
# Challenges in Differentiating Safeguards and Independent Protection Layers in a LOPA Analysis

**Holman Leonardo Sotelo Rojas**

**CST – CONSERTO S.A.S.**

**Bogotá, CO**

**holman.sotelo@cstrisk.com**

Prepared for Presentation at American Institute of Chemical Engineers

10th Latin American Conference on Process Safety Barranquilla, Colombia September

18-20, 2024

# Challenges in Differentiating Safeguards and Independent Protection Layers in a LOPA Analysis

**Holman Leonardo Sotelo Rojas**

**CST – CONSERTO S.A.S.**

**Bogotá, CO**

**holman.sotelo@cstrisk.com**

**Keywords:** LOPA (Layer of Protection Analysis) , Safeguards, Independent Protection Layers (IPL), Process Safety, Risk Assessment, Hazard Identification, Functional Safety, Risk Management, Process Hazard Analysis (PHA), HAZOP (Hazard and Operability Study).

**Abstract**

This paper discusses the challenges of differentiating between safeguards and Independent Protection Layers (IPLs) in a Layer of Protection Analysis (LOPA). The confusion between these concepts can lead to an underestimation of risks, potentially creating unsafe conditions. The paper emphasizes the importance of correctly identifying IPLs based on their independence, specificity, auditability, and reliability to ensure effective risk management in process safety.

## 1 Introduction

Over the years, there has been an increasing emphasis on the need to integrate different concepts of functional safety, as established in various international standards and regulations. These have become crucial in the identification of hazards and risk assessment in various industries, particularly in process safety. This integration focuses on the risk assessment phases and the definition of preventive measures for elements, components, equipment, people, environmental impact, corporate image, and other aspects that affect operational continuity in a given sector through the application of methodologies proposed in industry-related standards. One such methodology is known as Layer of Protection Analysis (LOPA). The data feeding this methodology comes from hazard identification studies, known as Process Hazard Analysis (PHA), such as HAZard & OPerability (HAZOP) and Failure Modes & Effects Analysis (FMEA), which are structured methodologies capable of analyzing potential high-consequence scenarios that may arise in any system under review. Thus, through the information generated during a

PHA study, risks are identified, safeguards are recorded, and then, through the application of LOPA, it is verified whether these safeguards meet the characteristics of Independent Protection Layers (IPLs) to determine if the target risk is managed by the organization.

LOPA is a semi-quantitative methodology that plays a crucial role in identifying high-severity scenarios defined during a process safety risk analysis. A key aspect to validate whether the design is sufficiently safe to cover the accepted target risk for an organization is the definition of Independent Protection Layers (IPLs) and their correct differentiation from the safeguards identified for each scenario under analysis. For this, it is essential that the LOPA analysis team knows the main characteristics that define an independent protection layer and distinguish it from a safeguard.

Thus, we can say that all independent protection layers are considered safeguards, but not all safeguards are considered independent protection layers. This distinction is crucial because confusing these concepts can lead to an underestimation of risk, creating a false sense of security where operations, personnel, assets, or the environment may be in a safe condition when they are not, leading to the occurrence of major accidents. An example of this is the Bhopal disaster, where the failure to identify and maintain IPLs contributed to the occurrence of an undesired scenario.

Given the catastrophic incidents that have occurred throughout the history of industries handling hazardous substances, is it really important to address the challenge of differentiating between safeguards and independent protection layers in a LOPA analysis?

## 2 General Concepts

The purpose of a safeguard, such as an alarm, is to try to prevent the initiating event from triggering a chain of events that could create a potential scenario for the organization or, failing that, to mitigate the associated impact resulting from equipment malfunction, process deviation, or abnormal conditions that require timely response. Safeguards help the operator maintain the process within normal operating conditions. They also play an important role in maintaining plant safety by providing a means of risk reduction (a layer of protection) to prevent damage from occurring due to a process hazard [1].

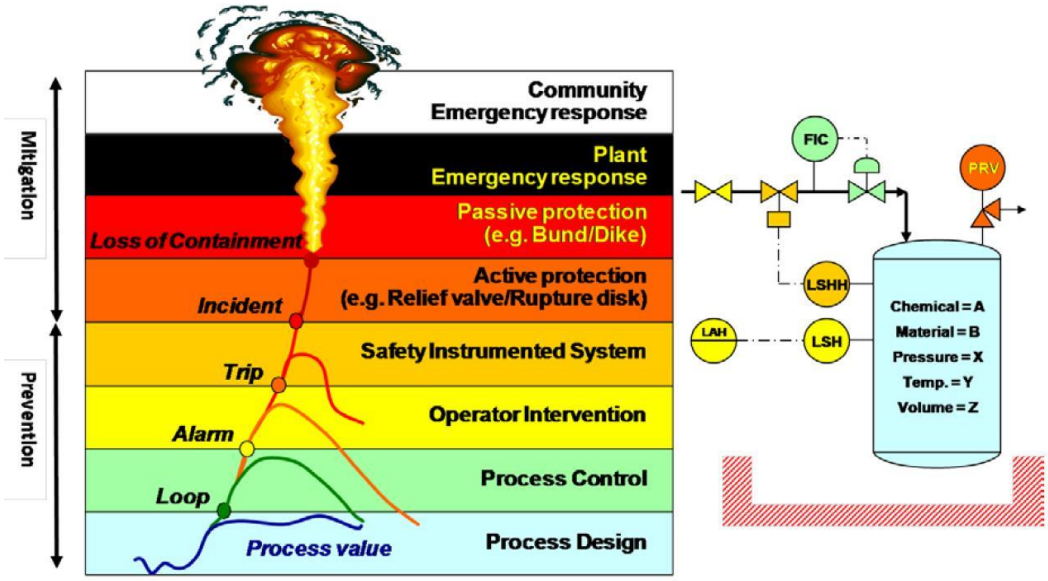


**Figure 1 Protection Layers and Their Impact on the Process**

Among the safeguards, due to their inherent characteristics, there are different types, such as structured rounds, operational discipline, an alarm with associated operational action, a relief valve, or a Safety Instrumented System (SIS). However, the effectiveness of safeguards, for example, the operator's response to an alarm—being a manual action subject to human error—raises questions about whether high-potential scenarios are being correctly managed. A failure to respond within the required time to address a process safety event could lead to catastrophic scenarios.

Due to the inherent unreliability of human behavior, many safety professionals struggle with determining the credit that can be attributed to a safeguard in a Layer of Protection Analysis (LOPA). Sometimes, the risk analysis team tends to be very conservative and does not accept any credit for safeguards, while others are overly optimistic and consider sufficient risk reduction to conclude that the scenario of interest falls within an organization's tolerable zone.

When safeguards do not meet the essential characteristics to be defined as Independent Protection Layers, the result can lead to catastrophic accidents, such as those in Milford Haven (UK), Texas City (USA), and Buncefield (UK). In the Buncefield oil depot, a failure in the tank level sensor prevented the associated high-level alarm from alerting the operator. When the tank level reached its "maximum" point, a second protection layer, an independent safety switch, failed to trigger an alarm to notify the operator and did not initiate a shutdown that would have automatically cut off the incoming flow. The tank overflowed, and the subsequent fire resulted in a loss of $1 billion ($1.6 billion) [1].

Therefore, understanding the difference between a safeguard—defined as any safety device that interrupts the chain of events following an initiating event to prevent a consequence or reduce the severity of a consequence, and generally reduce risk—is

crucial. Safeguards can be devices, systems, or actions performed by a person or operator. They help protect a process when the system deviates from safe operating conditions.

Safeguards are often used in Process Hazard Analysis (PHAs) or HAZOP studies as a way to reduce the severity or probability of an identified scenario through risk assessment.

A preventive safeguard is one that can prevent the primary event of a scenario from occurring. It intervenes between an initiating cause and a primary event. For example, in a scenario where the initiating cause is pump activation that would result in overfilling an upstream vessel, a preventive safeguard would be a low-flow alarm on the pump with the associated operator action. Ideally, the operator would respond to the low-flow alarm, either bringing the pump back into service or stopping the filling of the upstream vessel, thereby preventing the primary event of overfilling.

A mitigating safeguard is one that can mitigate the consequences of the primary event of a scenario. It intervenes between a primary event and its consequences. For example, in a scenario where the primary event is the overfilling of an upstream vessel and the loss of containment of materials with high H2S content, potentially causing injury due to personnel exposure to H2S, a mitigating safeguard would be H2S monitors for personnel. The H2S monitor is only necessary if a release occurs, but ideally, it would alert personnel to the high H2S content in the area, mitigating the primary event of overfilling by preventing injury due to exposure.

## 3 Correct Identification of IPLs

To correctly identify IPLs, a detailed analysis of each risk scenario must be conducted, evaluating the independence and effectiveness of each proposed layer. This includes reviewing the Probability of Failure on Demand (PFD) and applying criteria established by relevant regulations that define the main characteristics of an IPL, which not all safeguards are capable of meeting.

Before defining the characteristics of IPLs, it is necessary to understand some concepts that support the development of this paper.

Starting with the definition of safeguards, they can be described as control measures that prevent or reduce the likelihood of a hazardous event occurring. These can include alarm systems, operating procedures, safety equipment, etc.

Independent Protection Layers (IPLs) are elements that act as barriers to prevent or mitigate unwanted consequences. As their name implies, they must be independent of each other and meet specific criteria for independence, auditability, specificity, and reliability [2].

Independence is crucial; an IPL must operate autonomously and should not be influenced by the failure of another system or by the initiating event it is designed to control. It should not depend on other protection layers or the basic process control systems. Independence ensures that if one layer fails or is compromised, it does not affect the IPL's ability to perform its protective function.

Specificity refers to the fact that each IPL is designed to address a particular hazard or risk and effectively counter that specific risk scenario. This means that the IPL must be capable of detecting and mitigating a specific hazardous event without being generic or applicable to multiple situations without distinction.

For example, if an IPL is designed to prevent overpressure in a chemical reactor, it must be specific to that task, such as a pressure relief valve calibrated for that purpose. It would not be considered specific if the same valve is used to control different types of risks not directly related to overpressure.

The specificity of an IPL is important because it ensures that the protection is adequate and effective for the risk it is intended to mitigate. Additionally, it helps avoid relying on an IPL for multiple functions, which could compromise its protective capability if a risk scenario arises.

Auditability means that the IPL must be designed in such a way that its operation and effectiveness can be verified and validated. In other words, it must be possible to conduct audits to confirm that the IPL is operating as intended and is effective in preventing incidents. This implies that the IPL must have proper documentation and records that allow auditors to review its design, maintenance, and operation.

Moreover, it must be possible to test the IPL to ensure that it will function as expected in response to hazardous conditions. Auditability is crucial to ensure that the implemented safety measures are reliable and are working correctly at all times.

Reliability ensures that the IPL will perform as intended, while auditability allows for verification that the IPL remains effective over time.

Given that in a LOPA analysis, the working team may not be fully aware of the previously mentioned characteristics, there is a risk of classifying safeguards as IPLs when they are not. But then, how do we avoid this confusion?

A rigorous and conscious analysis must be conducted to make the LOPA analysis more effective and realistic, evaluating each control measure, whether preventive or mitigating, individually. To do this, the following questions should be asked: Is this safeguard independent? Is it auditable? Is it specific? Is it reliable? The identification of IPLs must be so strict that if the answer to just one of these questions is negative, that control measure or safeguard CANNOT be categorized as an IPL. Thus, verification must continue until it is ensured that the necessary IPLs are in place to cover the target

risk accepted by the organization.

Considering the previously defined criteria, the following safeguards are considered Independent Protection Layers.

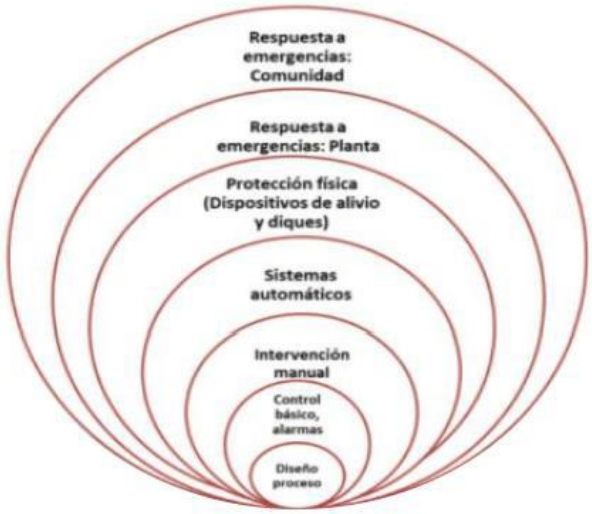


**Figure 2. Independent Protection Layers in Process Plants (IEC 61511)**

## 4 IPLs vs. Safeguards

In geometric terms, an IPL is a square and a protection layer is a rectangle. All IPLs are protection layers, but not all protection layers are IPLs. IPLs are protection elements that also meet more rigorous criteria.

Most of the time, the safeguards credited during the PHA or HAZOP part of the study are mentioned as possible IPLs for LOPA. Part of the LOPA process is to determine which safeguards qualify as IPLs. It should also be noted that a safeguard may be an IPL for one risk scenario but not for another. It is common to make mistakes when qualifying safeguards as IPLs, which means that this aspect of LOPA requires careful deliberation [4].

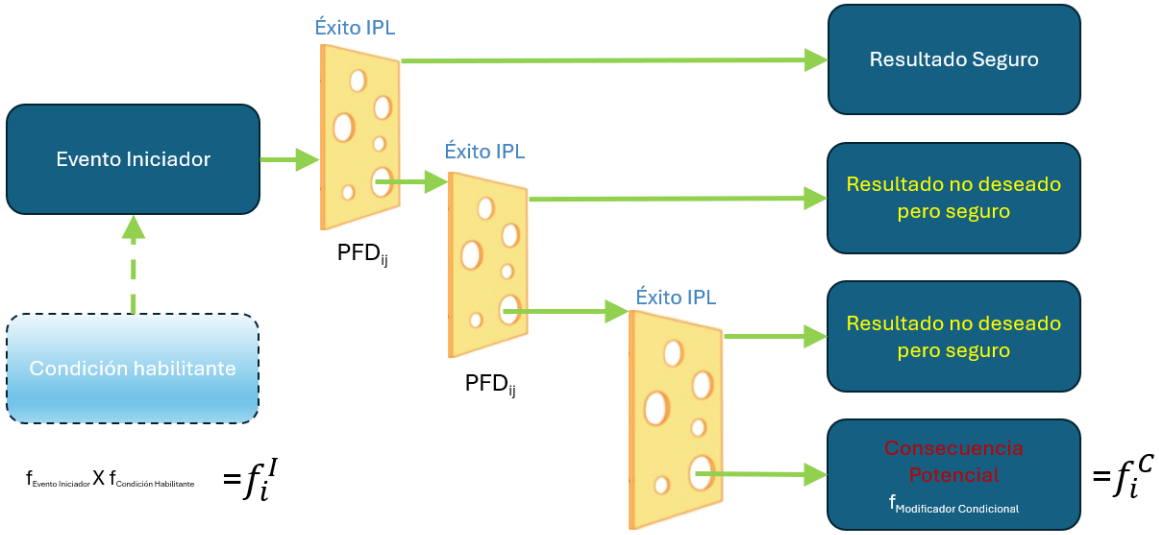


**Figure 3. Swiss Cheese Metaphor: Effectiveness of Safeguards as IPLs.**

## 5 Conclusion

The threat that an organization may face by underestimating high-severity potential scenarios studied in a Layer of Protection Analysis (LOPA) due to a lack of conceptual clarity regarding safeguards and independent protection layers, which play different roles, can lead to a situation where high-consequence scenarios are underestimated. This underestimation could result in individuals who work with hazards, such as handling dangerous substances, being constantly exposed to maximum risk or possible fatality.
According to their specific characteristics, the tools described in this paper are aimed at interrupting a chain of events triggered by a cause and ensuring that the operation maintains the necessary level of control and safety to prevent or mitigate the impact associated with the analyzed scenario. However, not all safeguards have the capacity to be independent protection layers.

As a result, by delving into the concepts of safeguards and independent protection layers, understanding how they play different roles in semi-quantitative analyses and recognizing the gap between these elements, one gains the ability to effectively, clearly, and realistically define and prioritize independent protection layers as the primary element to cover the target risk accepted by an organization. This avoids an incorrect interpretation by stakeholders interested in conducting proper preventive and mitigating management over high-consequence scenarios.

## 6 References

[1] Using Alarms as a Layer of Protection, Todd Stauffer, PE exida Consulting 64 N. Main Street, Sellersville, PA tstauffer@exida.com

[2] Layers in Layer of Protection Analysis-Wiley-AIChE (2014).

[3] IEC 61511 Seguridad funcional – Sistemas instrumentados de seguridad del sector de la industria de procesos.

[4] Center for Chemical Process Safety (CCPS)-Guidelines for process equipment reliability data with data tables-Center for Chemical Process Safety of the American Institute of Chemical Engineers (1989).

[5] IEC 61882 Hazard and operability studies (HAZOP studies) – Application guide

[4] The Buncefield Investigation" - www.buncefieldinvestigation.gov.uk/reports/index.htm