

Modifying LOPA for Improved Performance

**Glenn G. Young, CSP
Glenn Young & Associates, LLC PSM Consulting
Baton Rouge, Louisiana**

**Glenn S. Crowe, CSP
Safety Manager
PCS Nitrogen
Geismar, Louisiana**

Introduction

Layers of Protection Analysis (LOPA) is a semi-quantitative risk analysis method that has been popularized by the 2001 book, *Layers of Protection Analysis – Simplified Process Risk Assessment*. This book is offered by the American Institute of Chemical Engineers (AIChE). Finding wide support in the chemical, refining, and pipeline industries, the LOPA process has become a popular tool for assessing risk.

The LOPA process is built upon the principle that process experts in a given industry are cognizant of and accurate in assessing the *severity* of possible process events, but do a poor job of assessing the *likelihood* of these possible process events. Because risk is composed both of severity and likelihood, a divergence in either of the factors gives a skewed assessment of true risk.

LOPA attempts to overcome the inherent “human-nature problem” of misdiagnosing likelihood by taking likelihoods from insurance industry data. Using historical data, the likelihood is more likely to be accurate.

LOPA suffers from a number of shortcomings. Among these is the fact that each LOPA analysis is restricted to a single cause-consequence pair. When multiple causes can instigate the same consequence, multiple LOPA analyses must sometimes be done. When a single cause can instigate multiple consequences, multiple LOPA analyses must sometimes be done.

An additional shortcoming is that LOPA is a coarse tool. LOPA likelihoods are broken down into orders of magnitude change, and exact probabilities are impossible to calculate unless a large amount of field data is available. The Independent Protection Layers (IPLs) that protect against a specific scenario are also given probabilities-of-failure-on-demand (PFDs) that are broken down into orders of magnitude change.

Because LOPA has been so widely adopted over the past five years, and because its penetration of the process industries has been so deep, a broad and deep knowledge base has been developed.

The first consequence of such wide acceptance has been an expansion of LOPA's scope. The original LOPA book provided example tables that gave industry and insurance probabilities of a variety of process events. This table, called "Initiating Event Frequencies" listed such items as "loss of cooling" and "Human Error" without offering much guidance on their application.

Changes to the Initiating Events Table

Many companies were frustrated by the limitations of the Initiating Event Frequency tables and proceeded to expand the number of items in the table. The addition of new causes made the LOPA process more flexible and able to cover more of the scenarios developed in a typical Process Hazards Analysis (PHA).

A typical table in use for 2006 is shown below.

Initiating Event	Example Values /yr
Valves, etc.	
Check valve fails to check fully	1×10^0
Check valve sticks shut	1×10^{-2}
Check valve leaks internally (severe)	1×10^{-5}
Gasket or packing blows out	1×10^{-2}
Regulator fails	1×10^{-1}
Safety valve opens or leaks through badly	1×10^{-2}
Spurious operation of motor or pneumatic valves – all causes	1×10^{-1}
Vessels and Tanks	
Pressure vessel fails catastrophically	1×10^{-6}
Atmospheric tank failure	1×10^{-3}
Process vessel BLEVE	1×10^{-6}
Sphere BLEVE	1×10^{-4}
Small orifice ($\leq 2''$) vessel release	1×10^{-3}
Utility	
Cooling water failure	1×10^{-1}
Power failure	1×10^0
Instrument air failure	1×10^{-1}
Nitrogen (or inerting) system failure	1×10^{-1}
Piping and Hoses	
Loss of containment (flange leak or pump seal leak)	1×10^0
Flex hose leak – minor – for small hoses	1×10^0
Flex hose rupture or large leak – for small hoses	1×10^{-1}
Unloading or loading hose failure – for large hoses	1×10^{-1}
Pipe fails (large release) for $\leq 6''$ pipe	1×10^{-5}
Pipe fails (large release) for $> 6''$ pipe	1×10^{-6}
Piping leak – minor - per each 50 ft.	1×10^{-3}
Piping rupture or large leak – per each 50 ft.	1×10^{-5}
Maintenance Error	
External impact by vehicle (assuming guards are in place)	1×10^{-2}
Crane drops load	1×10^{-3} / # of lifts/yr.
LOTO (Lock-Out Tag-Out) procedure not followed	1×10^{-3} / opportunity
Operator Error	
Operator error - no stress (routine operations)	1×10^{-1}
Operator error – stress (alarms, startup, shutdown, etc.)	1×10^0
Machinery Failure	
Pump bowl failure (varies with material)	1×10^{-3}
Pump seal fails	1×10^{-1}

Initiating Event	Example Values /yr
Pumps and other rotating equipment with redundancy (loss of flow)	1×10^{-1}
Turbine-driven compressor stops	1×10^0
Cooling fan or fin-fan stops	1×10^{-1}
Motor-driven pump or compressor stops	1×10^{-1}
Overspeed of compressor or turbine with casing breach	1×10^{-3}
Instrumentation Failure	
BPCS loop fails	1×10^{-1}
External Events	
Lightning hit	1×10^{-3}
Large external fire (all causes)	1×10^{-2}
Small external fire (all causes)	1×10^{-1}
Vapor cloud explosion	1×10^{-3}

Table 1. This is a typical Initiating Events Table.

Note that a wider variety of causes has been included in Table 1 than was originally provided in the LOPA textbook. LOPA practitioners are also allowed to modify the table values, based on field failure experience or on the number of opportunities for the initiating event to occur. In every case where a modification of the table value is made, the LOPA report for that incident should include a clear and defensible rationale for *why* the table value was modified.

It is best to provide a specific procedure for deviation from the Initiating Events Table values, so that consistency can be achieved over time and over the multiple sites of a company. Each company should strive to provide an internal guidance document so that all sites will be consistent in their application of LOPA initiating event frequencies.

In cases where inconsistency is found in a review of LOPA analyses, some companies ban the modification of the LOPA values for initiating events. Consistency is generally preferable unless there is a strong rationale for exception. Also, in order to maintain consistency, most companies have a procedure for adding new causes to the Initiating Events Table. These new causes and their likelihoods should receive formal review and acceptance before being used.

A formal, periodic review should be made to verify that the Initiating Events table is consistent with not only local field experience but also with wider industry practice. Such verification can be done through internal incident reviews, through industry associations, through employment of outside consultants with experience specific to the LOPA procedures of your industry, or through commercial and insurance databases that are typically available for a fee.

Changes to the IPL Credits Table

Another modification that is coming into common use for LOPA practitioners is the change of the IPL credits table. IPL Credits tables commonly used today no longer use a raw probability-of-failure-on-demand number (PFOD) but a single digit credit number. The original LOPA tables gave PFOD in the same style as the initiating event likelihood (typically 1×10^x). This identical style, in some cases, led inadequately trained LOPA practitioners to misuse the PFOD table values and substitute them for initiating event values. With a different numbering system, such substitution becomes unlikely. In the “credit system” PFOD table, each number represents an

order-of-magnitude reduction in the *likelihood* of the scenario under study. A typical PFOD table commonly in use in 2006 would resemble the following:

IPL CREDITS: (Assumes adequate documentation, training, testing procedures, design basis, and inspection/maintenance procedures)	Credits (PFD)
Passive Protection	
Secondary containment (dikes) or other passive devices	1
Underground drainage system that reduces the widespread spill of a tank overfill/rupture/leak/etc.	2
Open snorkel vent with no valve that prevents overpressure	2
Equipment-specific fireproofing that provides adequate time for depressurizing/firefighting/etc.	2
Blast walls or bunkers that confine explosions and protect equipment/buildings/etc.	3
Vessel MAWP of $\geq 2x$ maximum credible internal or external pressures	2
Flame/detonation arrestors ONLY if properly designed, installed and maintained	2
Active Protection	
Automatic deluge or active sprinkler systems (if adequately designed)	2
Automatic vapor depressuring system (can't be overridden by BPCS)	2
Remotely operated emergency isolation valve(s)	1
Isolation valve designed to fail-safe (can't be overridden by BPCS)	2
Excess flow valve	2
Spring-loaded pressure relief valve	2
Rupture disc (if separate from relief valve)	2
Basic Process Control System can be credited as an IPL ONLY if not part of the initiating event	1
SIL 1 Trip (independent sensor, single logic processor, single final element)	2
SIL 2 Trip (dual sensors, dual logic processors, dual final elements)	3
SIL 3 Trip (triple sensors, triple logic processors, triple final elements)	4
Human Response	
Operator responds to alarms (stress)	1
Operator routine response (trained, no stress, normal operations)	2
Human action with ≤ 10 minute response needed. Simple, well-documented action with clear and reliable indications that action is required	1
Human action with between 10 and 30-minute response needed. Simple, well-documented action with clear and reliable indications that action is required	2

Table 2. This is a typical IPL credits table.

Note that the human response credits are generous in Table 2. Many companies reduce these numbers by one credit each.

Again, companies that choose to modify the IPL Credits table usually have a formal procedure for comment, review and acceptance. A formal, periodic review should be made to verify that the IPL Credits table is consistent with not only local field experience but also with wider industry practice. Such verification can be done through internal incident reviews, through industry associations, through employment of outside consultants with experience specific to the LOPA procedures of your industry, or through commercial and insurance databases that are typically available for a fee.

Changes to the Severity Table

The LOPA severity table (also used for P.H.A. studies) has changed significantly over the past few years. Industry practice, as recently as five years ago, used a single number for overall severity of an event. Within the severity description was a variety of verbiage describing multiple conditions, any of which would justify that level of severity.

Today, industry practice is to separate the various categories of severity. Each consequence of interest is then rated for severity within each category. The following table is typical:

Rank	On-Site Injury	Public Injury	Env. Releases	Reliability / Damage \$\$	Reputation
5 S Catastrophic	Potential for multiple life-threatening injuries.	Potential for multiple major injuries or illnesses or a single life-threatening injury. Toxic gas impacting more than 10,000 people or explosives impacting more than 1,000 people.	Potential for a major environmental incident requiring significant cleanup, remediation, or off-site response or a very large unconfined release.	Potential for long-term business interruption greater than six months or damage/ cumulative losses greater than \$50MM.	Potential for boycott or other disastrous community relations and/or national media attention.
4 S Major	Potential for multiple moderate injuries or illnesses or a single life-threatening injury or irreversible illness.	Potential for multiple moderate injuries or illness or a single major injury requiring a physicians care. Toxic gas impacting (civilian evacuation) up to 10,000 people or explosives impacting up to 1,000 people.	Potential environmental impact resulting in damage to sensitive environmental receptors or a minor unconfined release and significant mitigation response actions.	Potential for short-term business interruption greater than one month or damage/ cumulative losses up to \$50MM.	Potential for organized public protests, or widespread community relation's impact and/or regional media attention.
3 S Medium	Potential for multiple moderate injuries or illnesses or a single major injury requiring a physician's care.	Potential for multiple minor injuries or a single moderate injury or illness requiring medical treatment. Toxic gas impacting (shelter-in-place) up to 1,000 people or explosives impacting up to 100 people.	Potential for an environmental release requiring an NRC type release report and an on-site mitigation response action.	Potential for short-term business interruption greater than one week or damage. Cumulative losses up to \$5MM.	Potential for multiple public complaints and/or local media attention.

<p style="text-align: center;">2 S Low</p>	<p>Potential for multiple minor injuries or a single moderate injury or illness requiring medical treatment.</p>	<p>Potential for a single minor injury requiring first-aid treatment.</p>	<p>Potential for a minor environmental release requiring an internal or state only release report. No loss of site containment.</p>	<p>Potential for a plant upset resulting in efficiency loss or loss production. Potential for business interruption of less than one week. Cumulative losses up to \$500K.</p>	<p>Potential for a neighbor complaint without media attention.</p>
<p style="text-align: center;">1 S Negligible</p>	<p>Potential for a single minor injury requiring first-aid treatment</p>	<p>No off-site effect expected.</p>	<p>No environmental release expected</p>	<p>No business interruption expected. Cumulative losses up to \$50K</p>	<p>No potential for public inconvenience or nuisance.</p>

Table 3. This is a typical severity table.

A typical consequence of an on-site chemical release might receive a severity ranking of 2-1-3-2-2 with the five numbers corresponding to the categories of on-site injury, off-site injury, environmental consequence, cost, and publicity, respectively. The highest of these numbers (in this case, the “3” for environmental impact) would be the overall severity number used in the risk tolerance calculation.

Using a multi-factor severity table of this type allows insight into the PHA team’s concerns even years after the study. By looking at the severity category rankings done by the PHA team, the team’s actual concerns and thinking can be reconstructed by reviewing the study report documents. Without such categorization of severity, no such reconstruction is possible. The team (even if team members are available for interview) will have forgotten the exact scenario discussed and will be unable to reconstruct the “worst case scenario” from memory.

Severity categories of this kind are now considered standard industry practice in the chemical manufacturing, refinery, and pipeline industries. As of 2006, all such industries should have adopted a multi-factor severity matrix of this type.

Changes to the Risk Tolerance Table

LOPA analysis tends to drive initiating-event likelihoods to higher levels than actual field experience. Because LOPA typically classifies initiating-event likelihoods only in order-of-magnitude changes (once in ten years, once in a hundred, etc.), all likelihood numbers are rounded upwards to the next order of magnitude. For example, if an event were observed to happen twice in ten years, LOPA would round the likelihood upward to once per year. This LOPA likelihood (ten times in ten years) is eight events more than the actual, observed likelihood

of two in ten years. The LOPA method insists on this method of rounding, though. Therefore, risk-tolerance tables sometimes differ from the corporate PHA Risk Ranking Matrix in minor details. These deviations are artifacts of the LOPA evaluation method.

Many companies now use a LOPA-specific, risk-tolerance table that provides for somewhat greater tolerance of low severity events than the corporate risk-tolerance matrix. The skew in the LOPA-specific table is introduced by the LOPA procedure and is appropriate only to results derived from LOPA analysis.

The following example is a corporate risk-tolerance table with risk categorized from E to A in increasing magnitude:

CORPORATE RISK MATRIX		SEVERITY				
		1 S Negligible	2 S Low	3 S Medium	4 S Major	5 S Catastrophic
LIKELIHOOD ↑	5 - Probable 10^0	D	B	B	A	A
	4 - High 10^{-1}	D	C	B	B	A
	3 - Medium 10^{-2}	D	D	C	B	B
	2 - Low 10^{-3}	E	D	D	C	B
	1 - Remote 10^{-4}	E	E	D	D	C
	0 - Extremely Unlikely 10^{-5}	E	E	E	D	D

Table 4. This is a typical corporate risk-tolerance table.

The following example is the same company's LOPA risk-tolerance table using the same variables:

LOPA RISK MATRIX		SEVERITY →				
		1 S Negligible	2 S Low	3 S Medium	4 S Major	5 S Catastrophic
LIKELIHOOD ↑	5 - Probable 10^0	D	C	B	A	A
	4 - High 10^{-1}	D	C	C	B	A
	3 - Medium 10^{-2}	D	D	C	B	B
	2 - Low 10^{-3}	E	D	D	C	B
	1 - Remote 10^{-4}	E	E	D	D	C
	0 - Extremely Unlikely 10^{-5}	E	E	E	D	D

Table 5. This is typical LOPA risk-tolerance table.

The table is shown below showing ONLY the cells that were changed between the corporate and LOPA risk tables. The risk letter that comes first is the corporate table value, the second is the LOPA table value. Remember that risk is categorized from E to A in increasing magnitude:

		SEVERITY →				
		1 S Negligible	2 S Low	3 S Medium	4 S Major	5 S Catastrophic
LIKELIHOOD ↑	5 - Probable 10^0		B-C			
	4 - High 10^{-1}			B-C		
	3 - Medium 10^{-2}					
	2 - Low 10^{-3}					

	1 - Remote 10⁻⁴					
	0 - Extremely Unlikely 10⁻⁵					

Table 6. This is a typical risk divergence between corporate risk-tolerance tables and LOPA risk-tolerance tables.

The LOPA table allows for slightly higher tolerance of moderate risk events. This is done to compensate for LOPA’s “round-up” requirement for likelihoods. These changes in risk tolerance were artifacts of the LOPA process and should not provide significantly different risk to the company.

The company used for these examples makes another modification to their LOPA table. That modification is shown below:

LOPA RISK MATRIX		SEVERITY				
		1 S Negligible	2 S Low	3 S Medium	4 S Major	5 S Catastrophic
LIKELIHOOD	5 - Probable 10⁰	D	C-2	B-3	A-4	A-5
	4 - High 10⁻¹	D	C-1	C-2	B-3	A-4
	3 - Medium 10⁻²	D	D	C-1	B-2	B-3
	2 - Low 10⁻³	E	D	D	C-1	B-2
	1 - Remote 10⁻⁴	E	E	D	D	C-1
	0 - Extremely Unlikely 10⁻⁵	E	E	E	D	D

Table 7. This is a typical LOPA risk-tolerance table with IPL credit numbers.

Note the numbers after the A, B, and C risk letters. These numbers represent the number of credits required from the IPL Credits Table to reach what this company considers a minimally

acceptable risk (a “D”). By placement on the LOPA risk matrix, it will be evident that a specific number of credits will be required to reduce risk to an acceptable level. Since each credit in the IPL Credits Table represents an order of magnitude reduction in likelihood of the undesired event, this practice is consistent with the LOPA procedure, as defined by the AIChE guidelines.

The use of numbers in the LOPA Risk Matrix makes it less likely that an inexperienced LOPA practitioner will err in assessing the risk reduction required.

Changes in Instrument Assessment

Two new consensus standards have become significant in the assessment of instrument reliability. The Instrument Systems & Automation Society’s ISA-84.01 and the International Electrotechnical Commission’s IEC-61511 concern the implementation of Safety Instrumented Systems (SIS). In addition to these two main standards, the following standards and guidelines also affect SIS:

- IEC-61508
- ANSI/ISA TR84.00.04
- CCPS SIS Guidelines Book

While traditional instrument concerns have been over architecture and manufacturer’s recommendations, the SIS standards base instrument requirements on hazard analysis. LOPA is the most commonly used tool for assessing instrument reliability requirements.

The regulatory implementation of the SIS standards became active by way of an industrial explosion in 2004 where five workers were killed. OSHA cited the employer for not documenting that the plant’s programmable logic controllers and distributed control systems installed prior to 1997 (emphasis mine) complied with recognized generally accepted engineering practices such as ANSI/ISA 84.01. Since this citation was paid without contest, a precedent has been set that these SIS consensus standards are now “generally accepted engineering practice” in the chemical manufacturing, refining, and pipeline industries.

The SIS standards (to simplify significantly) require the company to ask the question, “If this safeguard fails to operate on demand, what will the consequences be?” After the worst-case severity of consequence is determined, then the likelihood of the existing control system to fail is calculated.

In calculating the likelihood of failure of an existing control system, all elements of the control system must be assessed, including the sensor(s), the logic element(s), and the actuated element(s) or valves. Because a failure of any of these elements will disable the entire control or trip system, the probabilities of failure are additive. Probability of failure on demand (PFOD) of the sensor(s) PLUS the PFOD of the logic element(s) PLUS the PFOD of the actuated element(s) equals the total PFOD.

Once the system total PFOD is determined, the severity of the consequences can be included to determine overall risk. Most companies use a chart to equate the expected risk to a desired reliability level for the instrumented system. If the existing system is not sufficiently reliable to

provide a desired risk level, then the reliability of the instrumented system can be improved by any combination of the following:

- Substituting more reliable components for the existing ones
- Adding redundancy to reduce the total PFOD for the system
- Increasing testing and calibration frequency to ensure desired function

The goal of SIS is to reduce the hazard assessment errors, design errors, installation errors, operations errors, maintenance errors, and change-management errors that might cause the instrument system to fail.

This paper (and its corresponding presentation at the 2006 Professional Development Conference of the American Society of Safety Engineers) does not focus primarily on Safety Instrumented Systems, but rather on LOPA. Because SIS reviews are typically done using LOPA risk assessments, this section was included.

Summary

Layers of Protection Analysis (LOPA) is now a firmly established, industry-wide “generally accepted engineering practice.” Businesses affected by OSHA’s 1910.119 (Process Safety Management of Highly Hazardous Chemicals) should already be using LOPA to verify risk assessments. The practices illustrated in this paper are typical of current industry LOPA practice.

The implementation of Safety Instrumented Systems (SIS) is going to be a firmly established, industry-wide “generally accepted engineering practice” within the next year. All industries that should be using LOPA should also be starting implementation of SIS.

For additional information on both LOPA and SIS, a wide variety of materials and training are available. The AIChE and Texas A&M University both have training sessions available for a fee.

Bibliography

Center for Chemical Process Safety. *Layers of Protection Analysis: Simplified Process Risk Assessment*. New York: John Wiley, 2001.