Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 10 (24): 3319-3324, 2010
ISSN 1812-5654

This article was presented in International Conference on Process Engineering and Advanced Materials 24th Symposium of Malaysian Chemical Engineers (15th-17th June, 2010)

Development of a Layer of Protection Analysis Tool to Determine the Safety Integrity Level in Process Industries

[1]M. El-Harbawi, [1]Z. Azhani Bt. Razali, [2]S.M. Faiz B Sy M Fuzi and [3]S. Mustapha
[1]Department of Chemical Engineering, Universiti Teknologi PETRONAS, 31750, Tronoh, Perak, Malaysia
[2]Process Safety Management, Petronas Penapisan (Melaka) Sdn. Bhd., Bangunan Pentadbiran Persiaran Penapisan, Sungai Udang, Melaka 76300, Malaysia
[3]Deparbnent of Chemical and Environmental Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor D.E., Malaysia

Abstract: The purpose of this study was to develop a tool to determine the Safety Integrity Levels (SILs) using Layer of Protection Analysis (LOPA) method. Various methods can be used in determining this SIL. However, LOPA has been chosen as the risk-based approach to evaluate the potential consequences and likelihood. Many factors could be considered in order to complete this task. To implement LOPA procedure in the real situation, an industry plant operation had been selected as a case study. The work had been initiated by gathering the information on SIL. Event Tree Analysis (ETA) has been used to develop the scenarios of each initiating events. Then undesirable outcomes of accident scenarios have been calculated. A tool is developed to generate the scenarios or sequence of events that result in undesirable outcomes. Each scenario consists of two elements which are the initiating event that starts the chain of events and a consequence that results if the chain of events continues without interruption. Finally and after developing the scenarios, the identified initiating event frequency and related Independent Protection Layers (IPLs) is generated. There are 25 initiating events that have been listed in order to proceed with LOPA.

Key words: Layer of protection analysis, safety integrity levels, safety instrumented system

INTRODUCTION

LOPA is a simplified form of risk assessment. LOPA typically uses order of magnitude categories for initiating event frequency, consequence severity and the likelihood of failure of Independent Protection Layers (IPLs) to approximate the risk of a scenario (CCPS, 2001; Baybutt and Haight, 1998). LOPA is an analysis tool that typically builds on the information developed during a qualitative hazard evaluation, such as a Process Hazard Analysis (PHA) (Ramesh Babu, 2007). LOPA often follows a qualitative risk analysis performed as part of a HAZOP (HAZard and OPerability Analysis) to identify and characterize hazards. Because of its ease of use, LOPA has become a popular alternative to a Quantitative Risk Assessment (QRA) or a screening approach to QRA. The accidental risk assessment methodology for industries (ARAMIS) methods sponsored by the European Commission involves a simplified risk assessment approach that employs LOPA to assess hazard barriers. The overall ARAMIS approach, however, requires more effort than needed for LOPA alone in its consistent use of fault trees and event trees to calculate initiating event probabilities and to represent accumulated risk from multiple outcomes of each initiating event (Gowland, 2006; Wei *et al*., 2008).

In the safety life cycle outlined in ANSI/ISAS84.01-1996 (ISA, 1996; Dowell, 1998), steps are included to determine if a SIS is needed and to determine the target SIL for the SIS. The SIL is defined by the PFD (Probability of Failure on Demand) of the SIS. S84.01 gives guidance on building an SIS to meet a desired SIL (Dowell, 1998).

MATERIALS AND METHODS

LOPA includes the method that falls between qualitative and quantitative methods. There are several steps involved in the development of this tool (CCPS, 2001):

Step 1: Identify the consequences to screen the scenarios
Step 2: Select an accident scenarios

Corresponding Author: Mohanad El-Harbawi, Department of Chemical Engineering, Universiti Teknologi PETRONAS, 31750, Tronoh, Perak, Malaysia Tel: +605-3687581

Step 3: Identify the initiating event of the scenario and determine the initiating event frequency (events per year)
Step 4: Identify the IPLs and estimate the probability of failure on demand of each IPL
Step 5: Estimate the risk of the scenarios by mathematically combining the consequences, initiating event and IPL data

Step 1: Identify the credible consequences: In LOPA, the consequences are estimated to an order of magnitude of severity. There are various types of consequence analysis used in LOPA. Consequences are the undesirable outcomes of accident scenario whereby the consequence evaluation is an integral part of any risk assessment methodology. The risk associated with the accident scenarios and the risk assessment methodology adopted by the organization and the resources the organization is willing to expend to refine the estimate are the factors of what consequences should be evaluated and how rigorously the consequences are assessed. The different types of consequence evaluation are (CCPS, 2001):

- Release size/characterization
- Simplified injury/fatality estimates
- Simplified injury/fatality estimates with adjustments
- Detailed injury/fatality estimates.

The methods used for consequence categorization are (CCPS, 2001):

Method 1: Category approach without direct reference to human harm
Method 2: Qualitative estimates with human harm
Method 3: Qualitative estimates with human harm with adjustments for post release probabilities

Step 2: Developing scenarios: A scenario is an unplanned event or sequence of events that results in an undesirable consequence. Each scenario consists of at least two elements:

- An initiating event that starts the chain of events
- A consequence that results if the chain of events continues without interruption

Each scenario must have a unique initiating event/consequence pair. If the same initiating event can result in different consequences, additional scenarios should be developed. In some cases many scenarios may spring from a common initiating event and separate scenarios should be developed for individual sections of the plant. In addition to the initiating event and consequence, a scenario may also include:

- Enabling events or conditions that have to occur or be present before the initiating event can result in a consequence
- The failure of safeguards (which may be IPLs)

Once a scenario has been identified, it must be developed and documented to the level where a basic understanding of the events and safeguards is achieved. The scenario may not be initially understood completely and may undergo several revisions. New scenarios may also be revealed that must be analyzed separately. Once the initiating event is identified for a specific scenario, the analyst must determine whether any enabling events or conditions are required for the initiating event to lead to the consequence. The next step is to confirm that the consequence is stated using the same criteria as the LOPA method.

Step 3: Identifying initiating event frequency: For LOPA, each scenario has a single initiating event. The frequency of the initiating event is normally expressed in events per year. Some sources use other units, such as events per 10^6 h. Initiating events are grouped into three general types: external events, equipment failures and human failures. Prior to assigning frequencies to initiating events, all causes from the scenario development step should be reviewed and verified as valid initiating events for the consequence identified. Any causes that are incorrect or inappropriate should be either discarded or developed into valid initiating events. Frequency estimations are also involved in this stage. This frequency estimation measures the failure rate data which consists of sources, selection of failure rates, failure rates in LOPA, derivation of initiating event frequency from failure data, time at risk, adjustment of frequency rates and high demand mode.

Step 4: Identifying independent protection layers: An IPL is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario. In order to be considered an IPL, a device, system, or action must be:

- Effective in preventing the consequence when it functions as designed
- Independent of the initiating event and the components of any other IPL already claimed for the same scenario

- Auditable: The assumed effectiveness in terms of consequence prevention and PFD must be capable of validation in some manner
- Specificity: The IPL should be designed specifically to prevent the consequences from occurring
- Dependability: The IPL should be dependable in preventing the consequences from occurring. The probability of failure of IPL should be demonstrated to be less than 10%

The basic requirements of effectiveness, independence and audit ability for an IPL are determined by several methods. The simplest is to use a written design basis, or IPL summary sheet, which must be available for review by the LOPA team or analyst.

Step 5: Determining scenario frequency: For scenario frequency calculation, Equation 1 is used to calculate the frequency for a release scenario with a specific consequence endpoint (Eq. 1):

$$f_i^C = f_i^I \times \prod_{j=1}^{j} PFD_{ij} = f_i^I \times PFD_{i1} \times PFD_{i2} \times .....PFD_{ij} \quad (1)$$

where, f_i^C is the frequency for consequence C for initiating event i, f_i^I is the initiating event frequency for initiating event i, PFD_{ij} is the probability of failure on demand of the jth IPL that protects against consequence C for initiating event i.

Equation 1 is applicable for low demand situations that is, f_i^I is less than twice the test frequency for the first IPL.

Step 6: Risk decisions making: Three basic types of risk judgment are used in conjunction with LOPA:

- The predominant method is to compare the calculated risk with predetermined risk tolerance criteria through use of various methods
- The second type is expert judgment by a qualified risk analyst, which as noted above, is not recommended by the authors but is included for completeness
- The third type is relative comparison among competing alternatives for risk reduction, using either of the methods described above

In making risk decision, tolerance risk frequency will be the benchmark to the calculated risk frequency. So, the calculated risk frequency will be compared to the tolerance risk frequency. In LOPA, LOPA ratio has to be calculated to make risk decision. The calculated ratio will determine whether the system is reliable or unreliable. In general, LOPA ratio is used to make related decisions whether the IPLs or safeguards available in the system is applicable to prevent undesired outcomes. Equation 2 used to calculate LOPA ratio (CCPS, 2001):

$$\text{LOPA ratio} = \frac{\text{Tolerance risk frequency}}{\text{Scenario frequency}} \quad (2)$$

Tolerance risk frequency can be obtained from historical data, a company itself and expertise. Scenario frequency is the frequency that was calculated above. Below are the criteria for LOPA ratio:

- If LOPA ratio $\geq$1.0, no need to add other IPLs.
- If LOPA ratio $\leq$1.0, has to add other IPLs (SIL) and determine SIL

After developing the scenarios, the initiating event frequency and related IPLs have been identified. There are 25 initiating events that have been listed in order to proceed with LOPA (Table 1). The data for IPLs and PFD also has been collected from various sources (CCPS, 2001, 1989; OREDA, 2002). There are passive IPLs and active IPLs, shown in Table 2 and 3.

Tool development: After gathering all data and information, event tree analysis method has been used to develop the scenarios of each initiating events. The initiating events which have been developed are:

- Third party intervention
- BPCS instrument loop failure
- Cooling water failure
- Fixed equipment failure
- Gasket/packing blowout
- Human error (routine task, 1 per day opportunity)
- Human error (non-routine Task, Low Stress)
- Human error (routine task, once-per-month opportunity)
- Loss of power
- Cooling water failure
- Piping leak (10% section)
- Piping residual failure
- Pressure vessel residual failure
- Pump seal failure
- Pumps and other rotating equipment
- Small external fire
- Turbine/diesel engine overspeed w/casing breach
- Unloading/loading hose failure

Table 1: Initiating events and likelihood of failure

Initiating causes	Likelihood of failure year^{-1} (CCPS, 1989, 2001)
BPCS instrument loop failure	1×10^{-1}
Regulator failure	1×10^{-1}
Fixed equipment failure	1×10^{-2}
Pumps and other rotating equipments	1×10^{-1}
Cooling water failure	1×10^{-1}
Loss of power	1×10^{-1}
Human error (Routine task, 1 per day opportunity)	1×10^{-1}
Human error (Routine task, once-per-month opportunity)	1×10^{-2}
Human error ((Non-routine task, low stress)	1×10^{-1}
Human error (Non-routine task, high stress)	1×10^{0}
Pressure vessel residual failure	1×10^{-6}
Piping residual failure-100 m-Ful breach	1×10^{-5}
Piping leak (10% section)-100 m	1×10^{-3}
Atmosphere tank failure	1×10^{-3}
Gasket/packing blowout	1×10^{-2}
Turbine/diesel engine over speed w/casing breach	1×10^{-4}
3rd party Intervention	1×10^{-2}
Lightning strike	1×10^{-3}
Safety valve opens spuriously	1×10^{-2}
Pump seal failure	1×10^{-1}
Unloading/loading hose failure	1×10^{-1}
Small external fire (aggregate causes)	1×10^{-1}
Large external fire (aggregate causes)	1×10^{-2}
LOTO procedure failure (overall failure of a multiple-element process)	1×10^{-3} per opportunity
Operator failure (Routine procedure, well-trained, unstressed, not fatigued)	1×10^{-2} per opportunity

Table 2: Passive IPLs (CCPS, 1989, 2001; OREDA, 2002)

IPL	Comments Assuming an adequate design basis and adequate inspection and maintenance procedures	PFD
Dike	Will reduce frequency of large consequences (widespread spill) of a tank overspill/rupture/spill etc.	1×10^{-2}-1×10^{-3}
Underground drainage system	Will reduce frequency of large consequences (widespread spill) of a tank overspill/rupture/spill etc.	1×10^{-2}-1×10^{-3}
Opent vent (No valve)	Will prevent overpressure	1×10^{-2}-1×10^{-3}
Fireproofing	Will reduce rate of heat input and provide additional time for depressurizing/firefighting etc.	1×10^{-2}-1×10^{-3}
Blast-wall/bunker	Will reduce frequency of large consequences of an explosion by confining blast and protecting equipment/buildings etc.	1×10^{-2}-1×10^{-3}
Inherently safe design	If properly implemented can significantly reduce the frequency of consequences associated with a scenario Note: The LOPA rule for some companies allow inherently safe design features to eliminate certain scenarios (e.g, vessel design pressure exceeds all possible high pressure challenges)	1×10^{-1}-1×10^{-6}
Flame/detonation arrestor	If properly designed, installed and maintained these should eliminate the potential for flashback through a piping system or into a vessel or tank	1×10^{-1}-1×10^{-3}

Table 3: Active IPLs (CCPS, 1989, 2001)

IPL	Comments Assuming an adequate design basis and adequate inspection and maintenance procedures	PFD
Relief valve	Prevent system exceeding specified overpressure	
	Effectiveness of this device is sensitive to service and experience	$1x10^{-1}$-$1x10^{-5}$
Rupture disc	Prevent system exceeding specified overpressure	
	Effectiveness of this device is sensitive to service and experience	$1x10^{-1}$-$1x10^{-5}$
Basic process controlsystem	Can be credited as an IPL if not associated with the initiating events being considered	$1x10^{-1}$-$1x10^{-2}$ ($>1x10^{-1}$ allowed by IEC)
Safety Instrumented sunction (Interlocks)	See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for life cycle requirements and additional discussion	
SIL 1	Typically consists of:	
	Single sensor (redundant for fault tolerant)	
	Single logic processor (redundant for fault tolerant)	
	Single final element (redundant for fault tolerant)	$\geq1x10^{-2}$-$< 1x10^{-1}$
SIL 2	Typically consists of:	
	Multiple sensor (for fault tolerant)	
	Multiple channel logic processor (for fault tolerant)	
	Multiple final element (for fault tolerant)	$\geq1x10^{-3}$-$<1x10^{-2}$
SIL 3	Typically consists of:	
	Multiple sensor	
	Multiple channel logic processor	
	Multiple final element	$\geq1x10^{-4}$-$<1x10^{-3}$

The developed scenario for several initiating events is shown in Fig. 1.

Risk decision making: Risk tolerance frequency for general industry (chemical, manufacturing, rail, trucking)

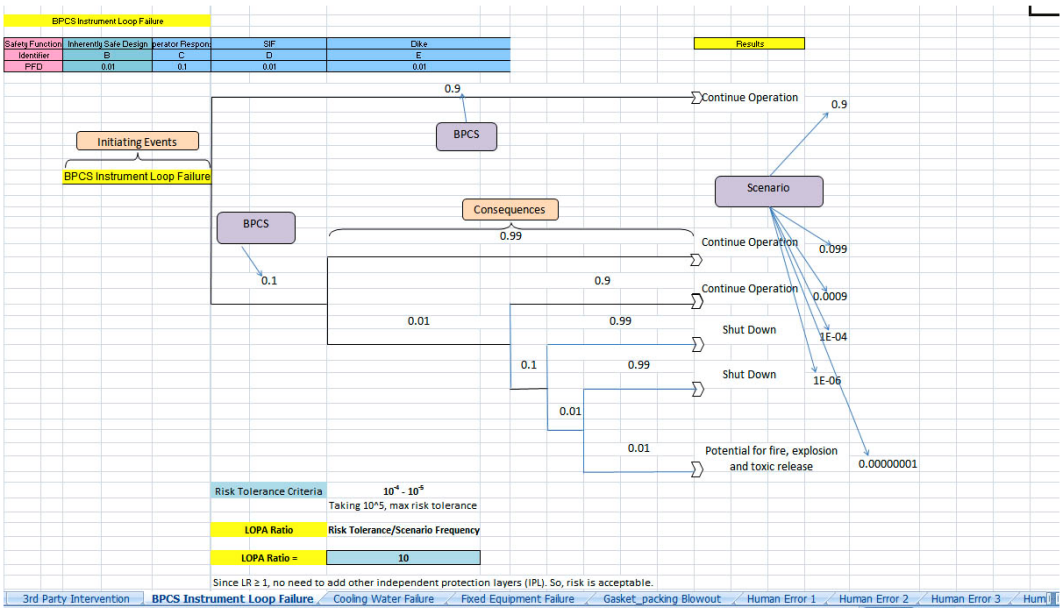

Fig. 1: The developed scenario for several initiating events

usually varies between 10^{-4} to 10^{-5} (probability of death per year). Let's take maximum allowable risk, 10^{-5} for safety purposes.

Scenario frequency: $f_{\text{BPCS Instrument Loop Failure}} * f_{\text{Inherently Safe Design}} * f_{\text{Operator Response}} * f_{\text{Dike}}$

From Fig. 1, LOPA ration that has been calculated is equal to 10 and since LOPA ration ≥1, therefore, no need to add other Independent Protection Layers (IPL). Therefore, IPLs are applicable and risk is tolerable.

CONCLUSION

An analysis tool has been developed to determine the SIL in process industries using LOPA method. The methodology provided by LOPA is to help in achieving the decision making process to assess the risk. Risk decision can be made by comparing the calculated scenario frequency with the tolerable risk frequency. Thus, such as risk has to be compared with permissible risk to ensure that the system in the plant is in inherently safe design. LOPA facilitates the determination of more precise cause-consequence pair and therefore, improves scenario identification. LOPA also helps resolve conflicts in decision making by providing a consistent, simplified framework for estimating the risk of a scenario and provides a common language for discussing risk. In other words, LOPA helps in risk decision making steps.

ACKNOWLEDGMENT

The authors would like to thank PETRONAS and the Chemical Engineering Department, Universiti Teknologi PETRONAS for their support.

REFERENCES

Baybutt, P. and J. Haight, 1998. Analysis of human factors for process safety: Application of LOPA HF to a fired furnace. http://www.primatech.com/info/paper_analysis_of_human_factors_for_process_safety_application_of_lopa_hf_to_a_fired%20furnace.pdf.

CCPS, 1989. Guidelines for Process Equipment Reliability Data with Data Tables. American Institute of Chemical Engineers, New York.

CCPS, 2001. Layer of Protection Analysis. Center for Chemical Process Safety, American Institute of Chemical Engineers (AIChE), New York.

Dowell, A.M., 1998. Layer of protection analysis for determining safety integrity level. ISA Trans., 37: 155-165.

Gowland, R., 2006. The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment. J. Hazardous Mater., 130: 307-310.

ISA, 1996. Application of Safety Instrumented Systems to the Process Industries, ANSI/ISA-S84.01-1996. Instrument Society of America, Research Triangle Park, NC, http://www.isa.org/~trini/pdf/ISA%20S84.01%20on%20ESD%20Valve%20Testing.pdf.

OREDA, (Offshore Reliability Data Handbook), 2002. OREDA Participants. Det Norske Veritas (DNV)

Ramesh Babu, J., 2007. Layer of protection analysis-an effective tool in PHA. Technical Paper: http://www.safetyusersgroup.com/documents/AR070003/EN/AR070003.pdf.

Wei, C., W.J. Rogers and M.S. Mannan, 2008. Layer of protection analysis for reactive chemical risk assessment. J. Hazardous Mater., 159: 19-24.