Effective Layers of Protection Analysis

Building upon Qualitative Risk Assessments
Keith Jackson, Managing Director
ETEC Consulting Group, LLC

- Process Safety and Risk Mgmt
- OSHA & EPA Compliance
- Operational Improvements
- Enhance Mechanical Integrity
- 34 yrs industry / 24 yrs PSM
- 5 continents / 20 countries
- Support clients in Exploration, Refining, Chemicals, Pipeline sectors.
- BP, ConocoPhillips, Shell, Tesoro, Valero, National Oil Companies worldwide.
Agenda

• Workshop Objectives
• Inherent hazards of Oil & Gas industry
• What is LOPA?
• LOPA Overview
• Making LOPA more effective
• What to do upon return to plant
LAYERS OF PROTECTION
You NEED Them

HERE'S WHAT HAPPENED......

During a non-routine procedure, materials were transferred into a vessel. A number of items were present (i.e., "layers of protection") to prevent vessel damage, including:

- A high pressure alarm (in this case, the alarm was acknowledged earlier when it was assumed to be caused by a faulty instrument)
- A pressure control system which allows pressure to be vented to another system in the area (in this case, this "second system" was out of service), and
- A pressure relief/vacuum system which vents to the atmosphere (this system contained a flame arrester which was found to be plugged).
- The net result of all these failures was a ruptured roof on the tank

What do layers of protection accomplish?

- A well designed facility includes multiple items of protection for equipment;
- These frequently include a number of the following: operator monitoring, procedures, alarms, interlocks, pressure-rated equipment and relief/vacuum valves, and
- In most cases, multiple systems must fail before vessel damage occurs
Pascagoula Gas Plant
Explosion & Fire
June 27, 2016
Elements of Basic Risk Assessment

Risk Understanding and Analysis

What impact is possible?

What can go wrong?

How likely is “IT” to occur?

WORST PLAUSIBLE CONSEQUENCE.

INITIATING EVENT, Or CAUSE

“IT’S” OCCURRENCE IS BASED ON PROTECTION LAYERS.
## Qualitative –vs- Semi-Quantitative

<table>
<thead>
<tr>
<th></th>
<th>Historical Records</th>
<th>Analytics Employed</th>
<th>Knowledge &amp; Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAZOP</td>
<td>Med</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>LOPA</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
What is LOPA?

- Semi-quantitative risk assessment method
- Adequacy of IPLs to prevent or mitigate consequence
- Determine if scenarios are within risk tolerance
- Determine the required SIL of a SIF, if required.

**Note**: The goal is to prevent or mitigate the high severity consequences, and not to implement expensive Safety Instrumented Systems (SIS), unless absolutely required.
Enhancements with LOPA

• Build upon qualitative analysis
• Based on statistical analytics
• Input cause frequency
• Use frequency modifiers
  – Time at Risk
  – Occupancy
  – Ignition Probability
• Validate independence

• Use PFD for LOP
• Validate LOP are available
• Define Risk Gaps quantitatively
• Close Risk Gaps with an instrumented device of a specific SIL.
LOPA Process

Define High Severity Consequences

Determine TMEL

Define Initiating Events & Frequency

IPL & PFD, with modifiers

Determine RRF

Deliverables: Risk Reduction Factor, need for SIS
LOPA Resource

- CCPS Concept Book
- Industry Resource
- www.ccpsonline.org
LOPA Governing Equation

Risk Reduction Factor  = \[ \frac{[IEF \times PFD_1 \times PFD_2 \times PFD_3 \ldots] \times P_{tr} \times P_p \times P_i}{TMEL} \]

RRF = Mitigations Frequency / Defined Risk Tolerance

If Risk Reduction Factor \( \geq 1 \)

No special integrity measures required

If Risk Reduction Factor \( < 1 \), additional IPLs required

Note: Incremental IPL may or may not be SIS
Making LOPA More Effective

1. Hazard Scenarios - What to include or exclude
2. Overstating hazards, protection layers and likelihoods
3. Using Frequency Modifiers effectively
4. Layers of Protection availability via MIP
Consequence Severity

- Scenarios developed in HAZOP or HAZID.
- **Common Error #1**: High pressure in vessel exceeding MAWP, leading to vessel rupture, loss of containment, fire with possible fatality.
- All pressure excursions do not lead to worst case of vessel rupture & fatality.
- **Common Error #2**: Pressure excursion in vessel leading to relief valve lifting. No significant safety conseq.
- The relief valve is an active safeguard. It has a certain PFD. For instance, it will not respond when called up 1 out of 100 times.
- The relief valve is a LOP. Consequence is defined based on pressure.
# Vessel Pressure Excursion

<table>
<thead>
<tr>
<th>% MAWP</th>
<th>Consequence</th>
<th>Severity</th>
<th>Probability</th>
<th>Vessel failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;= 2xMAWP</td>
<td>Flange leaks, jet fire</td>
<td>Moderate</td>
<td>0%</td>
<td></td>
</tr>
<tr>
<td>&gt;2 – 3xMAWP</td>
<td>Vessel damage</td>
<td>Moderate</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>3 to 3.5xMAWP</td>
<td>Severe Vessel damage</td>
<td>High</td>
<td>10%</td>
<td></td>
</tr>
<tr>
<td>&gt;3.5xMAWP</td>
<td>Catastrophic Vessel rupture</td>
<td>Very High</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
1. Define max pressure at vessel, due to reverse flow or high pressure blow through.
2. Calculate the maximum overpressure and define worst plausible consequence.
## Piping Pressure Excursion

<table>
<thead>
<tr>
<th>ANSI Rating</th>
<th>MAOP Non-shock</th>
<th>Hydro Pressure</th>
</tr>
</thead>
<tbody>
<tr>
<td>150</td>
<td>285 psig</td>
<td>428 psig</td>
</tr>
<tr>
<td>300</td>
<td>740 psig</td>
<td>1,110 psig</td>
</tr>
<tr>
<td>600</td>
<td>1,480 psig</td>
<td>2,220 psig</td>
</tr>
</tbody>
</table>

### Notes:
1. From ANSI B16.5 and ASTM A-105, Carbon Steel, Group 1.1, pipe flanges and fittings.
2. Based on temperature up to 100 degF.
3. Hydrotest performed at ambient conditions.
4. Pressure excursion must exceed maximum allowable non-shock pressure before any measurable consequence will be seen.
TMEL and Initiating Events

- Acceptable risk tolerance
- Defined by Corporate based on all plants.
- For instance:
  - An explosion that results in a fatality may have a risk tolerance of $1 \times 10^{-4}$ years.

- Initiating Events are identified in the HAZOP.
- Fall into 3 categories:
  - Equipment failure
  - Operator Error *
  - External events
- Actual failure frequency may be used
Not Typically LOPA’ble

- Escalation events
- General Fires
- Escape & Evacuation
- Control of Work
- Mechanical Integrity
- Occupational Safety
- Design Errors
- “Acts of God”
- Terrorism or sabotage
Frequency Modifiers: $P_{tr}$ & $P_p$

- Hazard present during certain operation or tasks.
- $P_{tr} = \frac{\text{Time at Risk}}{\text{total time}}$
- **Example:** Reactor batch operation where heat-up cycle is 2 hours each day. The hazard is potential decomposition during heatup cycle.
  
  $$P_{tr} = \frac{2\text{hrs}}{24 \text{ hrs}} = 0.0833$$

- Occupy hazard zone.
- $P_p = \frac{\text{Time in hazard}}{\text{total time}}$
- **Example:** The operator may be near the pump for 30 minutes out of their shift. In this case the occupancy factor is:
  
  $$P_p = \frac{0.5\text{hr}}{12 \text{ hrs}} = 0.04$$
Frequency Modifiers: \( P_i \)

• A fire or explosion hazard must be ignited.
• The following factors are suggested to used as probability of ignition given a release:
  – \( P_i = 1.0 \), auto-ignition or pyrophoric materials
  – \( P_i = 0.1 \), heavy oils
  – \( P_i = 0.2 \), volatile liquids
  – \( P_i = 0.3 \), flammable liquids/gas
Using Frequency Modifiers

• Be cautious when applying $P_{tr}$ & $P_p$. You can understate risk.

• If risk is present during a limited time, and the operator is present all that time, then $P_p = 1$. Don’t double dip!
Identifying IPLs

IPL is a device, system or action that is capable of preventing a scenario from progressing to the undesired consequence regardless of the initiating event or the performance of any other protection layer associated with the scenario.

• Two Classes of IPLs
  – Active: BPCS, human response to alarm, PSV, SIS.
  – Passive: Dike, open vent, blast wall/bunker, flame/detonation arrestors and restriction orifice.

• Start with HAZOP safeguards
• Some HAZOP safeguards will not meet the criteria for IPL’s
Independent Protection Layer Rules

- Designed to **prevent or mitigate** consequences of hazardous scenario.
- Must be **dependable**, and can be counted on to perform as intended.
- Can be **audited** to confirm performance.
- Must be **independent** of other IPL’s or initiated event.
Types of IPL’s

- BPCS
- Operator Response to Alarm
- SIS
- Relief Devices
- NOT >> Check Valves
PFD from Failure Rate

• PFD is probability of failure upon demand
• PFD depends on failure rate, failure mode and test interval
• Failure rate is divided into failures that cause failure on demand
• Most databases list the failure mode for an equipment item
• An untested device’s PFD gets larger as time increases at an exponential relationship.

\[ -\lambda t \]
LOPA Governing Equation

Risk Reduction Factor = \[
\frac{[\text{IEF} \times \text{PFD1} \times \text{PFD2} \times \text{PFD3} \ldots] \times \text{Ptr} \times \text{Pp} \times \text{Pi}}{\text{TMEL}}
\]

**TMEL:**
High pressure in vessel exceeding MAWP due to pressure regulator malfunctions. Possible vessel rupture, loss of containment, fire with possible fatality.

**TMEL = 1x10^{-4}**

**Mitigations:**
- IEF = 1x10^{-1} Instrument (regulator) fails
- PDF1 = 1x10^{-2} Relief Device
- \( P_p = 0.1 \) Random Occupancy
WHAT TO DO BACK AT YOUR PLANT?
For More Information:
Keith M. Jackson
keith@eteconsulting.com
www.eteconsulting.com
909-573-8002