Risk Analysis Using Layer of Protection Analysis

Kelsey Forde CIH CHMM
Owner, Principal EHS Professional
klforde@parvaticonsulting.com
(505)967-8917

Timothy Stirrup REM
Principal EHS Professional
tsstirrup@parvaticorp.com
(505)980-3743

Parvati Consulting LLC
...a woman-owned small business...
www.parvaticorp.com
ExxonMobil Refinery Explosion

- ExxonMobil Refinery Explosion
- Torrance, CA 2015

Discussion

- **ExxonMobil Refinery Explosion**
  - Controls
  - Assignment of Values
  - Hierarchy Analysis


Layer of Protection Analysis (LOPA)

- LOPA History
- LOPA Defined
- LOPA Common Elements
- LOPA Use - Motivating Factors
- LOPA Steps
- LOPA Limitations/Benefits
- LOPA References
LOPA History

- Origin with Company Specific Development
- Parallel Development of Safety Integrity Levels (SIL)
- Multiple Papers Published ~ 1997
- Center for Chemical Process Safety
  - Internal Conference ~ 1997
  - Workshop ~ 2000
  - LOPA Concept Book ~ 2001
  - "Redbook" Incorporation ~ 2008
LOPA Purpose

- Replace Quantitative Risk Assessment
- Determine if Sufficient Layers of Controls
- Use of LOPA as Semi Quantitative Hazard Evaluation Tool for Judging Risk of Accident Scenarios
- Risk Analysis Tool that Must be Applied Correctly
LOPA Defined

- Simplified Method of Risk Assessment
  - Semi-Qualitative
  - Semi-Quantitative
  - Intermediate Between Qualitative and Quantitative

- Simplified Rules to Evaluate Scenario Impacts
  - Initiating Cause Frequency
  - Independent Layers of Protection

- Provide Order of Magnitude Risk Estimate
Layer of Protection Analysis
Qualitative vs Quantitative
LOPA Defined

- Qualitative Hazard Evaluation Techniques
  - Generalized Cause - Consequence, Loss Events, and Assignment of Preventative or Mitigative Controls

- Quantitative Hazard Evaluation Techniques
  - Assigned Failure Rates for Equipment/Controls Using Ever Increasing Detail for Site/Industry

- Layer of Protection Analysis
  - Order of Magnitude Estimates of Cause Frequency & Control Effectiveness
  - Control Effectiveness = Independent Layers of Protection (IPL)
LOPA Defined

- Traditional Hazards Analysis Looks at Entire System or Process
  - Qualitative - What If, What-If/Checklist, HazOp
  - Quantitative - Fault Tree, Event Tree, QRA

- LOPA Looks at Individual Scenario

- Applied After Traditional Methods
  - Narrow Focus on Important Events
  - Derived Significant Controls
LOPA Defined

- Simplified Form of Risk Assessment
- Order of Magnitude Categories
  - Event Frequency
  - Consequence Severity
  - Likelihood of Failure of Independent Protection Layers (IPL)
- Builds On Qualitative Hazards Analysis ~ Semi Quantitative/Qualitative
- Rule-Based Implementation
Common Elements

- Consequence Classification Method
  - Typically Company Specific
  - Use of Standard Consequence Table
  - Derived from Qualitative HE

- Numerical Risk Tolerance Criteria
  - Fatalities & Fire Frequencies
  - Required Number of IPL Credits
  - Maximum Frequency for Specified Categories

- Method of Developing Scenarios
Common Elements

- Rules for Controls as IPLs
- Default Frequency Data
  - Event Frequencies
  - Credits for IPLs
- Procedure for Calculation
- Procedure for Application/Acceptance
- Rules for Controls as IPLs
  - Independence
  - Functionality
  - Integrity
  - Reliability
  - Auditability
  - Access Security
  - Management of Change
LOPA Use

- Effectively Used Throughout Safety Life Cycle

- Preferred Use
  - Detailed Design Stages
  - Modifications to Designs

- Techniques Where Defining
  - Control Hierarchy
  - Control Requirements

- Use for Engineering/Administrative Controls
Defense in Depth
LOPA Use

- Typically Performed After Analyzing System with Qualitative Hazard Evaluation (HE) Technique

- Higher Risk Scenario
  - Decision Quality Requires Increased Clarity

- Risk = Frequency x Consequence
  - Higher Consequence Requires Higher Confidence to Support Decision Making
  - Narrowed Focus on Frequency Control

- LOPA Uses Common Conservative Frequency and Control Effectiveness Values to Derive Acceptable Risk for a Given Scenario
LOPA Use

- LOPA is a Process to Evaluate Risk with Explicit Risk Tolerance for Specific (Higher) Consequences

- Support Rationale “Risk Based” Business Decisions

- Creating Value without Taking Unnecessary Risk

- Tolerable Frequency is Decision Criterion for Design and Operational Changes
Use of LOPA

- Tolerable Frequency is Decision Criteria for Design and Operational Changes

- Allocate Proportionate Resources Commensurate with Risk

- Higher Consequence - Lower Tolerable Frequency

- Acceptable Risk = Risk Tolerance

- Company Decisions Based On Risk Tolerance
LOPA Steps

- Step 1 - Analyze Single Event/Consequence
  - Specific Hazard, Receptor, & Consequence
- Step 2 - Determine Tolerable Frequency
- Step 3 - Assess Probability of Initiating Events
- Step 4 - Identify Independent Protection Layers (IPLs)
- Step 5 - Calculate Expected Frequency
  - Initiating Event x Failure of Safeguards
- Step 6 - Determine Safeguards
- Step 7 - Determine Residual Risk
- Step 8 - Apply Safeguards Until Acceptable Risk
# LOPA Worksheet

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Probability</th>
<th>Frequency (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiating Event</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabling Event or Condition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conditional Modifiers (If applicable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability of ignition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability of personnel in affected area</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability of fatality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequency of Unmitigated Consequence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Independent Protection Layers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safeguards (non-IPLs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total PFD for all IPLs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequency of Mitigated Consequence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Tolerance Criteria:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions Required:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>References:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality Review:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LOPA Steps

Event Side
- Identify Unacceptable Consequence
- Screen Events Against Consequence
- Determine Event Frequency

Control Side
- Identify IPLs
- Identify Probability of IPL Failure
- Add Controls to Tolerable Risk

Event Side - Control Side = Residual Risk
Event Side - Control Side = Acceptable Risk
# Failure Rates

- **Standard Industry Values**
- **Standard Corporate Values**
- **Comparable**
- **Common Risk Decisions**

## Table 5.1

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>Frequency Range from Literature (per year)</th>
<th>Example of a Value Chosen by a Company for Use in LOPA (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressure vessel residual failure</td>
<td>$10^{-5}$ to $10^{-2}$</td>
<td>$1 \times 10^{-6}$</td>
</tr>
<tr>
<td>Piping residual failure $-100$ m $-$ Full Breach</td>
<td>$10^{-5}$ to $10^{-3}$</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>$10^{-5}$ to $10^{-3}$</td>
<td>$1 \times 10^{-3}$</td>
</tr>
<tr>
<td>Gasket/packing blowout</td>
<td>$10^{-5}$ to $10^{-4}$</td>
<td>$1 \times 10^{-2}$</td>
</tr>
<tr>
<td>Turbine/diesel engine overspeed with casing breach</td>
<td>$10^{-5}$ 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>$10^{-2}$ to $10^{-4}$ per lift</td>
<td>$1 \times 10^{-4}$ per lift</td>
</tr>
<tr>
<td>Lightning strike</td>
<td>$10^{-2}$ 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/leading hose failure</td>
<td>$1$ to $10^{-3}$</td>
<td>$1 \times 10^{-1}$</td>
</tr>
<tr>
<td>BPCS instrument loop failure *Note: IEC 61511 limit is more than $1 \times 10^{-1}$ \text{hr or 8.76 x 10^{-2}} \text{yr} (IEC, 2001)</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 $10^{-4}$</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 (look-out tag-out) procedure* failure</td>
<td>$10^{-5}$ to $10^{-4}$ per opportunity</td>
<td>$1 \times 10^{-3}$ per opportunity</td>
</tr>
<tr>
<td>*overall failure of a multiple-element process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operator failure (to execute routine procedure, assuming well trained, unstressed, not fatigued)</td>
<td>$10^{-3}$ to $10^{-3}$ per opportunity</td>
<td>$1 \times 10^{-3}$ per opportunity</td>
</tr>
</tbody>
</table>

*Note: Individual companies should choose their own values, consistent with the degree of conservatism of the company’s risk tolerance criteria. Failure rates can also be greatly affected by preventive maintenance (PM) routines.*
Independent Protection Layer

- Independent from the Initiating Event
- Independent from other IPLs/Safeguards
LOPA IPL Values

- Standard Industry Values
- Standard Corporate Values
- Comparable
- Common Risk Decisions

6. Identifying Independent Protection Layers

can be credited as IPLs with a high level of confidence and will significantly reduce the frequency of events with potentially major consequences. However, there may be other, less serious consequences (such as a fire in dike, blast damage to some equipment) that should be analyzed in other scenarios.

Fireproofing is a means of reducing the rate of heat input to equipment (e.g., when considering the sizing basis for relief valves, for preventing a boil-

<table>
<thead>
<tr>
<th>TABLE 6.3 Examples of Passive IPLs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPL</strong></td>
</tr>
<tr>
<td>Dike</td>
</tr>
<tr>
<td>Underground Drainage System</td>
</tr>
<tr>
<td>Open Vent (no valve)</td>
</tr>
<tr>
<td>Fireproofing</td>
</tr>
<tr>
<td>Blast-wall/Bunker</td>
</tr>
<tr>
<td>&quot;Inherently Safe&quot; Design</td>
</tr>
<tr>
<td>Flame/Detonation Arrestors</td>
</tr>
</tbody>
</table>
Benefits

- Simplified Framework for Understanding Risk
- Defensible Process/Procedure
- Less Time Than Quantitative Risk Analysis
- Defines Safety Integrity Levels
- Defines Hierarchy of Controls
- Means of Comparing Risk
Limitations

- Internal Risk Comparisons Valid Only When Using Same LOPA Method
- Result Values Are Not Precise
- Should Not Be Applied to All Scenarios
- Time/Resource Commitment
- Not Hazard Identification/Evaluation Tool
- External Risk Comparisons Not Typically Valid
References

- Guidelines for Hazard Evaluation Procedures, 3rd Ed; CCPS 2008

- Layer of Protection Analysis: Simplified Process Risk Assessment; CCPS 2001

- Guidelines for Initiating Events and Independent Layers of Protection Analysis, 1st Ed; CCPS 2014

- Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis; CCPS 2015

- Layer of Protection Analysis; PII 2014
Follow Up with Parvati

➤ Kelsey L. Forde, CIH, CHHM
  ➤ klforde@parvaticorp.com
  ➤ (505) 967-8917

➤ Timothy S. Stirrup, IH, REM
  ➤ tsstirrup@parvaticorp.com
  ➤ (505) 980-3743

➤ www.parvaticorp.com

➤ Systems Safety
➤ Redbook Training
  ➤ Redbook Overview
  ➤ Redbook HE Techniques
    ➤ What-If/Checklist
    ➤ Failure Modes & Effects Analysis
    ➤ Hazard & Operability Analysis
    ➤ Layer of Protection Analysis (LOPA)
    ➤ Risk Analysis
    ➤ Inherent Safety Reviews

➤ Perform Process Hazards Analysis
➤ Compliance Auditing
➤ Facilitate Hazard Evaluations
➤ Peer Review PHA (HI + HE)
➤ STAMP/STPA
➤ Traditional ES&H/IH Services
Redbook DAP Example

See pg 96 for Process Description
Redbook DAP Example

DAP Production System Component List

Ammonia Subsystem
• Ammonia Unloading Station
• Ammonia Storage Tank
• Ammonia Tank Level [L1]
• Ammonia Line Valve [A]
• Ammonia Line Flow Meter [F1]
• Ammonia Lines

Phosphoric Acid Subsystem
• Phosphoric Acid Unloading Station
• Phosphoric Acid Storage Tank
• Phosphoric Acid Tank Level [L2]
• Phosphoric Acid Line Valve [B]
• Phosphoric Acid Line Flow Meter [F2]
• Phosphoric Acid Lines

DAP System

• DAP Reactor
• DAP Mixer
• DAP Reactor Valve [C]
• DAP Storage Tank
• DAP Storage Tank Valve [D]
• DAP Loading Station