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)
• 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
### 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</th>
<th>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>
<td></td>
</tr>
</tbody>
</table>

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

\[
= f_i^I \times PFD_{i1} \times PFD_{i2} \cdots \times PFD_{ij}
\]

- \(f_i^C\) = frequency for consequence C for initiating event i
- \(f_i^I\) = frequency requeency for initiating event i
- \(PFD_{ij}\) = probability of failure on demand of the jth IPL that protects against consequence C for initiating event i
## Typical Initiating Cause Likelihood

<table>
<thead>
<tr>
<th>Initiating Cause</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control loop failure</td>
<td>$1.0 \times 10^{-2}$ events per year</td>
</tr>
<tr>
<td>Relief valve failure</td>
<td>$1.0 \times 10^{-2}$ events per year</td>
</tr>
<tr>
<td>Human Error (trained, no stress)</td>
<td>$1.0 \times 10^{-2}$ events per number of times task was done</td>
</tr>
<tr>
<td>Human Error (under stress)</td>
<td>0.5 to 1.0</td>
</tr>
<tr>
<td>Other initiating events</td>
<td>Use experience of personnel, e.g., CTW pumps trip twice a year, total power failure once every two years.</td>
</tr>
</tbody>
</table>
## Typical Initiating Event Frequency

<table>
<thead>
<tr>
<th>Event</th>
<th>Estimated Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of cooling</td>
<td>1/year</td>
</tr>
<tr>
<td>(Standard simplex system)</td>
<td></td>
</tr>
<tr>
<td>Loss of power</td>
<td>1/year</td>
</tr>
<tr>
<td>(Standard simplex system)</td>
<td></td>
</tr>
<tr>
<td>Human error</td>
<td>1/year</td>
</tr>
<tr>
<td>(Routine, once per day opportunity)</td>
<td></td>
</tr>
<tr>
<td>Human error</td>
<td>1/10 years</td>
</tr>
<tr>
<td>(Routine, once per month opportunity)</td>
<td></td>
</tr>
<tr>
<td>Basic process control loop failure</td>
<td>1/10 years</td>
</tr>
<tr>
<td>Large fire</td>
<td>1/100 years*</td>
</tr>
<tr>
<td></td>
<td>1/1,000 years</td>
</tr>
</tbody>
</table>

*Fire frequency for an individual process system of 1/100 years is conservative.*
Layers of Protection

- Pressure Relief Devices
- Flare Systems
- Fire Suppression Systems
- Safety Instrumented System (SIS) or Emergency Shutdown System
- Automatic action safety interlock system
- Basic controls, critical alarms
- Community emergency response
- Inherently safe design features
- Operator intervention
- Plant emergency response
<table>
<thead>
<tr>
<th>Independent Protection Layer</th>
<th>PFD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control loop failure</td>
<td>$1.0 \times 10^{-2}$</td>
</tr>
<tr>
<td>Relief valve failure</td>
<td>$1.0 \times 10^{-2}$</td>
</tr>
<tr>
<td>Human Error (trained, no stress)</td>
<td>$1.0 \times 10^{-2}$</td>
</tr>
<tr>
<td>Operator Response to Alarms</td>
<td>$1.0 \times 10^{-1}$</td>
</tr>
<tr>
<td>Vessel pressure rating above maximum challenge from internal and external pressure sources</td>
<td>$10^{-2}$ or better, if vessel integrity is maintained (i.e., corrosion understood, inspections and repairs in place)</td>
</tr>
<tr>
<td>Other events</td>
<td>Use experience of personnel, e.g., CTW pumps trip twice a year, total power failure once every two years.</td>
</tr>
</tbody>
</table>
Implementing LOPA

• One Cause – One Consequence – One Scenario
  – Do not combine consequences or causes

• What is IPL
  – A device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario.
  – Procedure and inspection cannot be considered as IPL
LOPA – 1. Express target quantitatively

- **FAR**: Fatal Accident Rate - This is the number of fatalities occurring during 1000 working lifetimes ($10^8$ hours). This is used in the U.K.

- **Fatality Rate** = FAR * (hours worked) / $10^8$

- **OSHA Incidence Rate** - This is the number of illnesses and injuries for 100 work-years. This is used in the USA.
FAR Data for typical Activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>FAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chemical Industry</td>
<td>4</td>
</tr>
<tr>
<td>Steel Industry</td>
<td>8</td>
</tr>
<tr>
<td>Coal Mining</td>
<td>40</td>
</tr>
<tr>
<td>Construction</td>
<td>67</td>
</tr>
<tr>
<td>Uranium</td>
<td>70</td>
</tr>
<tr>
<td>Asbestos (old data?)</td>
<td>620</td>
</tr>
<tr>
<td>Staying home</td>
<td>3</td>
</tr>
<tr>
<td>Traveling by automobile</td>
<td>57</td>
</tr>
<tr>
<td>Traveling by airplane</td>
<td>240</td>
</tr>
<tr>
<td>Cigarette smoking</td>
<td>???</td>
</tr>
</tbody>
</table>

What is the fatality rate/year for the chemical industry?

What is FAR for cigarette smoking?
LOPA – 1. Express target quantitatively

• One standard used is to maintain the risk for involuntary activities less (much less?) than typical risks such as “staying home”
  - Results in rules, such as fatality rate $< 10^{-6}$/year
  - See Wells (1996) Table 9.4
  - Remember that many risks exist (total risk is sum)

• Are current risks accepted or merely tolerated?

• We must consider the inaccuracies of the estimates

• We must consider people outside of the manufacturing site.
People usually distinguish between voluntary and involuntary risk. They often accept higher risk for voluntary activities (rock climbing).

People consider the number of fatalities per accident

\[
\text{Fatalities} = (\text{frequency}) \times (\text{fatalities/accident})
\]

\[
.001 = (.001) \times (1) \quad \text{fatalities/time period}
\]

\[
.001 = (.0000001) \times (100,000) \quad \text{fatalities/time period}
\]

We need to consider frequency and consequence
The decision can be presented in a F-N plot similar to the one below.
(The coordinate values here are not “standard”; they must be selected by the professional.)

LOPA – 1. Express target quantitatively

The design must be enhanced to reduce the likelihood of death (or serious damage) and/or to mitigate the effects.
In Level of Protection Analysis (LOPA), we assume that the probability of each element in the system functioning (or failing) is independent of all other elements.

We consider the probability of the initiating event (root cause) occurring.

We consider the probability that every independent protection layer (IPL) will prevent the cause or satisfactorily mitigate the effect.
LOPA – 2. Determine the risk for system

X is the probability of the event

Y_i is the probability of failure on demand (PFD) for each IPL

Initiating event, X

Unsafe, Y_1

Unsafe, Y_2

Unsafe, Y_n

Unsafe

Safe/tolerable
Recall that the events are considered independent.

The probability that the unsafe consequence will occur is the product of the individual probabilities.

\[ P_{\text{consequence}} = (X) \left( \prod_{i=1}^{n} Y_i \right) \]
The Layer of Protection Analysis (LOPA) is performed using a standard table for data entry.

Likelihood = X

Probability of failure on demand = Yi

Mitigated likelihood = \( (X)(Y_1)(Y_2) \cdots (Y_n) \)

<table>
<thead>
<tr>
<th>#</th>
<th>Initial Event Description</th>
<th>Initiating cause</th>
<th>Cause likelihood</th>
<th>Process design</th>
<th>BPCS</th>
<th>Alarm</th>
<th>SIS</th>
<th>Additional mitigation (safety valves, dykes, restricted access, etc.)</th>
<th>Mitigated event likelihood</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How do we determine the initiating events?

How do we determine the probability of the initiating event, X?

How do we determine the probability that each IPL will function successfully?

How do we determine the target level for the system?
Some typical protection layer Probability of Failure on Demand (PFD)

- BPCS control loop = 0.10
- Operator response to alarm = 0.10
- Relief safety valve = 0.001
- Vessel failure at maximum design pressure = $10^{-4}$ or better (lower)

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.)
The general approach is to

- Set the target frequency for an event leading to an unsafe situation (based on F-N plot)
- Calculate the frequency for a proposed design
- If the frequency for the design is too high, reduce it
  - The first approach is often to introduce or enhance the safety interlock system (SIS) system
- Continue with improvements until the target frequency has been achieved
The Layer of Protection Analysis (LOPA) is performed using a standard table for data entry.

<table>
<thead>
<tr>
<th>#</th>
<th>Initial Event Description</th>
<th>Initiating cause</th>
<th>Cause likelihood</th>
<th>Process design</th>
<th>BPCS</th>
<th>Alarm</th>
<th>SIS</th>
<th>Additional mitigation (safety valves, dykes, restricted access, etc.)</th>
<th>Mitigated event likelihood</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Likelihood = X

Probability of failure on demand = Yi

Mitigated likelihood = (X)(Y1)(Y 2) •• (Yn)
Class Exercise 1: Flash drum for “rough” component separation for this proposed design.
**LOPA – Process Example**

Class Exercise 1: Flash drum for “rough” component separation. Complete the table with your best estimates of values.

<table>
<thead>
<tr>
<th>#</th>
<th>Initial Event Description</th>
<th>Initiating cause</th>
<th>Cause likelihood</th>
<th>Protection Layers</th>
<th>BPCS</th>
<th>Alarm</th>
<th>SIS</th>
<th>Additional mitigation (safety valves, dykes, restricted access, etc.)</th>
<th>Mitigated event likelihood</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High pressure</td>
<td>Connection (tap) for pressure sensor P1 becomes plugged</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assume that the target mitigated likelihood = $10^{-5}$ event/year
Class Exercise 1: 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.)
# LOPA – Process Example

## Class Exercise 1: Solution using initial design and typical published values.

<table>
<thead>
<tr>
<th>#</th>
<th>Initial Event Description</th>
<th>Initiating cause</th>
<th>Cause likelihood</th>
<th>Process design</th>
<th>BPCS</th>
<th>Alarm</th>
<th>SIS</th>
<th>Additional mitigation (safety valves, dykes, restricted access, etc.)</th>
<th>Mitigated event likelihood</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High pressure</td>
<td>Connection (tap) for pressure sensor P1 becomes plugged</td>
<td>0.10</td>
<td>0.10</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td>.01</td>
<td>Pressure sensor does not measure the drum pressure</td>
</tr>
</tbody>
</table>

**Much too high! We must make improvements to the design.**
### Class Exercise 1: Solution using enhanced design and typical published values.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Initial Event Description</td>
<td>Initiating cause</td>
<td>Cause likelihood</td>
<td>Process design</td>
<td>BPCS</td>
<td>Alarm</td>
<td>SIS</td>
<td>Additional mitigation (safety valves, dykes, restricted access, etc.)</td>
<td>Mitigated event likelihood</td>
<td>Notes</td>
</tr>
<tr>
<td>1</td>
<td>High pressure</td>
<td>Connection (tap) for pressure sensor P1 becomes plugged</td>
<td>0.10</td>
<td>0.10</td>
<td>1.0</td>
<td>0.10</td>
<td>1.0</td>
<td>PRV 0.01</td>
<td>.00001</td>
<td>Pressure sensor does not measure the drum pressure</td>
</tr>
</tbody>
</table>

Enhanced design includes separate P sensor for alarm and a pressure relief valve. Sketch on process drawing.

The enhanced design achieves the target mitigated likelihood. Verify table entries.
LOPA – Process Example

Class Exercise 1: Solution.

Feed
Methane
Ethane (LK)
Propane
Butane
Pentane

Process fluid
Steam
L. Key

Vapor product
Liquid product

Split range
cascade

TC-6
PC-1

P-2
PAH

LAL
LAH

F1
FC-1

T1
T2
T5
T3

F2
F3

AC-1

LOPA – Process Example

Class Exercise 1: Solution.

Feed
Methane
Ethane (LK)
Propane
Butane
Pentane

Process fluid
Steam
L. Key

Vapor product
Liquid product

Split range
cascade

TC-6
PC-1

P-2
PAH

LAL
LAH

F1
FC-1

T1
T2
T5
T3

F2
F3

AC-1
Class Exercise 1: Each IPL must be independent.

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 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.
LOPA – Approaches to reducing risks

• 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.
LOPA – Approaches to reducing risks

• The safety instrumented 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.
LOPA – Approaches to reducing risks

Performance for the four SIL’s levels for a safety interlock system (SIS)

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Probability of Failure on Demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL-1</td>
<td>0.10 to 0.001</td>
</tr>
<tr>
<td>SIL-2</td>
<td>0.01 to 0.001</td>
</tr>
<tr>
<td>SIL-3</td>
<td>0.001 to 0.0001</td>
</tr>
<tr>
<td>SIL-4</td>
<td>Less than 0.0001</td>
</tr>
</tbody>
</table>
LOPA – Approaches to reducing risks

Two common designs for a safety interlock system (SIS)

- **1 out of 1** must indicate failure
  - T100
  - Failure on demand
  - False shutdown
  - 5 x 10^{-3} 5 x 10^{-3}

- **2 out of 3** must indicate failure
  - T100, T101, T102
  - Same variable, multiple sensors!
  - 2.5 x 10^{-6} 2.5 x 10^{-6}

Better performance, more expensive
Class Exercise 2: Fired heater to increase stream’s temperature.
# Initial Event Description
Initiating cause
Cause likelihood
Process design
BPCS
Alarm
SIS
Additional mitigation (safety valves, dykes, restricted access, etc.)
Mitigated event likelihood
Notes

Comestibles in stack, fire or explosion
Limited air supply because air blower reaches maximum power

All equipment is functioning properly in this scenario. The feed rate is very high, beyond its design value.


Melhem, G. and P. Stickles, How Much Safety is Enough, Hydrocarbon Processing, 1999