Are You Being Honest With Yourself Regarding IPL Integrity?

Mr. Andrew C. Madewell, P.E.
Cognascents Consulting Group, Inc.
11777-A Katy Freeway, Ste 438
Houston, TX 77079
andrew.madewell@cognascents.com

Prepared for Presentation at
American Institute of Chemical Engineers
2014 Spring Meeting
10th Global Congress on Process Safety
New Orleans, Louisiana
March 30 – April 3, 2014

Are You Being Honest With Yourself Regarding IPL Integrity?

Mr. Andrew C. Madewell, P.E.
Cognascents Consulting Group, Inc.
11777-A Katy Freeway, Ste 438
Houston, TX 77079
andrew.madewell@cognascents.com

Keywords: Independent Protection Layer (IPL), Process Safety Management (PSM), Layer of Protection Analysis (LOPA), Process and Instrumentation Drawing (P&ID), Process Hazard Analysis (PHA), Process Safety Lifecycle, Safety Integrity Level (SIL).

Abstract

Independent Protection Layers (IPLs) are critical pieces of armor designed to protect against process upsets that may harm people, the environment, and/or commercial interests. IPLs play a key role in any Process Safety Management (PSM) program. They are often used to close the risk gap between elimination/mitigation measures and associated hazard scenario causes and consequences; hence, regulations exist that require companies to demonstrate IPL integrity and adequacy.

When conducting a Process Hazard Analysis (PHA) using the Layer of Protection Analysis (LOPA) methodology, IPLs are used to close the risk gap between elimination/mitigation measures for a given hazard scenario and its cause, consequence, and conditional modifiers. In order for an IPL to be "available", it must meet certain criteria defined by industry standards and company-specific guidance documents.

Demonstrating IPL effectiveness, or adequacy, involves multiple pieces of information that are not always linked together and kept "evergreen". In addition, the various data repositories and tasks required to maintain the integrity of an IPL are "owned" by several functional roles. Required data for IPL adequacy include the following: IPL design information, IPL integrity level analyses, maintenance and function testing data, and process safety time and IPL response time analyses.

Companies do not approach IPL integrity the same way. For example, companies perform IPL function testing and maintenance using different criteria; some employ a standard function testing methodology of confirmation that the IPL acts within the designated time window per regulatory requirements, while other companies actually measure the specific time it takes an IPL to respond to get to its process safe condition. Either of these approaches provides compliance as to whether the IPL will act adequately given a process upset; however, vulnerabilities may exist depending on the approach employed.

The author posits that use of an evergreen IPL lifecycle reduces potential vulnerabilities in the design and function of an IPL. In this paper, the author presents the advantages and disadvantages of using an evergreen lifecycle approach to establish and maintain the integrity and "availability" of IPLs. The author also provides recommendations to enhance the robustness of maintaining IPL adequacy throughout the lifecycle of the protection layer. Specifically, the author provides examples of IPL integrity successes through the use of an evergreen lifecycle methodology, enhanced operational insight, and potential pitfalls when not employing a holistic IPL lifecycle approach in maintaining IPL integrity and adequacy.

The target audience for this paper includes project managers, project or process engineers, EH&S managers, PSM coordinators, and operators; however, anyone involved with small or large capital projects may also benefit from this paper's content.

1. Background and Purpose

Demonstrating IPL integrity plays a critical role in mitigating or eliminating undesired events across the oil, gas, and chemical industries. These safety devices are strategically designed and installed to reduce the risk involved during process operation. The design and operational effectiveness of a particular safety device involves multiple pieces of information/data. Required information includes design basis and process description, Safety Integrity Level (SIL) calculations, IPL testing and maintenance philosophy, and process safety time analysis.

Protective instruments are typically specified during early facility design (i.e. Define stage); however, the author has found that ongoing review and analysis of each installed IPL at a given facility throughout the facility lifetime does not always occur, leaving potential safety protection shortfalls. Something as simple as changing an alarm or trip set-point may affect the integrity of an installed IPL, and the author can reference multiple instances where minor changes like this have proven an IPL to be inadequate at providing proper protection.

One way to ensure IPL integrity throughout the lifetime of a facility is the implementation of an evergreen lifecycle approach to capture the "real-time" process risk. This paper outlines such a methodology, documenting the benefits and potential hardships. Specifically, the author outlines how all pieces of information surrounding the integrity of an IPL relate to one another, and how a small change in one process parameter may have profound changes to IPL integrity, and ultimately the risk profile. Without the implementation of an evergreen lifecycle approach, vulnerabilities may exist leaving a system inadequately protected against a process excursion.

2. IPL Criteria

When conducting a PHA using the LOPA methodology, IPLs are used to close the risk gap between elimination/mitigation measures for a given hazard scenario and its cause, consequence, and conditional modifiers. In order for an IPL to be "available", it must meet certain criteria defined by industry standards and company-specific guidance documents. The required criteria based on Recognized and Generally Accepted Good Engineering Practices (RAGAGEP) is given below.

2.1 Effectiveness

In order to take credit for an IPL in a LOPA study, the system, device, or action must be deemed effective at either mitigating or eliminating the undesired event from occurring. The following is a list of questions that should be asked when discussing potential IPLs during a LOPA session. Note that the list of questions below is not a complete exhaustive list.

- Will the potential IPL detect the unwanted condition?
- Will the potential IPL act quick enough to prevent the undesired consequence?
- Does the potential IPL have adequate capacity to protect against the undesired scenario (i.e. relief device capacity)?

2.2 Independence

For a safeguard to be considered an IPL, the LOPA team must ensure that the IPL is independent of the hazard scenario initiating event, as well as independent from any additional IPLs credited for the same event. For example, if the initiating event is an inadvertent valve opening due to human error, credit should not be taken (as an IPL) for operator response to an alarm, regardless of the time required to reach an unsafe condition. Furthermore, if credit is taken for a high pressure interlock that is acting as part of the safety shutdown system, credit should not be given to any additional IPLs installed on the same safety shutdown system.

2.3 Auditability

An IPL must be auditable in order to demonstrate that it meets the necessary risk mitigation criteria. This audit process must confirm the effectiveness and independence of the IPL(s) in question as outlined above. The auditability ties directly into the evergreen IPL lifecycle outlined below in that if one incorporates an evergreen lifecycle approach to their IPLs, then the auditability aspect becomes part of the evergreen lifecycle.

3. Data Required for IPL Integrity

When designing a protective system or device, the following information/data is required. This information is considered the bare minimum required when implementing protective devices to mitigate and/or eliminate undesired events.

3.1 Design Basis

A protective device, or IPL, is designed and installed for a specific function in the process, and design information ensures that the device specified will meet those requirements. Design information includes the following:

- Process conditions, including equipment and process limitations
- Drawings and diagrams
- Installation criteria
- Potential hazard scenarios the device is designed to protect against

3.2 Safety Integrity Level (SIL) Analysis

The quantitative analysis documenting a IPLs capability to protect against a hazard scenario is the SIL calculation analysis. Major inputs to these calculations include process conditions (including equipment and process limiting criteria), as well as applicable hazard scenarios for which the IPL is designed and installed to protect against (as identified in all applicable LOPA analyses). These inputs are used to generate a specific Probability of Failure on Demand (PFD) for the IPL in question. This PFD value will encompass all the demands placed on the IPL (i.e.

the PFD value will reflect whether the IPL is installed to protect against one hazard scenario or four hazard scenarios).

3.3 IPL Operational Surveillance

The output PFD from the SIL calculations is typically based on a low-usage rate for the IPL; therefore operational surveillance surrounding IPL trips needs to be conducted to track the instances where the IPL is being called upon to act. This data should be closely monitored as the integrity of the IPL may change if the IPL trip rate increases over time and exceeds the low-usage rate criteria limit.

3.4 IPL Testing and Maintenance Philosophy

The testing and maintenance philosophy and records are typically driven by regulatory and/or corporate specific compliance standards, as well as the SIL of the IPL. For example, an IPL with a PFD of $1x10^{-1}$ will have a different testing and maintenance schedule than an IPL with a calculated PFD of $1x10^{-3}$. The testing a maintenance programs around protective layers become stricter, and the frequencies of testing increase with increasing PFD values.

3.5 Process Safety Time (PST) and Response Time Analyses

The PST calculations document the time it takes for a process to deviate from normal conditions to an upset (i.e. the time required for the process to deviate from the maximum operating pressure to exceeding design pressure in the event of a blocked outlet). Process safety time criteria may deviate slightly across the industry, but the goal of the exercise is to compare the process safety time against the response time of the IPL to ensure that the protective device will act fast enough to avoid an unsafe condition and return the process to a safe state. The response time is the time it takes an IPL to act from the initial IPL initiation to the point of a safe condition.

4. Evergreen Lifecycle for IPL Integrity

All of the data previously identified around an IPL is typically overseen by multiple disciplines. The design information and SIL calculations are usually owned by the instrumentation discipline, while the testing and maintenance activities are employed by operations and/or maintenance disciplines. The process surveillance and process safety times are typically owned by the process engineering discipline. This multi-discipline ownership creates a potential area of concern when ensuring the adequacy of an IPL as a lack of communication may cause an IPL to become inadequate in regards to its integrity rating due to changing process operating conditions.

A solution to this potential shortfall is an evergreen lifecycle approach to IPL integrity. The lifecycle starts with the design and installation of the IPL and continues through the decommissioning process. The use of an evergreen lifecycle reduces potential vulnerabilities in the design and function of an IPL. When established correctly, an evergreen lifecycle effectively ensures that when one set of data or information is updated or modified, all other sets of data are reviewed and/or updated during the process.

One main challenge which the author has witnessed across the industry is ensuring adequate cross-communication between disciplines. All too often separate disciplines (i.e. instrumentation and process engineering) operate in a semi-vacuum and do not effectively communicate process design or operation changes. This creates the potential for an IPL and its associated design to not be maintained and updated properly through the design change process, leading to the question of whether or not an installed IPL is really protecting against an unsafe condition.

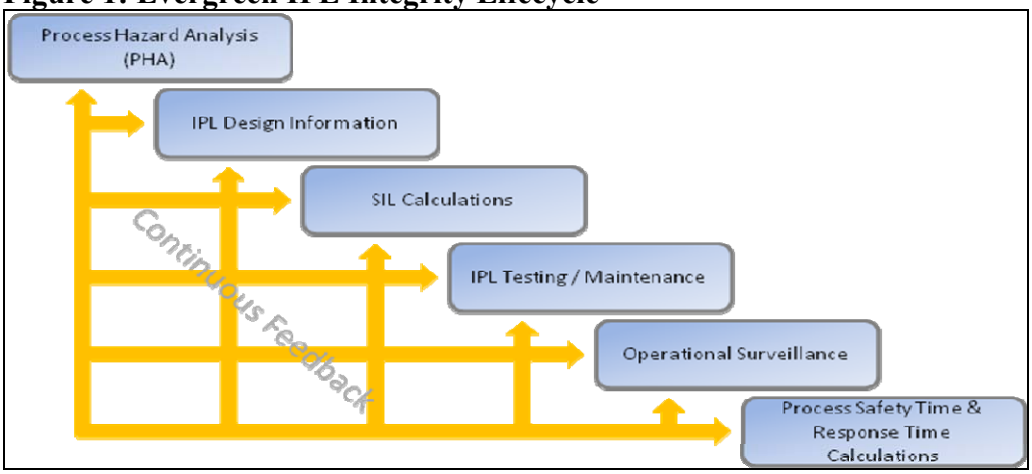
With an evergreen lifecycle approach to IPL integrity, this communication gap is reduced as separate functional teams are required to communicate with one another. For example, if operating conditions are modified to increase process throughput, then instrumentation and operations personnel are responsible for consulting with each other to evaluate whether the operating condition change will affect the design or SIL values for the IPL installed. The collaboration would then help determine whether or not the IPL will still provide adequate protection against undesired events, or if modifications are required.

A second challenge that has been witnessed surrounds process safety times. Multiple instances have occurred in which process safety times have been examined when reviewing an IPL and it has been determined that the process safety time calculations were outdated and not based on current operational conditions. If the process safety times are not accurate, then the adequacy of an IPL may be in question as the process safety time may be lower than the device response time. Using an evergreen lifecycle, a change in process conditions would require a review of the process safety times. The reviewed and/or updated process safety times would then be compared with the IPL response time to ensure adequate IPL integrity.

A third challenge is the lack of operational surveillance around IPL trips. A SIL calculation is based on a low usage rate for the IPL in question. If process surveillance is not being conducted to determine when and how many trips an IPL has over a specified time duration, a SIL calculation and resulting PFD value may be inaccurate and no longer valid. If trip rates exceed the low-usage rate criteria in the SIL calculations, then the resulting PFD may in fact be lower (i.e. $1x10^{-1}$ instead or $1x10^{-2}$) leaving the system in a lower state of protection. Employing an evergreen lifecycle approach would facilitate the comparison of such pieces of information and provide feedback for the ongoing integrity of an IPL.

An evergreen approach to IPL analysis ensures that all aspects of the IPL lifecycle are being analyzed and maintained in “real-time”, with the added benefit of allowing continual feedback. If a change in operating conditions occurs (i.e. alarm or trip set-point change), then the process safety times are revalidated based on the change to reflect accuracy. This will then be used to revalidate the SIL calculations to achieve the new PFD for the IPL. The updated SIL rating will drive any necessary changes to the IPL testing and maintenance frequencies, along with changes to the risk profile resulting from the updated PFD values in the LOPA analyses. Figure 1 below shows this inter-relationship, specifically outlining how each piece of data has the capability to affect any and all other information surrounding an IPL.

Figure 1: Evergreen IPL Integrity Lifecycle



The evergreen lifecycle approach will also facilitate greater operational insight to the process, which may lead to future Inherently Safer Design (ISD) opportunities. For example, if an IPL is determined to be tripping at an elevated rate (through operational surveillance), one may determine that reducing operating conditions may be an inherently safer option than ensuring that the IPL SIL calculations are valid for the elevated usage rate (may require IPL design changes). This type of analysis is at the heart of process safety and falls in alignment with process safety principles.

A potential hardship of employing an evergreen lifecycle approach to IPL integrity may be the additional time required to complete multiple comparisons and analyses when ensuring integrity compliance. However, this additional time (man hours and cost) can be weighed against the potential impacts of not using such a methodology. The author argues that the safety and financial impacts of not using such a philosophy is far greater than the cost of following an evergreen approach.

5. Conclusion

The author recommends implementing an evergreen lifecycle approach to IPLs, which will help aid cross-discipline communication. This is a main challenge routinely observed when looking into IPL integrity at different facilities. Although all necessary IPL information may be available, it is common to observe pieces of data that are based on slightly different design and operational parameters due to a lack of effective communication among necessary shareholders.

More specifically, the author suggests that an evergreen lifecycle approach to IPL integrity will help ensure that IPLs (1) are designed adequately, (2) will effectively provide protection against process upsets throughout the life of the process, and (3) are accurately reflected during LOPA analyses to determine the "real-time" risk of the process being evaluated. This approach will also ensure compliance with Process Safety Management (PSM) regulations and audits. Failure to implement a lifecycle approach or similar methodology to IPLs may leave one susceptible to inadequate process safety protection and/or potential process incidents, something industry seeks to avoid.

6. References

[1] Center for Chemical Process Safety, *Layer of Protection Analysis - Simplified Process Risk Assessment*, Copyright © 2001, American Institute of Chemical Engineers, 3 Park Avenue, New York, NY 10016-5991.

[2] Center for Chemical Process Safety, *Guidelines for Process Safety Documentation*, Copyright © 1995, American Institute of Chemical Engineers, 345 East 47th Street, New York, NY 10017.

[3] Center for Chemical Process Safety, *Guidelines for Safe and Reliable Instrumented Protective Systems*, Copyright © 2007, Published by John Wiley & Sons, Inc., Hoboken, 111 River Street, New Jersey 07030.