Is It Really an Independent Protection Layer?

A. M. (Art) Dowell, III, PE
Chemical Process Safety Consultant

Copyright © 2011 A M Dowell III PE
Art Dowell Bio Sketch

- Principal, AM Dowell III PE
- 42 years, Rohm and Haas Company, now Dow
- BA/BS ChE, Rice University, 1966/1967
- Fellow, AIChE. Member, ISA
- Bill Doyle Award, 1991
- 2002 Albert F. Sperry Founder’s Award from ISA for “outstanding contribution in the development of layer of protection analysis”
Agenda

Why is Independence Important?
- How LOPA math works
- IPL Characteristics & Core Attributes
- Examples
- Conclusion
How LOPA Works -- Unmitigated

Initiating Cause

Freq

Consequence
Inherently Safer

- Reduce or eliminate hazards
- Intensify
- Moderate
- Apply inherently safer concepts to the process design and chemistry.
LOPA Model -- Mitigated

Initiating Cause

Controls

SIFs

RVs

Potential Consequence Frequencies Reduced
Event Tree Model

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>IPL1</th>
<th>IPL1</th>
<th>IPL1</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimated Frequency</td>
<td>$f_i = x$</td>
<td>$PFD_1 = y_1$</td>
<td>$f_1 = x \cdot y_1$</td>
<td>$f_1 = x \cdot y_1 \cdot y_2$</td>
</tr>
</tbody>
</table>
• The mitigated consequence frequency is given by

\[ f_c = f_i \times PFD_1 \times PFD_2 \times \ldots PFD_n \]

where

- \( f_i \) is the frequency of the initiating cause,
- \( PFD_n \) is the probability of failure on demand of the \( n^{th} \) independent protection layer,
- \( f_c \) is the mitigated frequency of the consequence.
- Each protection layer is independent
IPL Characteristics

- Independent protection layers (IPLs) should be
  - unique and applicable,
  - independent,
  - dependable, and
  - auditable

CCPS [2001], *Layer of Protection Analysis: Simplified Process Risk Assessment*
IPL Core Attributes

- Independence
- Functionality
- Integrity
- Reliability
- Auditability
- Access Security
- Management of Change

CCPS [2007] Guidelines for Safe and Reliable Instrumented Protective Systems
Core Attributes

• Independence
  – the performance of a protection layer is not affected by the initiating cause of a hazardous event or by the failure of other protection layers;

• Functionality
  – the required operation of the protection layer in response to a hazardous event;
Core Attributes, Continued

• Integrity
  – related to the risk reduction that can reasonably be expected given the protection layer’s design and management;

• Reliability
  – the probability that a protection layer will operate as intended under stated conditions for a specified time period;
Core Attributes, Continued

• Auditability
  – ability to inspect information, documents and procedures, which demonstrate the adequacy of and adherence to the design, inspection, maintenance, testing, and operation practices used to achieve the other core attributes;

• Access Security
  – use of administrative controls and physical means to reduce the potential for unintentional or unauthorized changes; and
Core Attributes, Continued

• Management of Change
  – formal process used to review, document, and approve modifications to equipment, procedures, raw materials, processing conditions, etc., other than “replacement in kind,” prior to implementation.
Keywords

- **“3 Ds”**
  - Detect
  - Decide
  - Deflect

- **“4 Enoughs”**
  - Big Enough
  - Fast Enough
  - Strong Enough
  - Smart Enough

- The Big “I” – Independent

- Of Initiating Cause
- Of Other IPLs
“3Ds” Example

• Pressure relief valve
  – Spring **Detects** rising pressure
  – Spring **Decides** to open valve
  – Open valve **Deflects** overpressure consequence, if sized correctly.
“4 Enoughs” Examples

• Pressure relief valve is
  – **Big Enough**
  – Opens **Fast Enough**

• Pressure Isolation valve is
  – **Strong Enough** to stop the surge

• Purge system is
  – **Smart Enough** to purge the vessel and then isolate vessel.
Frequent conflicts with the Big “I”

• Using the initiating cause sensor for the protection layer sensor.
• Using the same sensor for two protection layers.
• Using the initiating cause valve for the protection layer final element.
• Using the same final element for two protection layers.
• Using the initiating cause controller for the protection layer logic solver.
• Using the same logic solver for two protection layers (it may be possible to use the same safety-certified PLC as the logic solver for two protection layers if its probability of failure on demand is low enough).
Tank Overflow Example

**Consequence:** overflow of a flammable material

**Cause:** failure of LIC loop (LT1, LIC1, LV1)
Tank Overflow with Op Response?

• “4 Enoughs”
  – Big Enough?
  – Fast Enough?
  – Strong Enough?
  – Smart Enough?

• “The Big I”
  – Independent of Initiating Cause
  – Independent of other IPLs?

Need 10 minutes

Density change?

Red — initiating cause
Magenta — Operator response
Blue — SIF
Op Response NOT Independent

Red — initiating cause
Magenta — Operator response
Blue — SIF
Tank Overflow Example

- Instr. Air Supply
- SIS Valve A
- LV1
- LAH
- LIC1
- SIF
- SH1

- Red — initiating cause
- Magenta — Operator response
- Blue — SIF
Auditability

• "If you never test your IPL, you will find out that it is broken when your plant blows up."
Auditability

• Test equipment?

Instr. Air Supply → SIS Valve A → SIF

From process-wetted sensor element to process-wetted final element
Auditability

• Test the operator response?
  – Every shift?
  – Relief operators?
  – Manual valve?

• Procedures available & current?
Auditability

• “Procedures are subject to a form of corrosion more rapid than that which affects steel; they can vanish without a trace once management stops taking an interest in them. . . .”

-- Trevor Kletz
Access Security

- Who has access to the configuration of the logic solver that annunciates the high level alarm?
Access Security

• What are the procedures to ensure that the set point for an analogue high level alarm is not changed?
Access Security

• What are the procedures to ensure that the high level alarm is not disabled or inhibited?

LAH ___
❎ Disabled
❎ Inhibited
Management of Change

Don’t Increase the Risk!

• Tank LAH
  – In future, a process improvement specialist may ask, “Why is the set point for this alarm so low? We could be using a lot more of the volume of this tank.”

• The management of change system must be able
  – to retrieve the specifications for the operator response to high-level alarm IPL,
  – to recognize that the alarm set point provides sufficient time for the operator to make the response, and
  – to retain the required setting for a manual response or to automate the response for a higher set point.
Spreadsheet to Test IPL Attributes

• Do candidate protection layers (safeguards) meet the requirements?

• Consider a spreadsheet
  – characteristics of IPLs for each candidate IPL
  – Versus
  – scenarios

• Can be useful where
  – there are a number of existing safeguards, and
  – the historical culture has assumed that the safeguards are sufficient.
<table>
<thead>
<tr>
<th>Scenarios</th>
<th># of Safeguards that meet IPL criteria</th>
<th>Safeguard 1</th>
<th>Safeguard 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  LIC loop failure overfills tank with release</td>
<td>1</td>
<td>Operate response to alarm from level control loop sensor</td>
<td>Operator response to alarm from fixed point level probe</td>
</tr>
<tr>
<td>2  Fluid in tank has lighter density than specified in level transmitter design, overfills tank with release</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
1. If the LIC loop sensor fails, it cannot detect. If the LIC controller fails, it may not be able to annunciate the alarm.
2. Not independent of the operator response to alarm from the fixed point level probe.
3. Ensure there is at least 10 minutes for the operator to respond to the high level alarm at the maximum fill rate.
• “It’s time to take our own data!”
  – Relief valves
    • Inspect and document inlet and outlet nozzle
    • “Pre-pop” test before rebuild
  – SIS: “as found, as left”
    • Sensors
    • Valves
    • Logic
  – Operator Response to Alarm
    • Annunciation
    • Each operator
    • Final element
Audit features with potential to disable IPLs
  - Block valves around relief devices
    • Tagged, locked, or “car sealed”
  - Bypasses around SIF shut-down valves
    • Tagged, locked, or “car sealed”

Record deviations from the required configuration

Modify the calculated PFD (probability of failure on demand)

If needed, add more protection layers.
Does your experience support the risk reduction assumed in the LOPA?

- If no, then add more layers
- Do root cause analysis to improve the performance of existing layers
• Listen to the voice of the process
  – Log and investigate every activation of an IPL
    • Relief valve opening
    • SIF trip
    • Operator response to alarm
    • These are “near misses”
  – Modify equipment and procedures to avoid challenges to the IPLs.
• Avoid “high demand” on the IPLs
  – That is, challenges to the IPLs of more than once/year, or more than twice in the test interval.
  – In high demand mode, the safety system is being used for basic control. 😞
Observations on Tsunami vs Nuclear Plant

• Nuclear plant shutdown requires active cooling after trip.
  – We prefer IPLs that are
    • Passive
    • De-energize to trip
    • Spring to move to trip state
Observations on Tsunami vs Nuclear Plant

• Beware of common cause!
  – Earthquake caused trip of the reactors – no power generated
  – Earthquake damaged electric grid – no power from off-site
  – Earthquake caused tsunami that damaged back-up generators (located in potentially vulnerable area).
Should LOPAs be Revalidated?

- US OSHA PSM rule requires PHAs (HAZOPs) to be revalidated every 5 years.
- What about the LOPA for my plant?
  - What has changed?
    - Volume?
    - Frequency?
    - Training?
    - Chemicals?
    - Conditions?
Conditional Modifiers

- Time at risk
- Probability of Ignition
- Probability of Person Present
- Probability of Injury

- Easy to double count!
- USE WITH GREAT CARE!!
- Don’t kid yourself!
Conditional Modifiers

• CCPS is writing a guidance book this year.
When to go beyond LOPA

• Protection Layers and Initiating Cause share common elements. – Use Fault Tree Analysis

• Several safeguards can detect the beginning of a scenario but there is only one safeguard that can prevent the scenario from proceeding to the consequence. – Use Event Tree Analysis
References

• Center for Chemical Process Safety (CCPS),
• *Layer of Protection Analysis, Simplified Process Risk Assessment*,
References

• ISA -TR84.00.04, Part 1,
• Guideline on the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511 Mod)
• ISA, 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, North Carolina 27709
  — www.isa.org
References

• Center for Chemical Process Safety (CCPS),

• *Guidelines for Safe and Reliable Instrumented Protective Systems*,

• American Institute of Chemical Engineers, New York, NY, 2007.
  – www.AIChE.org
References

• Center for Chemical Process Safety (CCPS),

• Title to be Determined: “Initiating Event Frequencies and IPL PFDs”

• American Institute of Chemical Engineers, New York, NY, 2011.
  – www.AIChE.org
Conclusion

• Remember the core attributes of IPLs
  – 3Ds
  – 4 Enoughs
  – The Big I

• Use the core attributes to test the IPLs to ensure that the desired risk reduction is achieved.

• Document in the SRS.