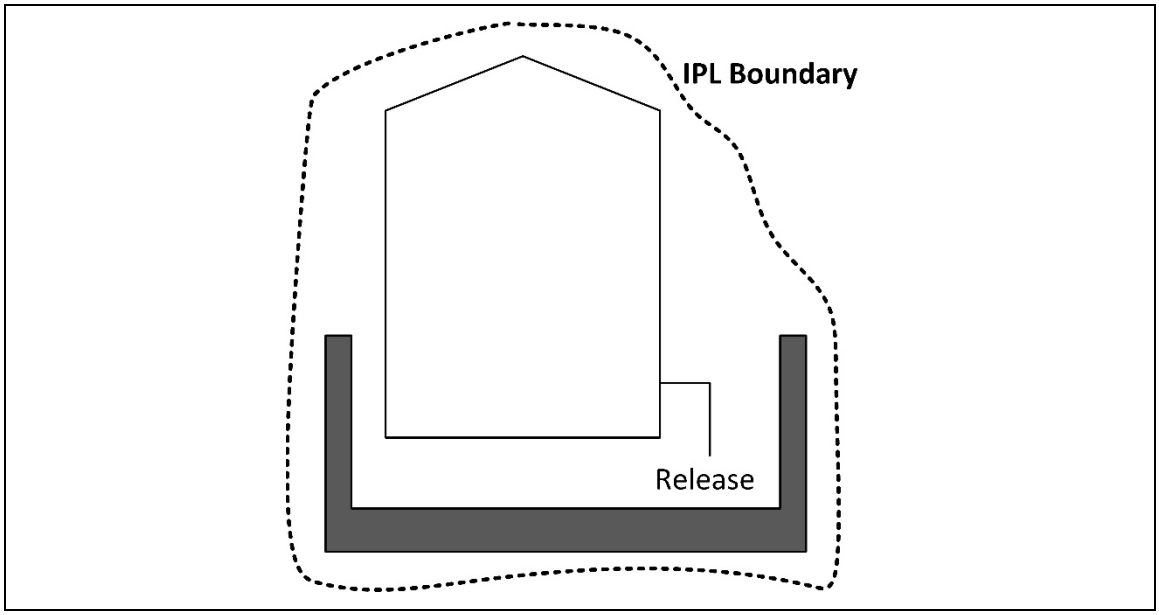

Figure 3: Leak from one tank in the dike; no flow into tank

2.2.2. Narrow (incorrect) IPL boundary

If the initiating cause is, for example, failure of the tank level control loop, then continuing flow from the pipeline supplying the tank (not shown in Figure 3) could easily lead to an overflow from the tank into the dike. The dike can only prevent liquid release into the facility until it fills up. In many LOPAs, the analyst simply writes “IPL: Dike, sized for 1.x * tank volume” (Figure 4, narrow IPL boundary).

In order for the dike to be an effective IPL, the overflow must be detected and the pipeline flow must be stopped before the dike overflows. The analyst made an implicit undocumented assumption that the release into the dike would be detected by some means and the source flow into the tank would be stopped before the dike overflowed. (Or perhaps the analyst knows the source tank will run dry before the dike overflows.) What is the

mechanism to detect and stop the flow before dike overflow? Is there instrumentation (flammable gas detector, level detector in the dike) with operator response to alarm? Will operator rounds detect the flow into the dike in time? In the middle of the night? In a snowstorm? When the ambient temperature is -40° F (-40° C)? If someone sees the overflow, how is the flow stopped?

2.2.3. Expanded (correct) IPL boundary

For this scenario, (if the source tank has enough volume to overflow both the tank and the dike), the IPL boundary must include the dike itself, AND the detection of flow into the dike, AND the action to stop the flow into the tank. The probability of failure on demand for detecting the flow into the dike and stopping the flow into the tank must be added to the PFD for the dike itself. The periodic inspection and testing of the dike must include verification and testing of the system to detect flow into the dike and to stop flow into the tank. Figure 4 displays both the narrow IPL boundary and the appropriate expanded IPL boundary.

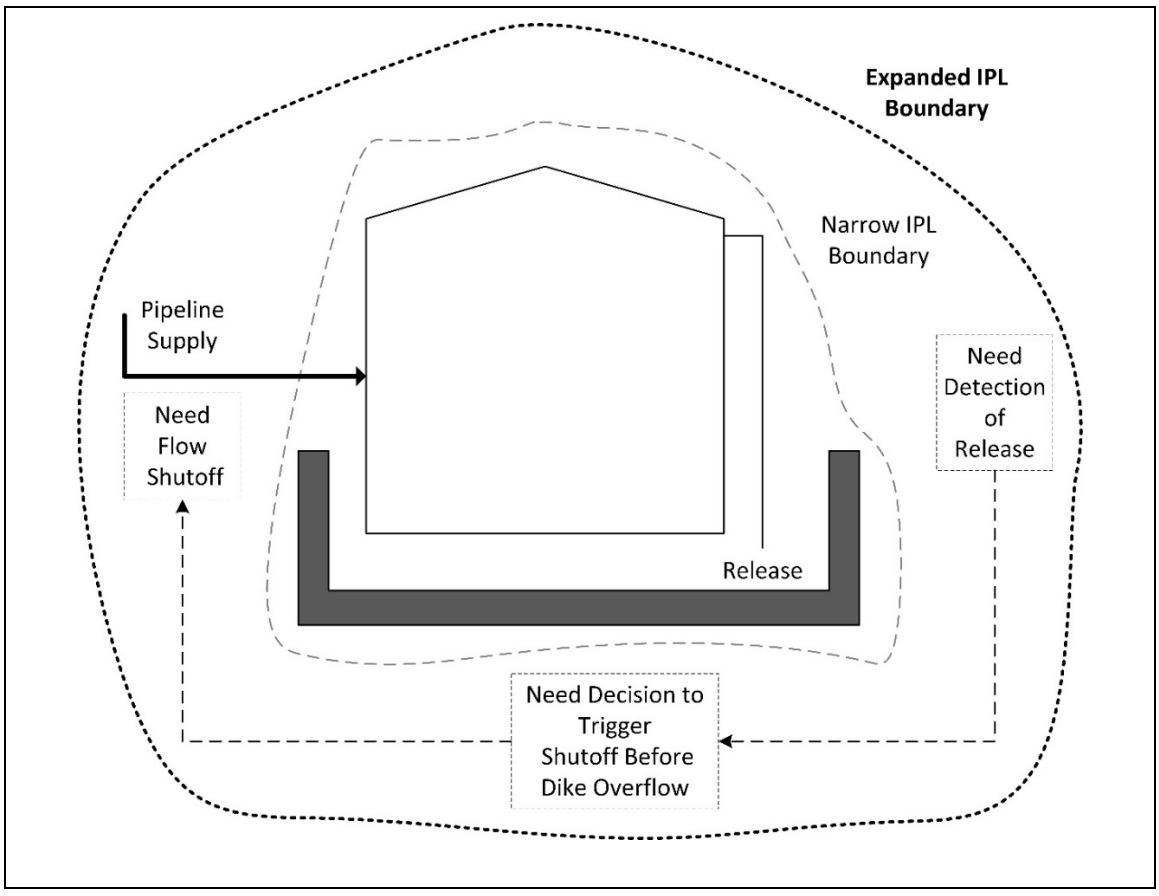

Figure 4: Dike as IPL, narrow and expanded IPL boundaries to prevent overflow while filling tank

For a continuous flow into the dike, the IPL boundary must be expanded to include detection of liquid in the dike and action to stop the flow. The LOPA cannot assume that a random passerby will see the liquid in the dike, alert the operators, and the operators will stop the flow before the dike overflows. This consideration increases the complexity of determining the PFD for the dike.

Another issue with release into the dike is that a corrosive fluid can attack the wall of the dike. The author is aware of a loss of containment where the dike wall began to leak from reaction with the released fluid. The hazmat responders used a baseball bat to plug the dike wall leak until the release into the dike could be stopped and the contents could be removed from the dike. Note that the exposed external bolts for piping and tank flanges, as well as the tank hold down bolts, are usually not designed for the corrosivity of the process fluid because the designers don't expect them to be exposed to the process fluid.

For the scenario of corrosive fluid release into the dike, the IPL boundary must be expanded to include the detection of the release and removal of the corrosive fluid before corrosion to the exposed bolts causes more loss of containment; otherwise the dike cannot be an IPL because it will not survive the scenario.

3. Pressure relief valve

2.3.1. Pressure relief valve IPL description

LOPA might identify a pressure relief valve (PRV) as an IPL to prevent the consequence of catastrophic rupture of the vessel with potential for fatality.

2.3.2. Narrow (incorrect) IPL boundary

The temptation is for the analyst to enter the nominal PFD for the PRV itself from the lookup table, thus, assuming the flow path looks like Figure 5. (The widely-used PFD is 1E-2, but it is incorrect for the configuration in Figure 5).

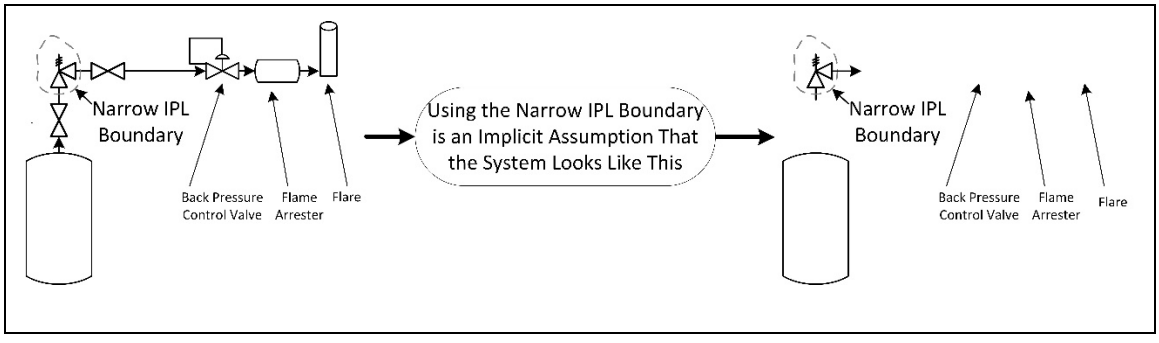

Figure 5: Results of the narrow IPL boundary

2.2.3. Expanded (correct) IPL boundary

In reality, for the pressure relief valve to prevent vessel rupture, the inlet piping from the vessel to the relief valve and the outlet piping from the relief valve to the ultimate destination must provide sufficient flow capability (Figure 6). For the initial design, the relief calculations must include the pressure drop in the inlet and outlet piping (including block valves) and any other devices (such as the flame arrestor) in the flow path.

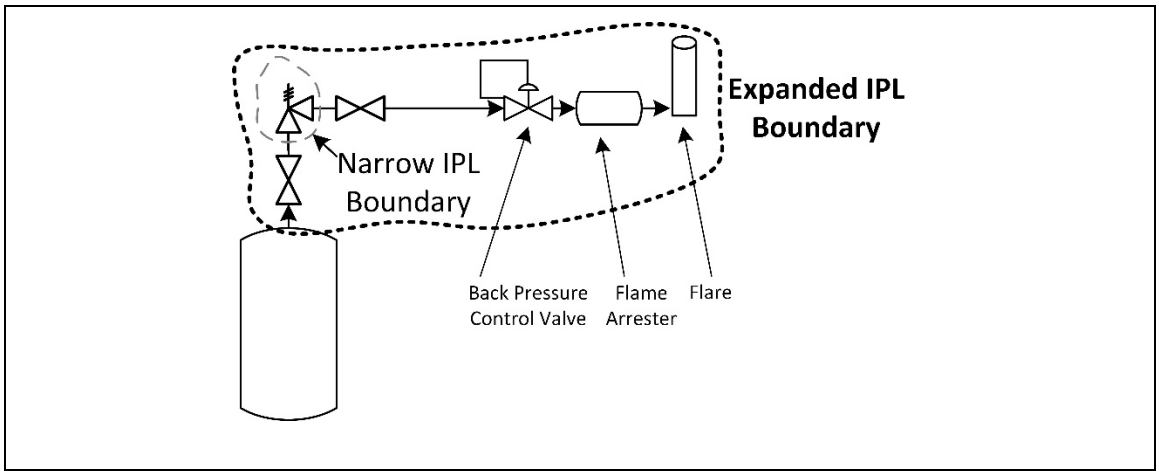

Figure 6: PRV with narrow and expanded IPL boundaries

During the operational phase of the lifecycle, the inspection and testing of the relief valve IPL must include inspection of the inlet and outlet piping, including any devices such as flame arrestors, knockout pots, or back pressure controllers. This inspection and testing is in addition to the inspection and testing of the relief valve itself. Moreover, the management system for any block valves in the inlet or outlet must be evaluated and audited to confirm that the relief path is not compromised by human error that blocks the path.

Again, the actual PFD for the PRV IPL equals the PRV PFD plus the human error PFD for the compromised relief path plus the PFD for the other devices (Eq. 3**Error! Reference source not found.**). Calculation of the human error PFD would take into account the frequency of closing block valves, and the procedures and cross checks for restoring a relief path to service.

$$\textbf{Eq. 3} \quad PFD_{IPL} = PFD_{PRV} + PFD_{Human\ Error} + \sum PFD_{Other\ devices}$$

Periodic audits of block valves around PRVs is an important function to understand the average PFD for the facilities PRV block valves, but an effective crosscheck must be performed immediately when PRV block valves are repositioned. The facility cannot wait days, weeks, or months until the next audit to confirm that the block valves are correctly positioned. Human error PFD may dominate or overwhelm the PRV PFD. In some cases, features must be installed to prevent or compensate for the human error, such as limit

switches or captive key (trapped key) valves, so that non-human means are used to assure the position of the isolation valves.

4. Relief device with fire-resistant insulation and cladding on the vessel

2.4.1. IPL description

ANSI/API standards for PRV sizing allow reducing the PRV sizing for a vessel that has fire resistant insulation and cladding [6]. The fire-resistant insulation and cladding is sufficient to prevent the vessel from boiling for the **duration of the fire**.

2.4.2. Narrow (incorrect) IPL boundary

Over time, the facility can easily forget that the fire-resistant insulation and cladding is part of the fire case relief design basis. They assume that the IPL boundary is just the relief device and forget to take care of the fire-resistant insulation and cladding.

2.4.3. Expanded (correct) IPL boundary

The IPL boundary must now be expanded to include the fire-resistant insulation and cladding sufficient to prevent boiling for the duration of the fire. If the insulation is damaged, the relief system has now been compromised and the facility must evaluate the relief scenarios for the vessel and provide an alternate means of protection.

If the quantity of available fuel for a fire increases near the vessel, then the relief design must be reevaluated.

Since it may be easy to inadvertently compromise the relief for a vessel or system, it is recommended to note on the P&ID (piping and instrumentation diagram) that the fire-resistant insulation is part of the fire case relief design.

5. Operator response to alarm using a manual valve

2.5.1. Operator response to alarm using a manual valve description

An appropriately designed IPL using an alarm depends upon an operator to decide to respond to the alarm and to take action, such as closing a manual valve that prevents the consequence from occurring.

2.5.2. Narrow (incorrect) IPL boundary

When the author began his observation of HAZOP and PHA reports in 1978, the HAZOP safeguard might be listed as “PAHH-702”. (Figure 7A represents the nominal boundary for the candidate IPL, ignoring the root valve and the deflection parts of the IPL). As the industry began to implement LOPA, it was quickly recognized that “PAHH-702” only described the detection and alarm annunciation for the safeguard. Recalling the memory aid for IPLs, the IPL should be able to detect, decide, and deflect. For the safeguard to be

an IPL, an operator must decide to take action and then execute the action to deflect the consequence.

2.5.3. Expanded (correct) IPL boundary

The safeguard should really be written as "Operator response to PAHH-702 to close manual valve 703 in the vessel feed line" (Figure 7B depicts the actual boundaries for an effective IPL).

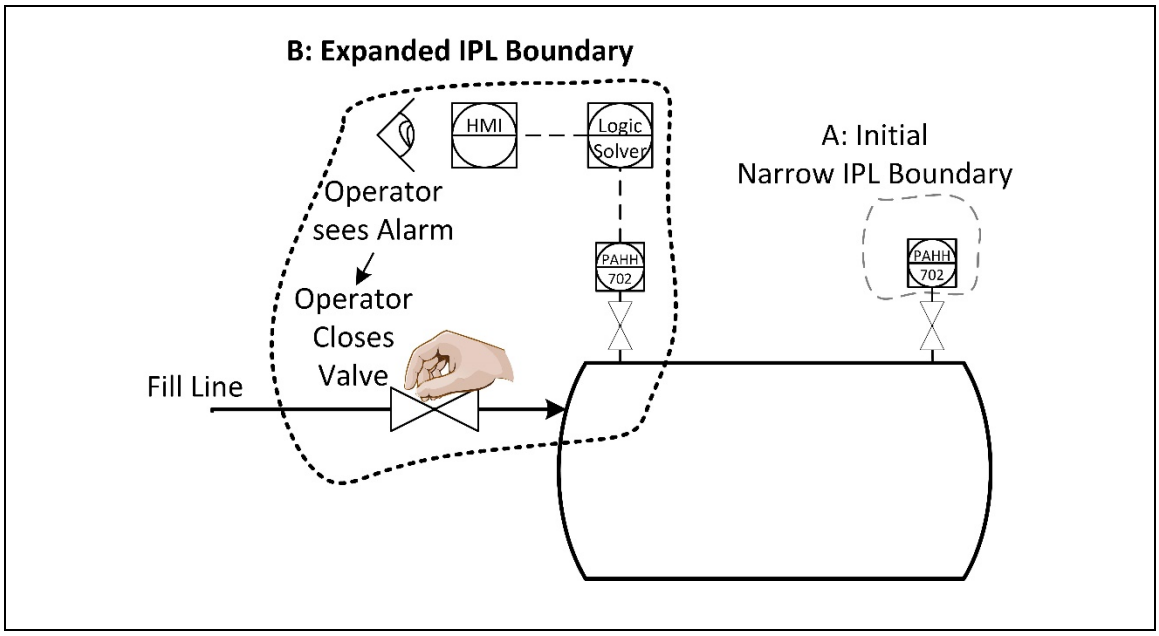

Figure 7: Operator response to alarm IPL, narrow and expanded boundaries

Why is it important to have the correct boundaries for an operator response to alarm IPL? If a truncated boundary is used, the lifecycle requirements for the complete IPL may be overlooked. Design, verification, validation testing, training, drills, may be incomplete.

Today, LOPA practitioners still frequently see safeguards written as "PAHH-702". When they attempt to do the LOPA, they have to search for the documentation for the PAHH (a cause and effect matrix would be helpful, if the deflection action is automated). Since deflection for the PAHH is operator response, they have to search for documentation that a procedure exists for the operator response to the PAHH. They have to find the SIL validation test results for the PAHH and they have to find the training and drilling records for the operator response.

Since the IPL uses a human response, the IPL boundaries must include every human who might reasonably be expected to need to perform the response. For a four-shift operation, the appropriate operator on each shift must be trained and must participate in periodic drills. But wait, people are sometimes absent for sickness, for vacation, for training, etc. The

facility must ensure that the substitute personnel are trained and drilled as well as the regular personnel. The vacation relief operator, the department relief operator, the step-up operator, or step-up supervisor must all be included in the training/drilling effort and this effort must be documented and audited.

When a LOPA analyst looks at the expanded boundaries for the operator response to alarm IPL, it is critical to recognize that the manual valve or other manual action must be inspected and tested periodically. When was the last time the manual block valve was operated? Is a handle available for the manual block valve? Is a valve wrench or cheater bar needed to close or open the valve? When was the manual block valve last lubricated? Is the manual block valve still accessible? Is the valve chained in the running position? Has a tree branch grown through the valve wheel?

It should also be recognized that the alarm portion of the operator response to alarm requires instrument power to annunciate the alarm. While most SIFs are designed to fail to the safe state on loss of utility (such as instrument air and instrument power), power is always needed for the alarm annunciation. Consideration should be given to redundant power supplies and sufficient battery backup time so that the alarm can be annunciated when required.

6. Complex alarm annunciation with human response

2.6.1. Complex alarm annunciation with human action IPL description

Suppose a facility has extended down time where the unit operations people are not at work 24/7 (for example, weekends, holidays, inventory control shutdowns). There are alarms, say, for high tank level that might require response before the scheduled return time for the unit operators. The facility observed that the boiler house is always staffed. The facility hardwired the tank high level transmitter to a logic solver at the boiler house. If the high-level alarm occurs, the boiler operators have a procedure to telephone or radio the unit operator to troubleshoot and take preventive action. If the unit operator is not available (during the extended down time), then the boiler operator notifies the emergency response team to investigate and take preventive action. The LOPA analyst wonders if this system can be an IPL. If yes, then what is the PFD?

2.6.2. Narrow (incorrect) IPL boundary

The intended IPL could easily be described as “LAHH-201” as discussed in the previous section.

2.6.3. Expanded (correct) IPL boundary

Applying the thought process from the previous section, the candidate IPL might be described as “Tank 201 LT-201-02 hardwired to BH-3 logic solver, LAHH-201, with boiler operator response to radio a message to the unit operator, (or the emergency response team) to investigate and close block valves A, B, and C in the fill lines to Tank 201” (Figure 8).

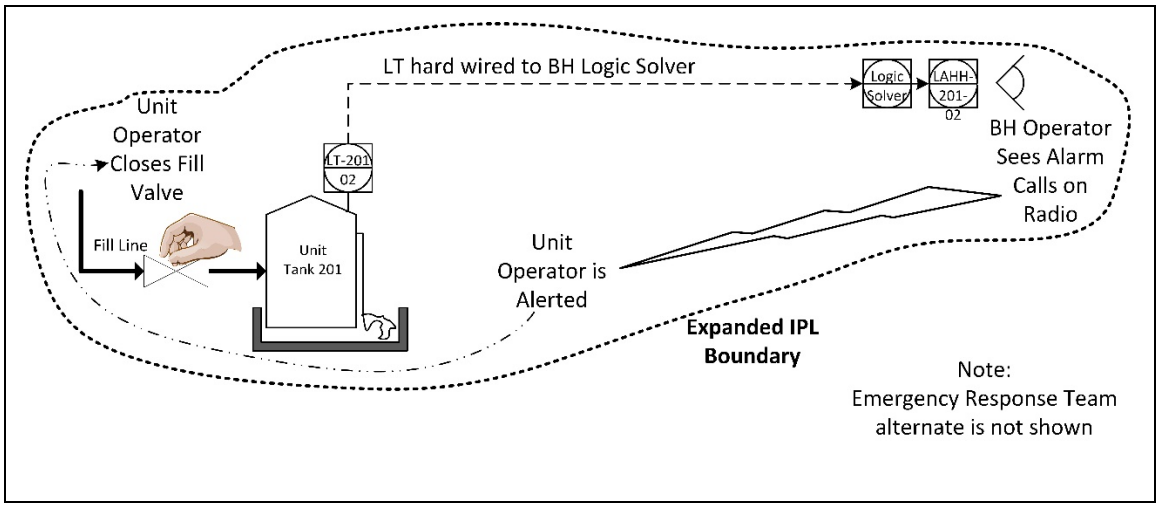

Figure 8: Complex alarm annunciation with human response, expanded boundary

As described in the previous section, the facility should provide lifecycle validation and testing for all the hardware from the level transmitter, through the loop wires, through the logic solver, and through the annunciation HMI (human machine interface). Training and drilling are required for the boiler operator. Maintenance and testing are required for the radio alert from the warehouse to the unit operator. Training and drilling are required for the unit operator response and for the response of the emergency response team personnel. Preventive maintenance and testing are required for all communication gear.

The challenge is to calculate the PFD for the candidate IPL. The calculation is more complex than simply reading a value from a lookup table for generic operator response to alarm PFD. The calculation should include:

- PFD for Tank 201 LT-201-02 hardwired to BH-3 logic solver, LAH-201 – this equipment is the hardware for the instrumented portion of the candidate IPL.
- PFD Boiler operator response to alarm.
- PFD for the radio link between the boiler operator and the unit operator (or emergency response team).
- PFD for the unit operator response to close the block valves A, B, and C in the fill lines to Tank 201.
- PFD for the block valves A, B, and C in the fill lines to Tank 201.

In some implementations of a scheme like this, the tank level and its associated alarms may not be displayed on the HMI in the unit control room because of the complexity of communicating the level transmitter process variable to multiple locations. For faster response of the unit operators when they are available, the tank level and associated alarms should be annunciated on the unit control room HMI. The detailed design for a robust implementation of process variables and alarms into rogue remote locations can be

engineered with careful attention to eliminating single failure modes to danger, but the design is beyond the scope of this paper.

The analysis is more complex if the signal from the level transmitter is sent over ethernet to the boiler house logic solver.

7. Deflagration arrester

2.7.1. Deflagration arrester IPL description

A properly designed deflagration arrester can be an effective IPL against propagation of a flame through a piping system.

2.7.2. Narrow (incorrect) IPL boundary

However, if the flow of flammable gas continues, the flame will eventually heat up the elements of the arrester and the deflagration will pass through the arrester (Figure 9). Note that the IPL boundary excludes the part of the detonation arrester where the fire is burning on the elements surface.

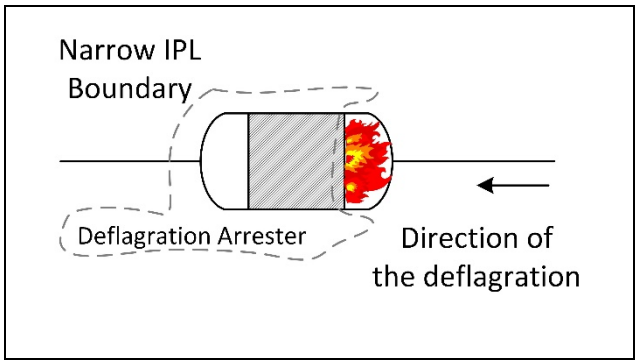

Figure 9: Deflagration arrester with narrow IPL boundary

2.7.3. Expanded (correct) IPL boundary

If a continued flow of flammable gases is possible, the detonation arrester design must include temperature sensors and response to high temperature to stop the flow of flammable gas. Some systems inject “snuffing” steam to move the composition out of the flammable region. The IPL boundaries must be expanded to include the temperature monitoring (TAHH), and the associated flow shut-down or snuffing steam injection. The expanded IPL boundary in Figure 10 includes recognition of continued flammable gas flow and recognition of the burn-through hazard. This knowledge leads to the addition of the TAHH and shutdown valve.

When the expanded IPL boundaries are considered, the facility should recognize that lifecycle design, verification, validation, and testing requirements apply not only to the detonation arrester itself, but to the temperature monitoring and the TAHH response

equipment (and personnel, if the shutdown or snuffing steam is activated by an operator). If the temperature monitoring and TAHH response is not available when there is a continuous flow of flammable gas, the detonation arrester cannot be effective.

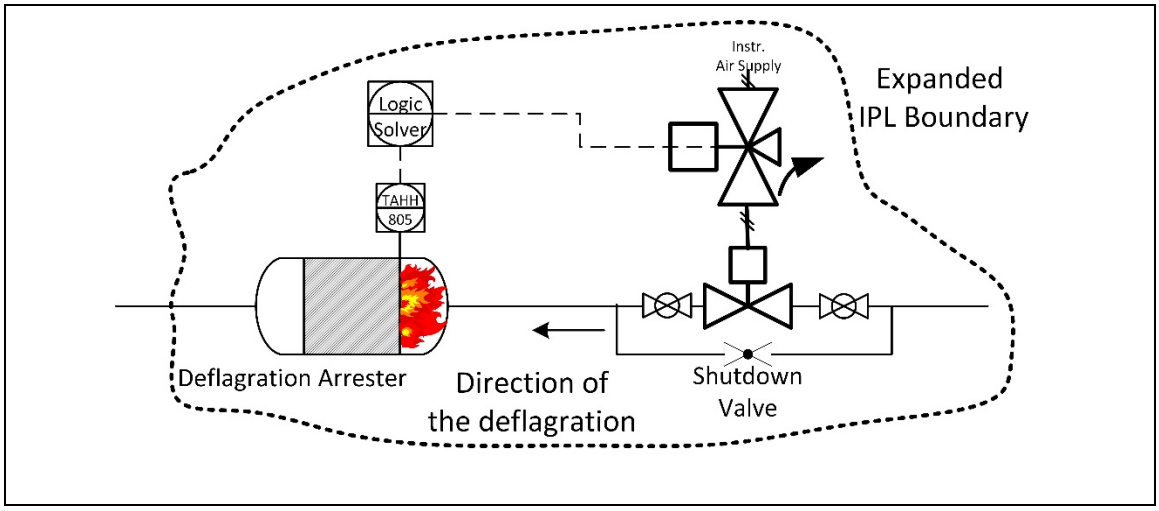

Figure 10: Deflagration arrester with expanded IPL boundary, including TAHH and shutdown valve

Likewise, the IPL PFD calculation must include the PFD of the temperature monitoring and the TAHH response.

8. Unseen part of the IPL boundary

In many of the examples shown above, there are parts of the expanded IPL boundary that are unseen as personnel typically review the documentation. It is critical to drill down into the details to understand fully what the expanded boundary is.

For example, in the SIF example, the auto/manual switch that can disable the SIF is not displayed on a P&ID. The auto manual switch may be a physical device or it may be coded in the logic solver software. With either configuration, the P&ID viewer does not know that the auto manual switch exists, and does not know to include it in the expanded boundary.

Likewise, although the root valves and the bypass valves around the SIF shutdown valve are visible on a P&ID, they may be unseen. Personnel may simply overlook them and may not recognize that they should be part of the expanded IPL boundary.

For pressure relief devices, the block valves and other devices (such as flame arrestors and back pressure valves) may be seen on the P&ID, but may be overlooked in considerations of the PFD for the relief device. The P&ID may not show the relief device design basis (e.g., fire, blocked outlet), and most P&IDs do not show that the fire-resistant insulation and cladding are part of the relief design basis.

For these reasons, analysts, engineers, designers, and maintainers must go beyond what is readily visible and thoroughly understand all the equipment and human actions necessary for the IPL to operate. They must also understand all the bypasses and other device failures that can prevent the IPL from operating correctly.

3 Conclusion

To correctly evaluate IPLs, the boundary of each IPL must be correctly understood and critically evaluated. These questions must be answered:

- What has to happen from the process-wetted-surface of the detection part of the IPL through the decision-making part of the IPL to the process-wetted-surface deflection part of the IPL?
- What equipment and what humans must take what actions?

Omitted equipment and actions may not be appropriately designed, tested, verified, validated, or maintained, thereby increasing the risk of the process. If equipment and actions are omitted from the IPL boundary, then the PFD calculated for the IPL may be much more optimistic than the PFD that takes into consideration all of the required equipment and actions.

4 References

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

[2] Bridges , W. G., & Dowell, A. M., III, "Identify SIF, SIL, and IPLs as Part of PHA, or Why It is Not Necessary to ‘Boldly Go Beyond HAZOP and LOPA'," in *12th Global Congress on Process Safety*, April 2016.

[3] ANSI/ISA 84.00.01-2004 (IEC61511-1 Mod), "Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Part 1: Framework, Definitions, System, Hardware and Software Requirements," 2004.

[4] Bridges, W. G., & Thomas, Hal, "Accounting for Human Error Probability in SIL Verification Calculations," in *8th Global Congress on Process Safety*, April 1-4, 2012.

[5] Bridges, W. G., & Dowell, A. M., III, "Key Issues with Implementing LOPA – Perspective from the Originators of LOPA," in *11th Global Congress on Process Safety*, April 2015.

[6] CCPS, *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*, New York, New York: Center for Chemical Process Safety, American Institute of Chemical Engineers, 2015.