Limitations and misuse of LOPA

Roger Casey, Cantwell Keogh & Associates, Ireland

Summary

Layers of Protection Analysis (LOPA) is a simplified form of numerical risk assessment. It is an order of magnitude approach and hence precise figures are not used. The technique does have significant limitations compared to more advanced techniques such as Fault Tree Analysis, QRA, etc.

This paper highlights some of the mistakes that are seen in its application and challenges some of the practices that are occurring within LOPA calculations – in particular with the use of conditional modifiers related to exposure times which causes an underestimation of the risk.

Keywords: Layer of Protection Analysis, LOPA, risk assessment

Introduction

Layers of Protection Analysis (LOPA) is a simplified form of numerical risk assessment. It is an order of magnitude approach and hence precise figures are not used. The technique was published by the Centre of Chemical Process Safety (CCPS)[1] of the American Institute of Chemical Engineers (AIChE) in 2001. LOPA builds on qualitative studies such as HAZOP and the aim of the technique is to reduce risk by using Independent Protective Layers (IPLs). The purpose of LOPA is to determine if there are sufficient safeguards/ IPLs for a particular scenario to reduce the risk of it occurring. LOPA applied properly provides a consistent basis for judging within a company or organisation so that similar results are obtained for similar situations.

However, LOPA is a simplified form of numerical risk analysis and hence has significant limitations. Also, from auditing and reviewing LOPA studies there is concern at the level of mistakes being made using the technique.

The purpose of this paper is to highlight some of the mistakes being made and challenge some of the practices that are occurring within LOPA calculations.

Limitations of LOPA

LOPA is a very useful technique, but like everything else it has its limitations. LOPA is a simplistic risk assessment technique designed to be suitable for general technical personnel so that, for example, process engineers who are not process safety specialists can contribute to a LOPA team.

It is an order of magnitude risk calculation and hence uses figures such as i.e. 0.1, 0.01, 10^{-3} yr^{-1} not precise figures such as e.g. 43.2 x 10^{-4} yr^{-1}. From the AIChE book, some examples of failure rates are given in Table 1.

Item	Failure Rate
Pipe failure / 100 m	1 x10^{-5} yr^{-1}
Impact from vehicle	1 x10^{-2} yr^{-1}
Cooling failure	1 x10^{-1} yr^{-1}
Large external fire	1 x10^{-2} yr^{-1}
LOTO procedure	1 x10^{-3} per opportunity

Table 1 – Example LOPA initiating event frequencies

As can be seen, they are all order of magnitude figures such as 1x 10^{-3} yr^{-1}. Probability of demand figures are similarly based on order of magnitude e.g. 0.1 or 0.01, etc. Hence results are not precise. There is also a cumulative effect on the final event frequency figure where the combination of a number of conservative figures will make the final figure more conservative.

To look at scenarios that involve a large number of initiating events (which have different IPLs) other techniques such as Fault Tree Analysis may be more suitable. For example, for a bunded pool fire resulting from a storage tank spill there may be up to ten possible initiating events. These include overfilling, inlet pipeline leaks, outlet pipeline leaks, drain valves left open, pump leaks, pin holes in the tank, catastrophic failure of the tank, etc. While possible with LOPA it would require multiple simple LOPA sheets or more complex LOPA software and the situation would be further complicated if a number of outcomes, such as pool fire, flash fire, vapour cloud explosion, are to be included.

The AIChE book repeatedly mentions that LOPA analysis looks at a single cause–consequence pair, e.g. pool fire from overfilling.

LOPA is not suitable for analysing scenarios where there is common cause failure as it cannot handle these mathematically. More detailed risk analysis such as Fault Tree Analysis uses boolen algebra / minimum cut set analysis to factor in these common cause failures.

Also, the AIChE book states that *LOPA may be inappropriate for very high consequence events …….and it may be necessary to proceed to risk assessment techniques nearer to Chemical Process Quantitative Risk Assessment (CPQRA) in such cases.*

Misuse of LOPA

The UK HSE commissioned a report[2] post-Buncefield, on overfill protection on storage tanks which reviewed LOPA

0260-9576/19/$17.63 + 0.00

studies performed by a number of companies and their consultants. The report raised issues such as the quality of data used, over optimistic human error probabilities, degree of rigour applied, misunderstanding of risk targets and invalid logical arguments. Another comment in the report was that *LOPA may appear to be an easy method to apply at first but this may be deceptive.*

The following are examples that the author has encountered where mistakes have been made or where there is dubious use of the technique. While none of these led to incidents, the event frequency and risk was or may have been significantly underestimated.

Some of the examples relate to the use of conditional modifiers. A conditional modifier is defined[1] as enabling events or conditions that have to occur or be present before the initiating event can result in the consequence. Examples of conditional modifiers are:

- Probability of ignition of a flammable spill;
- An event exposure time e.g. a major toxic leak reaching a football stadium and effecting the 20,000 crowd. However, the large numbers will only be present say 20 times a year for 3-4 hours.

Example 1 – Pipeline failure rate adjustment

This involved a solvent recovery area in a pharmaceutical company where a 220 m pipeline was pumping solvent 45% of time and is empty 55% of the time.

From reference 1 the pipe failure rate / 100 m is 1 $\times 10^{-5}$ yr^{-1} for a full-bore rupture. The analyst multiplied the pipe failure rate by 0.45 i.e. the failure rate of solvent spill is:

$$= 2.2 \times 10^{-5}\ yr^{-1} \times 0.45 = 9.9 \times 10^{-6}\ yr^{-1}$$

However, the use of a factor of 0.45 implies the pipeline cannot be damaged / degraded or interfered with when not in use. For example, if the pipe is subjected to corrosion under insulation (CUI) the failure rate may not be reduced by the reduced pumping time. Ageing of gaskets at flanges will not be reduced by the reduced pumping time. Also, if a fitter unbolts the wrong flange, or someone leaves a drain valve open, the leak will occur next time the pipeline is used. Hence the failure rate of the system is unlikely to be linear with use time. Based on this logic the conditional modifier of 0.45 should not have been used. Essentially its use led to an underestimate of the event frequency.

What would be a reasonable conditional modifier in a similar but different case would be where solvent was being pumped 45% of time and water 55% of the time. It would not be a major hazard if the pipe failed during water pumping and the site would be very likely aware of the water release event which would prevent the next solvent pumping operation.

Example 2 – Runaway reaction exposure time

Consider the case in a batch chemical reaction where a runaway reaction is caused by agitator failure and re-start. This is usually caused in controlled additions over time where the agitator fails, reagent is still being added and accumulating but not reacting and if the agitator is re-started, the whole uncontrolled reaction occurs and the cooling cannot cope.

In this example, the particular product was only made for approximately three months of the year. The LOPA analyst multiplied the initiating event frequency by 0.25 to allow for this. Also, the batch time in the reactor was 14 hours but the actual reaction time was 4 hours. The analyst took the view that it did not matter if the agitator fails during other times e.g. during vessel inerting, solvent loading, etc. The initiating event (agitator failure rate, a Basic Process Control System failure[1]) was multiplied by 0.285 (4/14) to account for this. There was also a bursting disk (sized for the scenario) which a probability of failure on demand of 0.01[1] was correctly allowed for. The analyst calculated the event frequency as:

$$0.1\ yr^{-1}\ \text{(agitator failure)} \times 0.25 \times 0.285 \times 0.01\ \text{(disk)} = 7.125 \times 10^{-5}\ yr^{-1}$$

At first glance, the use of 0.285 for reaction time to batch time seems reasonable. However, it raises the question that if the agitator fails before the reaction how will it be picked up? Just hoping that the operator will see the agitator failure is not reliable and certainly not consistent with the conservative nature of LOPA. If there was something reliable to pick up agitator failure, such as an independent speed sensor on the agitator shaft, this would have been used as an IPL in the calculation. Hence, as a latent failure, the time-at-risk factor of 0.285 is not appropriate and should not have been used in this case.

The use of a factor of 0.25 to allow for the particular product being only made for three months is also dubious. The plant in question was a multipurpose batch plant with a wide variety of hazardous reactions most of which had runaway reaction hazards. Hence for the rest of the year the operator is exposed to the same hazard but from a different process in the same vessel. So again, this time-at-risk factor is not appropriate and should not have been used.

If the other processes used in the vessel for the other nine months were all relatively non-hazardous, the factor of 0.25 would have been a reasonable conditional modifier.

Ignoring these conditional modifiers, the event frequency is only 1 $\times 10^{-3}$ yr^{-1}.

Example 3 – Adjustment of hose and regulator failure frequencies

The author has seen a number of cases where equipment failure frequencies are being multiplied by the hours used per day. This has, in some cases become an almost standard practice and is often done without thinking through the logic. Common examples are flexible hose failure or pressure regulators. If a flexible hose or regulator is used for one hour a day the failure frequency is multiplied by 1/24. Again, it should be questioned whether this is really appropriate. Yes, a flexible hose used once a day is likely to last longer than one which is under pressure more often, but it is doubtful that the failure rate relationship is linear. Again, the use of 1/24 implies that the hose often left outside exposed to the elements, cannot be damaged or degraded when not in use.

For road tanker unloading hoses the UK HSE FRED document[3] has detailed failure rate data related to the number of times a hose is used in transfer operations. However, for process hoses or items such as pressure regulators, factoring in use time to the

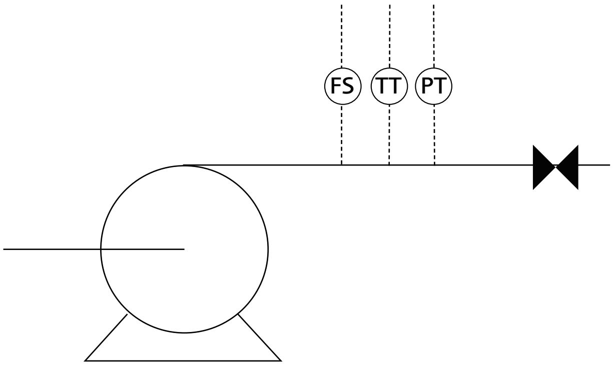

Figure 1 – Pump set up

basic failure rate is not simple and probably requires further research into failure rates in such situations.

Example 4 – Pumping thermally unstable material

A reaction mixture which was prone to a violent thermal decomposition was being pumped from the reaction vessel to another vessel for further processing. Dead heading the pump and heat input leading to decomposition was identified as an issue and a LOPA calculation was performed. There was one manual valve between the two vessels. There were a number of instrumented trips to protect against this. The plant typically ran 9 am – 5.30 pm five days a week. The situation is depicted in Figure 1.

The initiating event was taken as the manual valve being closed in error. The valve was used once a fortnight for a cleaning procedure. A failure rate of operator error 0.01 per opportunity was used (Reference 1 — routine procedure, well trained, not fatigued, etc) The analyst also factored in the plant operating hours as a conditional modifier to give the following adjusted initiating event failure rate:

$$0.01 \text{ (per opportunity) x 26 (opportunities/yr) x } \\ 0.24 \text{ (40/168 hrs)} = 0.062 \text{ yr}^{-1}$$

Reflecting on this, the factor of 0.24 is inappropriate, should have not been used and leads to underestimation of the frequency. The frequency of the initiating event is related only to how often the valve is used. If for example, the plant moved to a 24/7 operation, the cleaning would be likely to occur more often, and the valve error failure rate would be adjusted accordingly.

The HSE document on Standards for Fuel Storage Sites[4] discusses this type of human error calculation and states that *the time at risk is already included in the number of times the task is carried out in a year and no further factor should be applied.*

Example 5 – SIL calculation for batch runaway reaction

An (non-chemical) engineer was performing a SIL assessment calculation using the LOPA technique to determine the rating for independent interlocks recommended at a HAZOP for a very strong exothermic reaction (adiabatic temperature rise T_{ad} of > 320°C) which would subsequently lead to a violent decomposition of the product reaction mixture in a reactor. The HAZOP team had concluded that the runaway event was un-ventable even with the largest possible bursting disk on the vessel and recommended duplicate interlocks or a single interlock with a higher SIL rating in lieu of this.

As the scenario related to over-pressure, the engineer performing the SIL calculation allowed a relief valve on the 4,000 L vessel to be used as an IPL with a probability of failure of demand of 0.01[1]. However, the relief device was a 3"/4" relief valve which would not be any use for such an exothermic event in question. While part of the problem was that the SIL assessor did not study the HAZOP report properly, nevertheless to an experienced process safety engineer familiar with DIERS (Design Institute of Emergency Relief Systems) methodology, the thermal data which was available was such that it would be very unlikely that this event could be vented. The SIL assessor didn't have the knowledge to question whether the relief device was appropriate.

In effect, the person in question did not have the qualifications, knowledge or experience to make the risk decisions they were making. This problem was alluded to in an article in TCE[5] in relation to SIL assessments when it was stated that *it is possible to attend courses.....and obtain certification – giving the impression of expertise without any proper understanding of the underlying principles and mathematics involved.*

Discussion

So why are these types of mistakes / errors of judgement occurring?

In all the cases above, the personnel involved had been trained in the technique. Inexperience may have been the problem in a number of the examples. Just because a person has attended a training course does not make them competent in a subject. Years of practical experience in the application of risk assessment techniques is required for competence. Conducting LOPA in a team setting may help counter this problem. Like any element of a safety management system LOPA studies need to be subjected to auditing and any calculations by less experienced engineers need to be checked.

There appears to be a problem with the use of conditional modifiers (particularly in batch type processes) with time at risk factors. Before using such factors, people need to think carefully and do a reality check as to whether the conditional modifier used is correct and appropriate to the situation being studied. Again, auditing and supervision are important.

One has to question whether LOPA has over simplified risk assessment and hence allowed inexperienced personnel to perform calculations? In any risk analysis, judgements have to be made. The use of the various spreadsheets that are available for LOPA may be allowing people to plug in data and get answers without fully understanding or thinking through the issues involved. A similar situation exists with consequence modelling packages.

People using the technique need to be aware of the other risk assessment techniques available and when LOPA is / is not appropriate. LOPA was only ever meant to be an order

0260-9576/19/$17.63 + 0.00

of magnitude risk estimate of relatively simple scenarios. Appropriate coverage in training courses of where LOPA fits in with other techniques is important.

The use of a consistent set of data within a company for common initiating events, IPLs, etc is also important to ensure consistency of studies by different analysts within an organisation.

Conclusion

LOPA applied properly is a very useful technique in the toolbox of the risk analyst. However, people must always be aware of its limitations compared to more advanced techniques such as Fault Tree Analysis, QRA, etc. While LOPA is a relatively simple technique, common mistakes are occurring particularly with the use of conditional modifiers related to exposure times which causes an underestimation of the risk. Analysts need to be sure conditional modifiers are appropriate and correct for the situation under assessment.

Personnel carrying out LOPA studies must be experienced and competent and where necessary adequately supervised.

References

1. *Layer Of Protection Analysis Simplified process risk assessment, CCPS, AIChE, 2001*
2. *A review of Layer Of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks, Prepared by the Health and Safety Laboratory for the Health and Safety Executive, 2009*
3. *Failure Rate and Event Data for use within Land Use Planning Risk Assessments, UK HSE, 2012.*
4. *Safety and environmental standards for fuel storage sites, Process Safety Leadership Group Final Report, UK HSE, 2009*
5. *IEC 61508: uses and abuses, David J Smith, The Chemical Engineer Magazine, February 2012.*