tonyfrederickson@msn.com

The Layer of Protection Analysis (LOPA) method

Look for best practices and guidelines on how to use the LOPA method as an alternative to mitigate risks.

Anton A. Frederickson, Mr., *Dr.* (prepared answer)
Independent Consultant – member of Safety Users Group Network
01 April, 2002

The Layer of Protection Analysis (LOPA) method is a Process Hazard Analysis tool. The method utilizes the hazardous events, event severity, initiating causes and initiating likelihood data developed during the Hazard and Operability analysis (HAZOP). The LOPA method allows the user to determine the risk associated with the various hazardous events by utilizing their severity and the likelihood of the events being initiated. Using corporate risk standards, the user can determine the total amount of risk reduction required and analyze the risk reduction that can be achieved from various layers of protection. If additional risk reduction is required after the reduction provided by process design, the basic process control system (BPCS), alarms and associated operator actions, pressure relief valves, etc., a Safety Instrumented Function (SIF) may be required. The safety integrity level (SIL) of the SIF can be determined directly from the additional risk reduction required.

Annex F – Layer of Protection Analysis from the Draft IEC 61511 Part 3 Standard is attached. The IEC 61511 is the process industry specific safety standard based on the IEC 61508 standard and is titled « Functional Safety of Safety Instrumented Systems for the Process Industry Sector ». IEC 61511 Part 3 is informative and provides guidance for the determination of safety integrity levels. Annex F illustrates the general principles involved in the LOPA method and provides a number of references to more detailed information on the methodology. It should be noted that Annex F is derived from a CDV version of the IEC 61511 Part 3 Standard dated 24 November 2000. The CDV version of the standard is for National Committee comments and vote on the draft. The draft will be subject to change based upon comments received from various National Committees around the world. I have included a few editorial comments received from members of the ISA SP84 Committee that were submitted to the IEC with a positive vote for the IEC 61511 Part 3 standard.

Annex F (informative) – Layer of Protection Analysis (LOPA)

F.1 Introduction

This annex describes a Process Hazard Analysis tool called Layer of Protection Analysis (LOPA). The method starts with data developed in the Hazard and Operability analysis (HAZOP) and accounts for each identified hazard by documenting the Initiating Cause and the protection layers that prevent or mitigate the hazard. The total amount of risk reduction can then be determined and the need for more risk reduction analysed. If additional risk reduction is required and if it is to be provided in the form of a Safety Instrumented Function (SIF), the LOPA methodology allows the determination of the appropriate Safety Integrity Level (SIL) for the SIF.

This annex is not intended to be a definitive account of the method but is intended to illustrate the general principles. It is based on a method described in more detail in the following references:

- Guidelines for Safe Automation of Chemical Processes, CCPS, New York 1993 Dowell, A. M., III;
- “Layer of Protection Analysis: A New PHA Tool after HAZOP, Before Fault Tree Analysis”, International Conference and Workshop on Risk Analysis in Process Safety, CCPS, (1997) pp 13-28;
- Ewbank, R, M., and York, G. S., “Rhone-Poulenc Inc. Process Hazard Analysis and Risk Assessment Methodology”, International Conference and Workshop on Risk Analysis in Process

Safety, CCPS, (1997) pp 61-74;

- Huff, A. M., and Montgomery, R. L., “A Risk Assessment Methodology for Evaluating the Effectiveness of Safeguards and Determining Safety Instrumented System Requirements”, International Conference and Workshop on Risk Analysis in Process Safety, CCPS, (1997), pp 111-126;

- Dowell, A. M., III, “Layer of Protection Analysis for Determining Safety Integrity Level”, ISA Technical Paper #973012 Technical Papers (1997) Dowell, A. M., III, “Layer of protection analysis for determining safety integrity level”, ISA Transactions 37(3) 1998 pp155-165;

- Layer of Protection Analysis, CCPS New York (in draft, expected in 2000);

- Bollinger et al, Inherently Safer Chemical Processes, A Life Cycle Approach, CCPS, New York, 1996.

F.2 Layer of Protection Analysis

The safety lifecycle defined in IEC 61511-1 requires the determination of a Safety Integrity Level for the design of a safety-instrumented function. The LOPA described here is a method that can be applied to an existing plant by a multi-disciplined team to determine the required safety instrumented functions and the SIL for each. The team should consist of:

- Operator with experience operating the process under consideration

- Engineer with expertise in the process

- Manufacturing management

- Process Control Engineer

- Instrument/Electrical maintenance person with experience in the process under consideration

- Risk analysis specialist

At least one person on the team should be trained in the LOPA methodology.

The information required for the LOPA is contained in the data collected and developed in the Hazard and Operability analysis (HAZOP). Table F.1 shows the relationship between the data required for the Layer of Protection Analysis (LOPA) and the data developed during the HAZOP. Figure F.1 shows a typical spreadsheet that can be used for the LOPA.

F.3 Impact Event

Using Figure F.1, each Impact Event (consequence) determined from the HAZOP is entered in Column 1.

F.4 Severity Level

Severity Levels of Minor (M), Serious (S), or Extensive (E) are next selected for the Impact Event according to Table F.2 and entered into Column 2 of Figure F.1.

LOPA

Note: Severity Level E = Extensive; S = Severe; M = Minor

Likelihood values are events per year, other numerical values are probabilities of failure on demand average

#	1	2	3	4		5		6	7	8	9	10	11
					PROTECTION LAYERS F.7, F.9								
	Impact Event Description F.3 F.14.1	Severity Level F.4 F.14.1	Initiating Cause F.5–F.14 F.14.2	Initiation Likelihood F.6 F.14.3	General Process Design F.14.4	BPCS F.14.5	Alarms F.14.6	Additional Mitigation Dikes, Pressure Relief, Restricted Access F.8 F.14.7	IPL Additional Mitigation Dikes, Pressure Relief, Restricted Access F.8 F.14.7 F.14.8	Interme-diate Event Likelihood F.10 F.14.9	SIF Integrity Level F.11 F.14.10	Mitigated Event Likelihood F.12	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0.1	0.1	0.1	0.1	0.1	PRV .01	10^{-7}	10^{-2}	10^{-9}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0.1	0.1		0.1	0.1	PRV .01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

BPCS is Basic Process Control System

Figure F.1 - LOPA Report

F.5 Initiating Cause

All of the Initiating Causes of the Impact Event are listed in Column 3 of Figure F.1. Impact Events may have many Initiating Causes, and it is important to list all of them.

F.6 Initiation Likelihood

Likelihood values of the Initiating Causes occurring, in events per year, are entered into Column 4 of Figure F.1. Table F.4 shows typical Initiating Cause likelihood. The experience of the team is very important in determining the Initiating Cause likelihood.

F.7 Protection Layers

Figure F.1 shows the multiple Protection Layers (PLs) that are normally provided in the process industry. Each protection layer consists of a grouping of equipment and/or administrative controls that function in concert with the other layers. Protection layers that perform their function with a high degree of reliability may qualify as Independent Protection Layers (IPL). The criteria to qualify a Protection Layer (PL) as an IPL are:

- The protection provided reduces the identified risk by a large amount, that is, a minimum of a 10-fold reduction.

- The protective function is provided with a high degree of availability (90% or greater).

- It has the following important characteristics:

  a) *Specificity*: An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event (e.g., a runaway reaction, release of toxic material, a loss of containment, or a fire). Multiple causes may lead to the same hazardous event; and, therefore, multiple event scenarios may initiate action of one IPL.

  b) *Independence*: An IPL is independent of the other protection layers associated with the identified danger.

  c) *Dependability*: It can be counted on to do what it was designed to do. Both random and systematic failures modes are addressed in the design.

  d) *Auditability*: It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary.

Only those protection layers that meet the tests of availability, specificity, independence, dependability, and auditability are classified as Independent Protection Layers.

Process design to reduce the likelihood of an Impact Event from occurring, when an Initiating Cause occurs, are listed first in Column 5 of Figure F.1. An example of this would be a jacketed pipe or vessel. The jacket would prevent the release of process material if the integrity of the primary pipe or vessel is compromised.

The next item in Column 5 is the Basic Process Control System (BPCS). If a control loop in the BPCS prevents the impacted event from occurring when the Initiating Cause occurs, credit based on its PFD avg is claimed.

The last item in Column 5 takes credit for alarms that alert the operator and utilize operator intervention. Typical protection layer PFD avg values are listed in Table F.3.

F.8 Additional Mitigation

Mitigation layers are normally mechanical, structural, or procedural. Examples would be:

- pressure relief devices,

- dikes, and

- restricted access.

Mitigation layers may reduce the severity of the Impact Event but not prevent it from occurring. Examples would be:

- deluge systems for fire or fume release,

- fume alarms, and

- evacuation procedures.

The LOPA team should determine the appropriate PFDs for all mitigation layers and list them in Column 6 of Figure F.1.

F.9 Independent Protection Layers

Protection layers that meet the criteria for IPL are listed in Column 7.

F.10 Intermediate Event Likelihood

The Intermediate Event Likelihood is calculated by multiplying the Initiating Likelihood (Column 4) by the PFDs of the protection layers and mitigating layers (Columns 5, 6 & 7). The calculated number is in units of events per year and is entered into Column 8.

If the Intermediate Event Likelihood is less than your Corporate Criteria for Events of this Severity Level, additional PLs are not required. Further risk reduction should, however, be applied if economically appropriate.

If the Intermediate Event Likelihood is greater than your Corporate Criteria for events of this Severity Level, additional mitigation is required. Inherently safer methods and solutions should be considered before additional protection layers in the form of Safety Instrumented Systems (SIS) are applied. If inherently safe design changes can be made, Figure F.1 is updated and the Intermediate Event Likelihood recalculated to determine if it is below Corporate Criteria. If the above attempts to reduce the Intermediate Likelihood below Corporate Risk Criteria fail, a SIS is required.

F.11 SIF Integrity Level

If a new SIF is needed, the Required Integrity Level can be calculated by dividing the Corporate Criteria for this Severity Level of event by the Intermediate Event Likelihood. A PFD_{avg} for the SIF below this number is selected as a maximum for the SIS and entered into Column 9.

F.12 Mitigated Event Likelihood

The Mitigated Event Likelihood is now calculated by multiplying Columns 8 & 9 and entering the result in Column 10. This is continued until the team has calculated a Mitigated Event Likelihood for each Impact Event that can be identified.

F.13 Total Risk

The last step is to add up all the Mitigated Event Likelihood for Serious and Extensive Impact Events that present the same hazard. For example, the Mitigated Event Likelihood for all serious and extensive events that cause fire would be added and used in formulas like the following:

- Risk of Fatality due to Fire = (Mitigated Event Likelihood of all flammable material release) X (Probability of Ignition) X (Probability of a person in the area) X (Probability of Fatal Injury in the Fire).

- Serious and Extensive Impact Events that would cause a Toxic release could use the following formula:

- Risk of Fatality due to Toxic Release = (Mitigated Event Likelihood of all Toxic Releases) X (Probability of a person in the area) X (Probability of Fatal Injury in the Release).

The expertise of the Risk Analyst Specialist and the knowledge of the team are important in adjusting the factors in the formulas to conditions and work practices of the plant and affected community.

The Total Risk to the corporation from this process can now be determined by totalling the results obtained from applying the formulas.

If this meets or is less than the corporate criteria for the population affected, the LOPA is complete. However, since the affected population may be subject to risks from other existing units or new projects, it is wise to provide additional mitigation if it can be accomplished economically.

F.14 Example

Following is an example of the LOPA methodology that addresses one Impact Event identified in the HAZOP.

F.14.1 Impact Event and Severity Level

The HAZOP identified High Pressure in a Batch Polymerisation Reactor as a Deviation. The stainless steel reactor is connected in series to a packed steel fiber reinforced plastic column and a stainless steel condenser. Rupture of the fiber reinforced plastic column would release flammable vapor that would present the possibility for fire if an ignition source is present. Using Table F.2 Severity Level Serious is selected by the LOPA team since the Impact Event could cause a serious injury or fatality on site. The Impact Event and its severity are entered into Columns 1 and 2, Figure F.1, respectively.

F.14.2 Initiating Causes

The HAZOP listed two Initiating Causes for High Pressure. Loss of cooling water to the Condenser and failure of the reactor steam control loop. The two Initiating Causes are entered into Column 3, Figure F.1.

F.14.3 Initiating Likelihood

Plant operations have experienced loss in cooling water once in 15 years in this area. The team selects once every 10 years as a conservative estimate of cooling water loss. 0.1 events per year is entered into Column 4, Figure F.1. It is wise to carry this Initiating Cause all the way through to conclusion before addressing the other Initiating Cause (failure of the reactor steam control loop).

F.14.4 Protection Layers Design

The process area was designed with an explosion proof electrical classification and the area has a process safety management plan in effect. One element of the plan is a management of change procedure for replacement of electrical equipment in the area. The LOPA team estimates that the risk of an ignition source being present is reduced by a factor of 10 due to the management of change procedures. Therefore a value of 0.1 so it is entered into Column 5, Figure F.1 under process design.

F.14.5 BPCS

High pressure in the reactor is accompanied by high temperature in the reactor. The BPCS has a control loop that adjusts steam input to the reactor jacket based on temperature in the reactor. The BPCS would shut off steam to the reactor jacket if the reactor temperature is above setpoint. Since shutting off steam is sufficient to prevent high pressure, the BPCS is a protection layer. The BPCS is a very reliable DCS and the production personnel have never experienced a failure that would disable the Temperature control loop. The LOPA team decides that a PFD_{avg} of 0.1 is appropriate and enters 0.1 in Column 5, Figure F.1 under BPCS (0.1 is the minimum allowable for the BPCS).

F.14.6 Alarms

There is a transmitter on cooling water flow to the condenser, and it is wired to a different BPCS controller than the temperature control loop. Low cooling water flow to the condenser is alarmed and utilizes operator intervention to shut off the steam. The alarm can be counted as a protection layer since it is located in a different BPCS controller than the temperature control loop. The LOPA team agrees that a 0.1 PFD_{avg} is appropriate since an operator is always present in the control room and enters 0.1 in Column 5, Figure F.1 under alarms.

F.14.7 Additional Mitigation

Access to the operating area is restricted during process operation. Maintenance is only performed during periods of equipment shut down and lock out. The Process Safety Management Plan requires all non-operating personnel to sign into the area and notify the process operator. Because of the enforced restricted access procedures, the LOPA teams estimate that the risk of personnel in the area is reduced by a factor of 10. Therefore .1 is entered into Column 6, Figure F.1 under additional mitigation.

F.14.8 IPL

The reactor is equipped with a relief valve that has been properly sized to handle the volume of gas that would be generated during over temperature and pressure caused by cooling water loss. Since the relief valve is set below the design pressure of the fiber glass column and there is no possible human failure that could isolate the column from the relief valve during periods of operation, the relief valve is considered a protection layer. The relief valve is removed and tested once a year and never in 15 years of operation has any pluggage been observed in the relief valve or connecting piping. Since the relief valve meets the criteria for an IPL, it is listed in Column 7, Figure F.1 and assigned a PFD_{avg} of 0.01.

F.14.9 Intermediate Event Likelihood

The columns in Row 1, Figure 1 are now multiplied together and the product is entered in Column 8, Figure F.1 under Intermediate Event Likelihood. The product obtained for this example is 10^{-7}.

F.14.10 SIS

The mitigation obtained by the protection layers are sufficient to meet corporate criteria, but additional mitigation can be obtained for a minimum cost since a pressure transmitter exists on the vessel and is alarmed in the BPCS. The LOPA team decides to add a SIF that consists of a current switch and a relay to de-energize a solenoid valve connected to a block valve in the reactor jacket steam supply line. The SIF is designed to the lower range of SIL 1, with a PFD_{avg} of 0.01. 0.01 is entered into Column 9, Figure F.1 under SIF Integrity Level.

The Mitigated Event Likelihood is now calculated by multiplying Column 8 by Column 9 and putting the result (1×10^{-9}) in Column 10, Figure 1.

F.14.11 Next Event

The LOPA team now considers the second initiation event (failure of reactor steam control loop). Table F.3 is used to determine the likelihood of control valve failure and 0,1 is entered into Column 4, Figure 1 under Initiation Likelihood.

The protection layers obtained from process design, alarms, additional mitigation and the SIS still exist if a failure of the steam control loop occurs. The only protection layer lost is the BPCS. The LOPA team calculates the intermediate likelihood (1×10^{-5}) and the Mitigated Event Likelihood (1×10^{-8}). The values are entered into Columns 8 and 10, Figure F.1 respectively.

The LOPA team would continue this analysis until all the deviations identified in the HAZOP have been addressed.

The last step would be to add the Mitigated Event Likelihood for the serious and extensive events that present the same hazard.

In this example, if only the one impact event was identified for the total process, the number would be 1.1×10^{-8}. Since the Probability of Ignition was accounted for under process design (0.1) and the probability of a person in the area was accounted for under additional mitigation (0.1), the equation for risk of fatality due to fire reduces to:

RISK OF FATALITY DUE TO FIRE = (MITIGATED Event Likelihood of all flammable material releases) X (PROBABILITY OF FATAL INJURY IN THE FIRE)

or

RISK OF FATALITY DUE TO FIRE = $(1.1 \times 10^{-8}) \times (.5) = 5.5 \times 10^{-9}$

This number is below the corporate criteria for this hazard so the work of the LOPA team is complete.

Table F.1 - Event Severity

LOPA REQUIRED	HAZOP DEVELOPED
INFORMATION	**INFORMATION**
Impact Event	Consequence
Severity Level	Consequence Severity
Initiating Cause	Cause
Initiating Likelihood	Cause Frequency
Protection Layers	Existing Safeguards
Required Additional Mitigation	Recommended New Safeguards

Table F.2 - Impact Event Severity Levels

Impact Event Level	Consequence
Minor (M)	Impact initially limited to local area of event with potential for broader consequence, if corrective action not taken.
Serious (S)	Impact Event could cause any serious injury or fatality on site or off site
Extensive (E)	Impact Event that is five or more times severe than a Serious event.

Table F.3 - Typical Protection Layer (Prevention & Mitigation) PFDs

INDEPENDENT PROTECTION LAYER	PFD
Control loop	1.0 x 10^{-1}
Relief valve	1.0 x 10^{-2}
Human performance (trained, no stress)	1.0 x 10^{-2}
Human performance (under stress)	0.5 to 1.0
Operator Response to Alarms	1.0 x 10^{-1}
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (i.e., corrosion understood, inspections and repairs in place)

Table F.4 - Initiation Likelihood

Low	A failure or series of failures with a very low probability of occurrence within the expected lifetime of the plant. Examples: * Three or more simultaneous Instrument, valve, or human failures. * Spontaneous failure of single tanks or process vessels.	f < 10^{-4} , /yr
Medium	A failure or series of failures with a low probability of occurrence within the expected lifetime of the plant. Examples: * Dual instrument or valve failures. * Combination of instrument failures and operator errors. * Single failures of small process lines or fittings.	10^{-4} < f < 10^{-2}, /yr
High	A failure can reasonably be expected to occur within the expected lifetime of the plant. Examples: * Process Leaks * Single instrument or valve failures. * Human errors that could result in material releases.	10^{-2} < f , /yr