TOPIC 2.5
LAYER OF PROTECTION ANALYSIS (LOPA)
How to reduce PFD

- Using redundant sensors and final redundant control elements
- Using multiple sensors with voting systems and redundant final control elements
- Testing the system components at specific intervals to reduce the PFD by detecting hidden failures
- Using deenergized trip system (i.e., a relayed shutdown system)
Independent Protection Layer Restrictions

- Sufficiently independent so that the failure of one IPL does not adversely affect the probability of failure of another IPL
- Designed to prevent the hazardous event, or mitigate the consequences of the event
- Designed to perform its safety function during normal, abnormal, and design basis conditions
- Auditable for performance
Add IPL to reduce Risks

Unmitigated Risk

Initiating Event
Frequency = 1/yr

Success = 0.9

Failure = 0.1

Mitigated Risk = reduced frequency * reduced consequence

Different Scenario
Consequence Occurs

Preventive Feature

PFD=0.1

PFD=0.1

PFD=0.01

Preventive Feature

Mitigative Feature

Success = 0.9

Success = 0.9

Success = 0.99

Failure = 0.1

Failure = 0.1

Failure = 0.01

Frequency = 0.9/yr
Safe Outcome

Frequency = 0.09/yr
Safe Outcome

Frequency = 0.0099/yr
Mitigated Release, tolerable outcome

Frequency 0.0001/yr
Consequences exceeding criteria

www.utm.my
WHAT ARE IPL?

- Each layer is independent in terms of operation.
- The failure of one layer does not affect the next.
Independent layer of protections (IPL) are features to provide risk reductions in plant operations.

Categories of IPLs:

- **Prevention (active – lower probability)**
  - Alarm with operator response
  - Safety Instrumented System

- **Mitigation (active – lower probability/consequence)**
  - Pressure relief valve

- **Protection (passive – lower consequence)**
  - Dikes
  - Mechanical design
  - Barricades
LOPA

- LOPA is a semi-quantitative risk analysis technique that is applied following a qualitative hazard identification tool such as HAZOP.
- Similar to HAZOP LOPA uses a multi-discipline team
- LOPA can be easily applied after the HAZOP, but before fault tree analysis
- LOPA focuses the risk reduction efforts toward the impact events with the highest risks.
- It provides a rational basis to allocate risk reduction resources efficiently.
- LOPA suggests the required Independent Layer of Protection (IPL) required for the system to meet the required Safety Integrity Level (SIL)
## LOPA

<table>
<thead>
<tr>
<th>Consequence &amp; Severity</th>
<th>Initiating event (cause)</th>
<th>Initiating event challenge frequency / year</th>
<th>Preventive independent protection layers Probability of failure on demand (PFD)</th>
<th>Mitigation independent protection layer (PFD)</th>
<th>Mitigated consequence frequency / year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Specific Scenario Endpoint

\[
f_i^C = f_i^I \times \prod_{j=1}^{J} PFD_{ij}
\]

\[
= f_i^I \times PFD_{i1} \times PFD_{i2} \ldots \times PFD_{iJ}
\]

- \( i \) = scenario or event
- \( j \) = IPL layer
- \( f_i^C \) = frequency for consequence C for initiating event \( i \)
- \( f_i^I \) = frequency for initiating event \( i \)
- \( PFD_{ij} \) = probability of failure on demand of the \( j \)th IPL that protects against consequence C for initiating event \( i \)

### Multiple Scenario Endpoint

\[
f^C = \sum_{i=1}^{I} f_i^C
\]
There are five basic steps in LOPA:

1. Identify the scenarios
2. Select an accident scenario
3. Identify the initiating event of the scenario and determine the initiating event frequency (events per year)
4. Identify the Independent Protection Layers (IPL) and estimate the probability of failure on demand of each IPL
5. Estimate the risk of scenario
<table>
<thead>
<tr>
<th>Initiating event</th>
<th>Frequency range from literature (per yr)</th>
<th>Example of a value chosen by a company for use in LOPA (per yr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressure vessel residual failure</td>
<td>$10^{-5}$ to $10^{-7}$</td>
<td>$1 \times 10^{-6}$</td>
</tr>
<tr>
<td>Piping residual failure, 100 m, full breach</td>
<td>$10^{-5}$ to $10^{-6}$</td>
<td>$1 \times 10^{-5}$</td>
</tr>
<tr>
<td>Piping leak (10% section), 100 m</td>
<td>$10^{-3}$ to $10^{-4}$</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Atmospheric tank failure</td>
<td>$10^{-3}$ to $10^{-5}$</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Gasket/packing blowout</td>
<td>$10^{-2}$ to $10^{-6}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Turbine/diesel engine overspeed with casing breach</td>
<td>$10^{-3}$ to $10^{-4}$</td>
<td>$1 \times 10^{-4}$</td>
</tr>
<tr>
<td>Third-party intervention (external impact by backhoe, vehicle, etc.)</td>
<td>$10^{-2}$ to $10^{-4}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Crane load drop</td>
<td>$10^{-3}$ to $10^{-4}$/lift</td>
<td>$1 \times 10^{-4}$/lift</td>
</tr>
<tr>
<td>Lightning strike</td>
<td>$10^{-3}$ to $10^{-4}$</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Safety valve opens spuriously</td>
<td>$10^{-2}$ to $10^{-4}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Cooling water failure</td>
<td>$1$ to $10^{-2}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Pump seal failure</td>
<td>$10^{-1}$ to $10^{-2}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Unloading/loading hose failure</td>
<td>$1$ to $10^{-2}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>BPCS instrument loop failure</td>
<td>$1$ to $10^{-2}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Regulator failure</td>
<td>$1$ to $10^{-1}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Small external fire (aggregate causes)</td>
<td>$10^{-1}$ to $10^{-2}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>Large external fire (aggregate causes)</td>
<td>$10^{-2}$ to $10^{-3}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>LOTO (lock-out tag-out) procedure failure (overall failure of a multiple element process)</td>
<td>$10^{-3}$ to $10^{-4}$/opportunity</td>
<td>$1 \times 10^{-3}$/opportunity</td>
</tr>
<tr>
<td>Operator failure (to execute routine procedure; well trained, unstressed, not fatigued)</td>
<td>$10^{-1}$ to $10^{-3}$/opportunity</td>
<td>$1 \times 10^{-2}$/opportunity</td>
</tr>
</tbody>
</table>

1 Individual companies choose their own values, consistent with the degree of conservatism or the company’s risk tolerance criteria. Failure rates can also be greatly affected by preventive maintenance routines.
# Typical Frequency Values

## Typical Frequencies of Initiating Events ($f'_{i}$) (From CCPS, 2001, Table 5.1)

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>Frequency (events/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressure vessel failure</td>
<td>$10^{-3}$ to $10^{-7}$</td>
</tr>
<tr>
<td>Piping failure (full breach)</td>
<td>$10^{-3}$ to $10^{-6}$</td>
</tr>
<tr>
<td>Piping failure (leak)</td>
<td>$10^{-3}$ to $10^{-4}$</td>
</tr>
<tr>
<td>Atmospheric tank failure</td>
<td>$10^{-3}$ to $10^{-5}$</td>
</tr>
<tr>
<td>Turbine/diesel engine overspeed (with casing breach)</td>
<td>$10^{-3}$ to $10^{-4}$</td>
</tr>
<tr>
<td>Third party intervention (impact by backhoe, etc.)</td>
<td>$10^{-2}$ to $10^{-4}$</td>
</tr>
<tr>
<td>Safety valve opens spuriously</td>
<td>$10^{-2}$ to $10^{-4}$</td>
</tr>
<tr>
<td>Cooling water failure</td>
<td>1 to $10^{-2}$</td>
</tr>
<tr>
<td>Pump seal failure</td>
<td>$10^{-1}$ to $10^{-2}$</td>
</tr>
<tr>
<td>BPCS loop failure</td>
<td>1 to $10^{-2}$</td>
</tr>
<tr>
<td>Pressure regulator failure</td>
<td>1 to $10^{-1}$</td>
</tr>
<tr>
<td>Small external fire</td>
<td>$10^{-1}$ to $10^{-2}$</td>
</tr>
<tr>
<td>Large external fire</td>
<td>$10^{-2}$ to $10^{-3}$</td>
</tr>
<tr>
<td>Operator failure (to execute routine procedure, assuming well trained, unstressed, not fatigued)</td>
<td>$10^{-1}$ to $10^{-3}$ (units are events/procedure)</td>
</tr>
</tbody>
</table>
# Probability of Failure on Demand

<table>
<thead>
<tr>
<th>Passive IPLs</th>
<th>Comments (assuming an adequate design basis, inspections, and maintenance procedures)</th>
<th>PFDs from industry</th>
<th>PFDs from CCPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dike</td>
<td>Reduces the frequency of large consequences (widespread spill) of a tank overfill, rupture, spill, etc.</td>
<td>$1 \times 10^{-2}$ to $1 \times 10^{-3}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Underground drainage system</td>
<td>Reduces the frequency of large consequences (widespread spill) of a tank overfill, rupture, spill, etc.</td>
<td>$1 \times 10^{-2}$ to $1 \times 10^{-3}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Open vent (no valve)</td>
<td>Prevents overpressure</td>
<td>$1 \times 10^{-2}$ to $1 \times 10^{-3}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Fireproofing</td>
<td>Reduces rate of heat input and provides additional time for depressurizing, fire fighting, etc.</td>
<td>$1 \times 10^{-2}$ to $1 \times 10^{-3}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Blast wall or bunker</td>
<td>Reduces the frequency of large consequences of an explosion by confining blast and by protecting equipment, buildings, etc.</td>
<td>$1 \times 10^{-2}$ to $1 \times 10^{-3}$</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Inherently safer design</td>
<td>If properly implemented, can eliminate scenarios or significantly reduce the consequences associated with a scenario</td>
<td>$1 \times 10^{-1}$ to $1 \times 10^{-6}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Flame or detonation arrestors</td>
<td>If properly designed, installed, and maintained, can eliminate the potential for flashback through a piping system or into a vessel or tank</td>
<td>$1 \times 10^{-1}$ to $1 \times 10^{-3}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
</tbody>
</table>

---

Some surprising data for human reliability in process operations

<table>
<thead>
<tr>
<th>PFD</th>
<th>Situation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Rapid action based on complex analysis to prevent serious accident.</td>
</tr>
<tr>
<td>$10^{-1}$</td>
<td>Busy control room with many distractions and other demands on time and attention</td>
</tr>
<tr>
<td>$10^{-2}$</td>
<td>Quiet local control room with time to analyze</td>
</tr>
</tbody>
</table>

Source: Kletz (1999)
Reduce risks to achieve the target

<table>
<thead>
<tr>
<th>Event Severity</th>
<th>extensive</th>
<th>moderate</th>
<th>high</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Medium</td>
<td>Major</td>
<td>Major</td>
</tr>
<tr>
<td>serious</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>minor</td>
<td>Minimal</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Minimal</td>
<td>Minimal</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Event Likelihood

Table entries
- word = qualitative risk description
- number = required safety integrity level (SIL)

Safety Integrity Levels
(Prob. Of failure on demand)
- 1 = .01 to .1
- 2 = .001 to .01
- 3 = .0001 to .001

Selection documented for legal requirements
SIS Depends on Structure of Redundancy

Design A. Single sensor, 1oo1
\[ \text{PFD}_{\text{sensor}} = 5.0 \times 10^{-3}, \text{Spurious trip}_{\text{sensor}} = 5 \times 10^{-2} \]

Design B1. Redundant sensors, 1oo2
\[ \text{PFD}_{\text{sensor}} = 3.3 \times 10^{-5}, \text{Spurious trip}_{\text{sensor}} = 1 \times 10^{-1} \]
SIS Depends on Structure of Redundancy

Design B2. Redundant sensors, 2oo2
(PFD_{sensor} = 1\times 10^{-2}, \text{(Spurious trip)}_{sensor} 1.4\times 10^{-5})

Design C. Redundant sensors, 2oo3 SIS logic, redundant and diverse final elements
(PFD_{sensor} = 1\times 10^{-4}, \text{(Spurious trip)}_{sensor} 4.2\times 10^{-5})
Design and Maintenance

Often, credit is taken for good design and maintenance procedures.

- Proper materials of construction (reduce corrosion)
- Proper equipment specification (pumps, etc.)
- Good maintenance (monitor for corrosion, test safety systems periodically, train personnel on proper responses, etc.)

A typical value is PFD = 0.10
The Layer of Protection Analysis (LOPA) is performed using a standard table for data entry.

<table>
<thead>
<tr>
<th>Consequence &amp; Severity</th>
<th>Initiating event (cause)</th>
<th>Initiating event challenge frequency / year</th>
<th>Preventive independent protection layers</th>
<th>Probability of failure on demand (PFD)</th>
<th>Mitigated event likelihood /year</th>
<th>Notes</th>
</tr>
</thead>
</table>

Likelihood

\[ \text{Probability of failure on demand} = f_i^C = f_i^I \left[ \prod_{j=1}^{n} (PFD)_{ij} \right] \leq f_i^{\text{max}} \]
LOPA Examples

Flash drum for component separation for this proposed design.

Feed
- Methane
- Ethane (LK)
- Propane
- Butane
- Pentane

Process fluid
- T1
- F2
- FC-1

Steam
- T2
- T3
- T5

L. Key
- T5
- TC-6
- PC-1
- LC-1
- AC-1

Vapor product
- PAH

Liquid product
- LAL
- LAH

Cascad

Split range
## LOPA Examples

Flash drum for component separation for this proposed design.

<table>
<thead>
<tr>
<th>Consequence &amp; Severity</th>
<th>Initiating event (cause)</th>
<th>Initiating event frequency /year</th>
<th>Preventive independent protection layers</th>
<th>Probability of failure on demand (PFD)</th>
<th>Mitigated event likelihood /year</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Pressure</td>
<td>Connection (tap) for sensor P1 plugged</td>
<td></td>
<td>Process design</td>
<td>BPCS</td>
<td>Operator response to alarm</td>
<td>SIF (PLC relay)</td>
</tr>
</tbody>
</table>

The target mitigated likelihood = $10^{-5}$ event/year

The likelihood of the event = $10^{-1}$ events/year
Some observations about the design.

• The drum pressure controller uses only one sensor; when it fails, the pressure is not controlled.

• The same sensor is used for control and alarming. Therefore, the alarm provides no additional protection for this initiating cause.

• No safety valve is provided (which is a serious design flaw).

• No SIS is provided for the system. (No SIS would be provided for a typical design.)
Solution: Original design.

When the connection to the sensor is plugged, the controller and alarm will fail to function on demand.

Feed
- Methane
- Ethane (LK)
- Propane
- Butane
- Pentane

Process fluid
- T1
- FC-1
- T2
- F2
- T5
- T3
- F3

Steam
- T1
- F2
- F3

L. Key
- TC-6
- PC-1
- PA
- PC-1

Vapor product
- Liquid product
- LAL
- LAH
Solution using initial design and typical published values.

<table>
<thead>
<tr>
<th>Consequence &amp; Severity</th>
<th>Initiating event (cause)</th>
<th>Initiating event frequency /year</th>
<th>Preventive independent protection layers Probability of failure on demand (PFD)</th>
<th>Mitigated event likelihood /year</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Pressure Connection (tap) for sensor P1 plugged</td>
<td>0.1</td>
<td>0.1</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Much too high! We must make improvements to the design.**

Gap = $10^{-2}/10^{-5} = 10^3$ (sometimes given as the exponent “3”)
LOPA Examples: Improved Design

Feed
Methane
Ethane (LK)
Propane
Butane
Pentane

Process fluid
Steam

Vapor product

Liquid product

L. Key
## LOPA Examples: Improved Design

### Consequence & Severity

<table>
<thead>
<tr>
<th>Initiating event (cause)</th>
<th>Initiating event frequency /year</th>
<th>Preventive independent protection layers probability of failure on demand (PFD)</th>
<th>Mitigated event likelihood /year</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Pressure</td>
<td>Connection (tap) for sensor P1 plugged</td>
<td>0.1</td>
<td>0.1</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Enhanced design includes separate P sensor for alarm and a pressure relief valve.

The enhanced design achieves the target mitigated likelihood.

Verify table entries.
For the solution in the LOPA table and process sketch, describe some situations (equipment faults) in which the independent layers of protection are

- Independent
- Dependent

Hints: Consider faults such as sensor, power supply, signal transmission, computing, and actuation

For each situation in which the IPLs are dependent, suggest a design improvement that would remove the common cause fault, so that the LOPA analysis in the table would be correct.
The most common are BPCS, Alarms and Pressure relief. They are typically provided in the base design.

The next most common is SIS, which requires careful design and continuing maintenance.

The probability of failure on demand for an SIS depends on its design. Duplicated equipment (e.g., sensors, valves, transmission lines) can improve the performance.

A very reliable method is to design an “inherently safe” process, but these concepts should be applied in the base case.
The safety interlock system (SIS) must use independent sensor, calculation, and final element to be independent!

We desire an SIS that functions when a fault has occurred and does not function when the fault has not occurred.

SIS performance improves with the use of redundant elements; however, the systems become complex, requiring high capital cost and extensive ongoing maintenance.

Use LOPA to determine the required PFD; then, design the SIS to achieve the required PFD.