# LOPA Tutorial

## Introduction

A Layers of Protection Analysis (LOPA) is a semi-quantitative study that helps identify safeguards and determine if there are sufficient safeguards to prevent against a given risk. A LOPA is conducted to ensure that process risks are successfully mitigated to an acceptable level. Figure 1 below is a visual to represent the layers of protection for a given process. The layers in the diagram are ranked from 1-9 as most-least desirable safeguards.

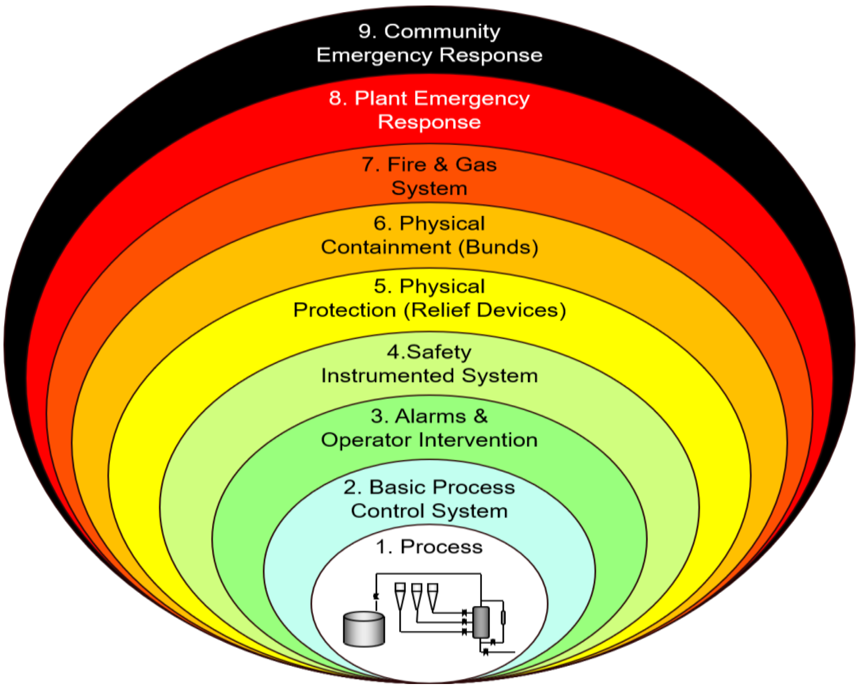


**Figure 1. Layers of Protection Example Visual [5]**

A LOPA is developed on the basis of a risk identification analysis, such as a Hazard and Operability Study (HAZOP). A HAZOP is usually carried out first and is then followed by a LOPA study. A HAZOP is a structured analysis of process design to identify process safety incidents that a facility is vulnerable to. A detailed HAZOP overview can be found in the HAZOP tutorial here.

Major hazardous scenarios, which have the potential to cause serious harm to people, environment, or business, that are discovered in a HAZOP are subjected to a LOPA. A HAZOP identifies potential hazards, while a LOPA quantifies the probability of the hazard, analyzes the system at risk, and identifies the mitigation measures that guard against the hazard. LOPA studies can be conducted with few resources, focus attention on major issues, eliminate unnecessary safeguards, establish valid safeguards to improve processes, and provides a basis for managing layers of protection. These mitigation safety measures, or “layers of protection” must meet the Center for Chemical Process Safety (CCPS) criteria of being Independent Protection Layers (IPL).

## Definitions and Relevant Information

***Independent***- Not requiring or relying on anything else

***Requirements for Independent Protection Layers (IPL)***

1) An IPL is effective in preventing the consequence
2) An IPL functions independently of the initiating event of the scenario and functions independently of all other layers that are used for that same scenario
3) An IPL is auditable (must be capable of validation including review, testing, and documentation)

There are many different possible independent protection layers that can be used in a process. Here is a list of examples of IPLs:

- Inherently Safer Design
  - Elimination or significant reduction of certain hazards
  - Examples include reducing the quantity of material involved, changing process condition, eliminating flanges, using less hazardous material, etc.
- Basic Process Control System (BPCS)
  - First layer of protection during normal operation which is designed to maintain process within a safe operating region.
  - It avoids operator intervention as process controls are done using control system.
  - Example could be a level transmitter controlling tank level by manipulating bottom control valve.
- Alarm & Operator Intervention
  - Second level of protection which alerts operator of deviation in operating parameters.
  - Examples are high level alarm, high pressure alarm

- Safety Instrumented System (SIS)
  - Detects out of limit conditions and acts to bring the process back to a safe state
  - Examples are Independent high-level switch, excess flow valves, automatic emergency shutdown etc.
- Physical Detection Devices
  - Provide a high degree of protection against overpressure
  - Examples are relief valves, rupture disc
- Passive Devices
  - Reduces the risk by preventing undesired consequences such as widespread leakage, widespread fire, etc.
  - Dike, Blast walls, flame arrestors

There are also many actions that are not considered independent layers of protection. Some examples of are NOT considered an IPL are fire brigade, manual deluge systems, and community responses.

Figure 2 below shows an example of an Independent IPL. It can be seen that each level transmitter has its own control logic and valve. If one of the control logic fails, then only one level transmitter fails to function, and the other is unaffected. Therefore, the level transmitters are independent.

Figure 3 below shows an example of a non-Independent IPL. It can be seen that the two level transmitters share the same control logic. If the control logic fails, then both the level transmitters fail to function Therefore, the level transmitters are not independent.

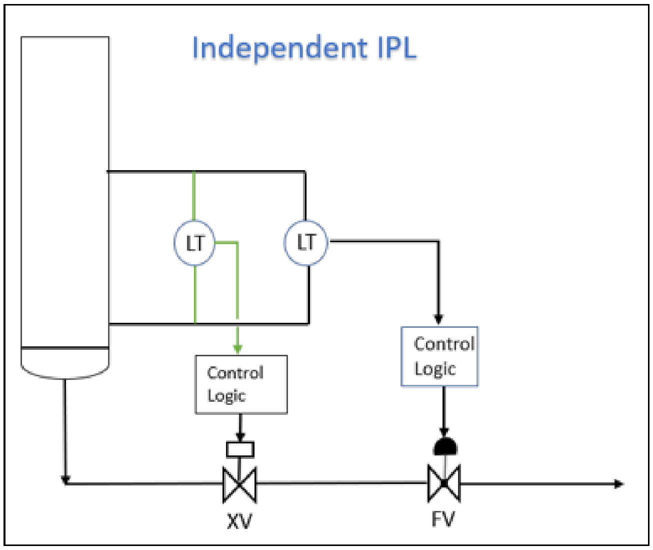


**Figure 2. Example of an Independent IPL**

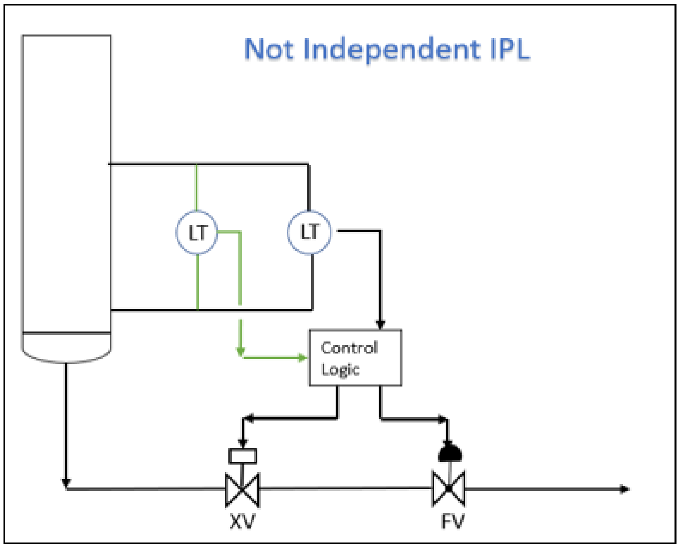


**Figure 3. Example of a Non-Independent IPL**

### *Categories of Consequences*

Potential consequences are ranked by their risk into categories 1-5. Category 1 includes the least severe consequences and category 5 includes the most severe. Consequences can put health, safety, and company finances at risk. Some consequences put safety and company finances at different levels of risk. For example, an incident could create a “category 5” consequence for safety but only a “category 3” consequence for finances. When determining the severity, consider the safety and business impacts independently and choose the highest severity.

See Tables 1 and 2  for more information on the different categories of consequence.

**Table 1. Categories Based on Safety Impact**

| | Severity | Safety Impact |
|---|---|---|
| Category 1 | Slight | First Aid Treatment Case |
| Category 2 | Minor | Minor Injury: Day Away from Work |
| Category 3 | Severe | Serious Injury: Hospital Stay |
| Category 4 | Major | Single Fatality |
| Category 5 | Catastrophic | Multiple Fatalities |

**Table 2. Categories Based on Business Impact**

| | Severity | Business Impact |
|---|---|---|
| Category 1 | Slight | \$0 - 100,000 |
| Category 2 | Minor | \$100,000 - 1 million |
| Category 3 | Severe | \$1 - 10 million |
| Category 4 | Major | \$10 - 100 million |
| Category 5 | Catastrophic | > \$100 million |

LOPA studies generally address approximately 5% of the significant risks issues. Most companies develop limits for LOPA studies, often focusing on major consequences of category 4 or 5 and accidents with fatalities. Most accidents occur during startup and shut down, consequently, a LOPA is often focused on consequences from incidents involving startup and shut down of equipment.

***Frequency of Initiating Event (FOIE)***

FOIE describes how often the initiating event, which is the failure that causes the given consequence, will occur. Initiating events can passive or active. Initiating events could be a natural phenomenon, control system failure, human error, etc. Probabilities of a given initiating event occurring can be found in Appendix A. When human error is deemed the initiating event, please follow the steps here:

1. Find the opportunity rate (the number of times that an activity is carried out by human annually)

2. Find human error probability (HEP). This represents probability of human mistakes in a given opportunity. The value is normally taken as $10^{-2}$/Opportunity

FOIE= Opportunities/year x HEP

***Probability of Failure of IPL on demand (PFD)***

PFD describes how often the protection layer will fail. Probabilities that a given layer will fail can be found in Appendix B.

***Mitigated consequence frequency (MCF)***

MCF describes how often an initiating event will occur and the IPL will fail. MCF is the frequency that a given consequence (see examples in Table 1) will occur. MCF is calculated by the given formula:

$$MCF = PFD \; x \; FOIE$$

## LOPA Process

The following method can be used for conducting a LOPA for any given system that possesses potential hazards:

1) Identify a single consequence to a potential process safety hazard
2) Identify an accident scenario and cause associated with the consequence
3) Identify the initiating event for the scenario and estimate the frequency of initiating event (FOIE).
4) Identify the independent protection layers that are available for this particular consequence and estimate the probability of failure on demand (PFD) for each protection layer
5) Combine the frequency of initiating event (FOIE) with the probability of failure (PFD) of the independent protection layer (IPL) to determine the mitigated consequence frequency (MCF) for the given initiating event
6) Plot the consequence frequency vs consequence severity to estimate the level of risk as seen below in Table 2. Each point will fit somewhere on this risk matrix.

$$Risk = MCF\ x\ Severity$$

**Table 2. Risk Matrix**

| | | | | | |
|---|---|---|---|---|---|
| Category 5 | | | | | |
| Category 4 | | | | | |
| Category 3 | | | | | |
| Category 2 | | | | | |
| Category 1 | | | | | |
| | Rare:<br>1 consequence every 10,000 years<br>(MCF ≤ 0.0001/year) | Unlikely:<br>1 consequence every 1000 years<br>(MCF = 0.001/year - 0.01/year) | Possible:<br>1 consequence every100 years<br>(MCF = 0.01/year - 0.1/year) | Probable:<br>1 consequence every 10 years<br>(MCF = 0.1/year - 1/year) | Highly Probably:<br>1 consequence every 1 year<br>(MCF ≥ 1/year) |

severe risk
major risk
moderate risk
minor risk

7) Compare risk found in step 6 to an acceptable level of risk and evaluate if additional IPLs are necessary

While you are completing a LOPA, please consider the following:

1. All the IPLs are maintained and working properly
2. Number of injuries/fatalities/economic loss as per CSB report
3. An initiating event cannot be taken as an IPL
4. If there are multiple IPLs in the system, then PFD of system will be product of each independent IPL PFD

$$PFD = PFD_1 * PFD_2 * PFD_3$$

5. If there are no IPLs present, the PFD value is 1.

## Example Using Explosion at Caribbean Petroleum Company (CAPECO)

In the CAPECO explosion, the main gasoline storage tank was full, so an additional shipment of gasoline had to be stored in four smaller tanks using a highly manual process. One of the tanks had a broken level transmitter so fill time was manually calculated, and unfortunately overestimated. The tank overfilled and created a gasoline vapor plume, which found a spark and rapidly exploded. Watch the video here: https://www.youtube.com/watch?v=41QMaJqxqIo and view the incident report here: https://www.csb.gov/file.aspx?DocumentId=5965

Before completing a LOPA for this example, a HAZOP was completed to expose potential hazards in CAPECO's facilities. You can view the completed interactive HAZOP worksheet for this scenario here.

After determining the main hazards in the system, a LOPA can be conducted as follows:

1) Identify a single consequence to a potential process safety hazard
*At CAPECO, the potential process safety hazard was the inaccurate filling of gasoline storage tanks. The consequence was overfilling of flammable gasoline which could lead to fire.*

2) Identify an accident scenario and cause associated with the consequence
*The storage tank could overflow due to operator error and lead to a fire.*

3) Identify the initiating event for the scenario and estimate the frequency of initiating event (FOIE).
*The initiating event would be manual operation leading to an operator error. Let's assume number of opportunities to be 100/year. According to Appendix A, the frequency of operator error is* $1x10^{-2}$.

$$\text{FOIE} = 1x10^{-2} \text{ x } 100 = 1/\text{year}$$

4) Identify the protection layers that are available for this particular consequence and estimate the probability of failure on demand (PFD) for each protection layer
*PFD values can be found in Appendix B. In this example, only a single layer of protection was available: a dike, which reduces the frequency of large consequences of a tank overfill or spill.*

$$\text{PFD (Dike)} = 1x10^{-2}$$

5) Combine the frequency of initiating event (FOIE) with the probability of failure (PFD) of the independent protection layer (IPL) to determine the mitigated consequence frequency (MCF) for the given initiating event

$$\text{MCF} = \text{FOIE x PFD (Dike)}$$
$$MCF = (1)\ x\ (1x10^{-2}) = 1x10^{-2}\ /year$$

6) Plot the consequence frequency vs consequence severity to estimate the level of risk as seen in Table 2. Each point will fit somewhere on this risk matrix.

   *An MCF of* $1.0x10^{-2}$*/year would mean there is 1 event every 100 years, which falls under the label of "Possible".*

   *In the CAPECO incident, there were no fatalities, but there were minor injuries (CSB report, page 31) corresponding to "Category 2" based on Table 1. The business impact was estimated to be more than $500 million, which corresponds to "Category 5". So, the severity category will be taken as the higher of the two, which is "Category 5".*

   *Using the risk matrix in Table 2 above, an "possible" event of "Category 5" falls into an orange box, which corresponds to a major risk.*

7) Compare risk found in step 6 to an acceptable level of risk and evaluate if additional IPLs are necessary
   *In this case, a major risk would NOT be acceptable. The layer of protection provided by installing a dike would not be adequate to prevent a major disaster.*

   *Since the risk is too high, additional layers of protection are needed. By adding more layers of protection, the MCF can be decreased which can lead to a different location in the risk matrix. In this case, additional layers of protection could decrease the risk of this event to "moderate", which is more acceptable than "major".*

   *To do this, iterate back through steps 1-6, but using additional layers and PFD values. Then evaluate again until the risk is at an acceptable level.*

To carry out a LOPA study in the safety modules, a table format will be used. A LOPA table for the CAPECO explosion is filled out for your reference based on the discussion above. Consider that the facility can only accept a moderate risk.

| **LOPA Study for CAPECO Explosion** | | |
|---|---|---|
| Initiating Event | Cause: | Operator error leading to miscalculated fill time |
| | Consequence: | Gasoline tank overfill leading to vapor cloud explosion |
| | FOIE: | $10^{-2}$ x 100= 1.0/year |
| IPL(s) | Description of $IPL_1$, $IPL_2$, ... | Physical Containment (Dike) |
| | $PFD = PFD_1 \times PFD_2 \times ...$ | $10^{-2}$ |
| MCF | MCF = FOIE x PFD | 1.0 x $10^{-2}$ /year |
| | Category of MCF: | Possible |
| Severity | Impact: | Business loss of more than $500 million |
| | Category: | 5 |
| Risk | Type of risk: | Major |
| | Acceptable / Unacceptable? | Unacceptable |
| If risk calculated above is unacceptable, please continue below: | | |
| Proposed IPL(s) (P-IPL(s)) | Description of P-$IPL_1$, P-$IPL_2$, ...: | Independent High-level alarm, Tank Overfill Protection System (SIS) |
| | P-PFD = P-$PFD_1$ x P-$PFD_2$ x ... | $10^{-1} \times 10^{-1} = 10^{-2}$ |
| MCF | MCF = FOIE x PFD x P-PFD | 1.0 x $10^{-2}$ /year x$10^{-2}$= 1.0x$10^{-4}$ / year |
| | Category of MCF: | Rare |
| Risk | Type of risk: | Moderate |
| | Acceptable / Unacceptable? | Acceptable |

It is important to note that sometimes seemingly sufficient IPLs will not be able to prevent a disaster. LOPA studies assume that equipment is well-maintained, and operators are well-prepared to complete their jobs effectively. If equipment is faulty and multiple layers of protection fail at once, unexpected incidents can still occur. While multiple layers of protection can usually prevent disasters, it is important to remember that some risks can still go undetected if process safety is not prioritized.

## Appendix A: Frequency of Initiating Event (FOIE) Values [1],[8]

| Initiating Event | FOIE Value (per Year) |
|---|---|
| Pressure vessel residual failure | $10^{-6}$ |
| Piping leak (10% section) | $10^{-3}$ |
| Atmospheric tank failure | $10^{-3}$ |
| Third-party intervention (e.g. external impact by vehicle) | $10^{-2}$ |
| Safety valve opens unexpectedly | $10^{-2}$ |
| Cooling water failure | $10^{-1}$ |
| Pump seal failure | $10^{-1}$ |
| Corrosion of tanks or equipment | $10^{-2}$ |
| Basic process control system (BPCS) instrument loop failure | $10^{-1}$ |
| External fire | $10^{-1}$ |
| Operator failure | $10^{-2}/opportunity$ |

## Appendix B: Probability of Failure on Demand (PFD) Values [1],[8]

| IPL | Comments and Definitions | PFD Value |
|---|---|---|
| Dike | Reduces the frequency of large consequences of a tank overfill, rupture, spill, etc. | $10^{-2}$ |
| Underground draining system | Reduces the frequency of large consequences of a tank overfill, rupture, spill, etc. | $10^{-2}$ |
| Open vent | Prevents overpressure | $10^{-2}$ |
| Motors, Fans, Blowers | Can be used to reduce concentration of dusts by exhausting air out of a system (e.g. dust collection system) | $10^{-2}$ |
| Fireproofing | Reduces rate of heat input and provides additional time for depressurizing, firefighting, etc. | $10^{-2}$ |
| Blast wall or bunker | Reduces the frequency of large consequences of an explosion by confining blast and by protecting equipment, buildings, etc. | $10^{-3}$ |
| Single Check Valve/ Slide Valve | Reduces the frequency of reverse flow by allowing flow in only one direction | $10^{-1}$ |
| Dual Check Valve/ Slide Valve | More efficient than single check valve in reducing frequency of reverse flow | $10^{-2}$ |
| Inherently safer design | If properly implemented, can eliminate scenarios, or significantly reduce the consequences associated with a scenario | $10^{-2}$ |
| Flame or detonation arrestors | If properly designed, installed, and maintained, can eliminate the potential for flashback through a piping system or into a vessel or tank | $10^{-2}$ |
| Relief Valve/Rupture Disk | Prevents system from exceeding specified overpressure. | $10^{-2}$ |
| Alarms | Alarms can be programmed to alert the operator to take an action | $10^{-1}$ |
| Basic process control system (BPCS) | Can be credited as an IPL if not associated with the initiating event being considered. | $10^{-1}$ |
| Safety Instrumented System (SIS) | SIS does not depend upon any operator interaction and works automatically to bring system to a safe state during an undesired event | $10^{-1}$ |
| Manual Emergency Shutdown (ESD) | Manual activation of button to shut down entire process | 0.4 |

**References**

[1] "LOPA – Layer of Protection Analysis." Process and HSE Engineering, 2 Feb. 2012, hseengineer.wordpress.com/lopa-layer-of-protection-analysis/.

[2] Summers, Angela E. (July 2014). "Introduction to Layer of Protection Analysis" (July 2014). *SIS-Tech.*

[3] "Risk Assessment ." *Chemical Process Safety: Fundamentals With Applications*, by Daniel A. Crowl and Joseph F. Louvar, 3rd ed., Pearson, 2011, pp. 577–587.

[4] Gate Inc. "Introduction to Layer of Protection Analysis (LOPA)". Gate Keeper: A Technical Newsletter for the Oil & Gas Industry (July 2014).

[5] Spencer, Gabi. "Multiple Layers of Protection & Mitigation." *ESC*, 26 Jan. 2109, www.esc.uk.net/guidance-for-performing-an-effective-lopa-2/multiple-layers-of-protection-mitigation/.

[6] Shuttleworth, Mike. "Qualitative and Quantitative Risk Analysis. What Is the Difference?" *Project Risk Manager*, 13 Oct. 2019, www.project-risk-manager.com/blog/qualitative-and-quantitative-risk-analysis/.

[7] "Independent." *Merriam-Webster*, Merriam-Webster, www.merriam-webster.com/dictionary/independent .

[8] Crowl, Daniel A., and Joseph F. Louvar. *Chemical Process Safety: Fundamentals with Applications*. Pearson, 2019.

**Created in Collaboration with Lydia Peters**