Calculating yourself into a corner using LOPA

Stephen Beedle, Principal Process Safety Consultant, ABB Consulting, Belasis Hall Technology Park, Byland Way, Billingham, TS23 4EB

In recent years Layer of Protection Analysis (LOPA) has become the tool of choice for carrying out both the SIL Assessment calculation for the reliability of Safety Instrumented Functions or predicting the frequency of individual events. LOPA is a time efficient and relatively straightforward technique which means there is no shortage in the number of practitioners. It can, when used by a skilled practitioner with the aid of a supportive technical team, provide great insight into the risk of individual hazardous events, but there are circumstances under which the output of a LOPA can be misleading resulting in incorrect risk conclusions. The output of a LOPA drives the design of Safety Instrumented Functions or the identification of further risk reduction by the installation where appropriate of additional layers of protection. In effect the output of the LOPA will very often drive capital expenditure, so the question is whether the LOPA is giving the 'right' answer to ensure that any further expenditure is proportionate.

In order to carry out a LOPA a set of equipment failure data and conditional modifiers is used. The resultant event frequency is then compared to target risk criteria specific to each individual company. By applying the strict rules of LOPA in terms of the independence of protective layers, conservatism in the selection of equipment failure rates and the probability of human error, very often a LOPA can suggest that a large risk gap exists, or that a high SIL category is required for the Safety Instrumented Function under assessment. Closing such a large risk gap may require significant capital expenditure.

This paper examines why LOPA can predict large risk gaps that in reality may not exist. Clearly pursuing a false risk gap could result in significant capital expenditure that brings little or no actual risk reduction.

Introduction

Layer of Protection Analysis (LOPA) is a rule-based technique for carrying out SIL Assessment calculations for the reliability of Safety Instrumented Functions and also establishing the frequency of individual hazardous events. In its application LOPA is a time efficient and relatively straightforward technique. This paper has drawn on the authors experience of leading, auditing and observing LOPA studies over the last 20 years. It is not intended as an in depth analysis of the technical nature of the LOPA technique or an examination of the sources of failure data as applied in LOPA. Instead, this paper is intended as a series of observations on how the rules of LOPA can be applied and also how sometimes they can give rise to potentially misleading results showing large risk gaps or high target SIL requirements. The intention being to understand why misleading results may occur and what to do about them whilst still meeting regulatory requirements.

To facilitate this review the theme of the paper will follow a LOPA analysis relating to hydraulic overpressure and subsequent failure of a 'Buffer Vessel' as shown in Figure 1, should it become liquid full co-incident with the failure of its overpressure protective systems.

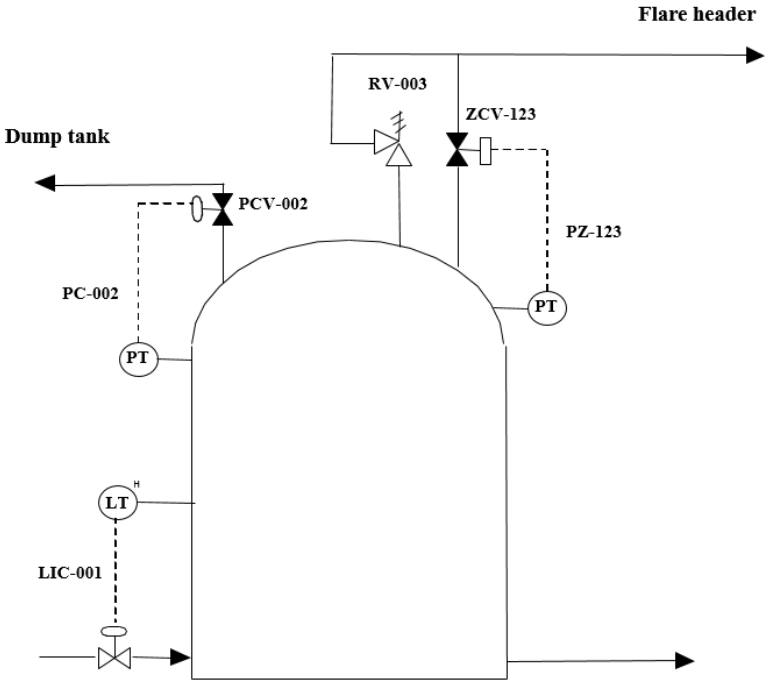

Figure 1 - Buffer Vessel general arrangement

Buffer Vessel LOPA

There are many forms in which a LOPA can be presented, the form used in this assessment follows a Microsoft Excel vertical format. The LOPA is being used to calculate the Safety Integrity Level (SIL) of a high pressure Safety Instrumented Function (SIF) PZ-123 for a Buffer Vessel. The LOPA record will be presented in the following sections:

- Hazardous event description and risk criteria
- Initiating causes
- Independent Protection Layers and Conditional Modifiers
- SIL (PFD_{avg}) calculation

The actual process design and control of this system is of no great relevance to the paper as the paper does not seek to examine whether the LOPA matches correctly the process design and operation of the system. It is assumed that the LOPA team had the correct technical knowledge to carry out this step competently. Instead the starting point of the paper is an assumption that the LOPA is a 'correct' representation of the process.

Hazardous event

The first step in the LOPA is the hazardous event which is defined as follows:

Site/Plant	Buffer Vessel
Event Description	Liquid overfill of Buffer Vessel causing it to be overpressured when hydraulically full. Vessel failure leading to a release of flashing hydrocarbon liquid, that upon ignition results in a flash fire.
Event Type	Safety
Event Consequences	On-site fatality
Target Frequency Ft /yr	0.000001
Safety Function Loop Number	High pressure trip PZ-123
Safety Function Trip Action	Opens vent valve ZCV-123 to release pressure to the flare header

Table 1 - Hazardous event

This LOPA relates to a hazardous event that unmitigated results in an on-site fatality for which the company involved has specific a target event frequency or risk criterion of 10^{-6} per year (1 in 1,000,000 years).

Initiating causes

There are two independent causes of overfilling the Buffer Vessel as follows:

Initiating Causes			
Ref	**Description**	**Freq (/yr)**	**Justification**
A	BPCS (Basic Process Control System) level control loop failure (LIC-001).	0.1	IEC 61511 dangerous failure rate for a BPCS control loop 0.1/yr.
B	Operator error during start-up when LIC-001 is operated in manual.	0.2	Buffer Vessel is filled twice per year with a probability of human error during start-up of 0.1.

Table 2 – Initiating causes

Independent Protection Layers and Conditional Modifiers

Table 3 presents all of the Independent Protection Layers (IPL) that are intended to prevent hydraulic overpressure of the Buffer Vessel, and also all of the Conditional Modifiers (CM) that prevent a hydraulic overpressure event leading to vessel rupture, a fire and an on-site fatality.

Independent Layers of Protection and Conditional Modifiers			
Ref	**Description**	**PFD_{avg}**	**Justification**
1	BPCS high level alarm from LIC-001.	0.1	Alarm is non-independent in the case of Initiating Cause A. For Initiating Cause B the alarm is independent so a probability of the operator failing to respond to the alarm of 0.1 is applied.
2	BPCS pressure control loop (PC-002) opens PCV-002.	0.1	IEC 61511 probability of failure on demand for a BPCS control loop 0.1. PC-002 is in the same BPCS as LIC-001 therefore not fully independent.
3	Relief valve (RV-003).	0.01	Clean duty, relief valve sized correctly for the liquid overfill case.
Conditional Modifiers			
4	Probability of rupture.	1	The maximum hydraulic pressure is 1.6 times the Buffer Vessel design pressure therefore a probability of rupture of 1 is applied.
5	Probability of ignition.	1	The Buffer Vessel is located in a remote area of the plant, but a large vapour release could encroach on areas that are not zoned, therefore a probability of ignition of 1 is applied.
6	Person present and injured.	0.1	Area local to the Buffer Vessel is not normally occupied. Based on routine operator patrols apply an occupancy probability of 0.1. At start-up the operator is present so apply a probability of 1.

Table 3 – IPL and CM

SIL (PFD_{avg}) calculation

PFDavg Calculation								
Initiating Cause	**Frequency (/yr.)**	**Independent Protection Layer and Conditional Modifier**						**Intermediate Event Frequency**
		1	**2**	**3**	**4**	**5**	**6**	
A	0.1	1	1	0.01	1	1	0.1	0.0001
B	0.2	0.1	0.1	0.01	1	1	1	0.00002
							Total Event Frequency, Fe /yr.	0.00012
							PFDavg for Safety Instrumented Function , Ft/Fe	**8.3E-03**
							Safety Integrity Level =	**SIL 2**

Table 4 – SIL calculation

The outcome of the LOPA is a SIL2 high pressure SIF PZ-123 with a PFD_{avg} of 0.0083. If this reliability is met with appropriate functional testing then the fatality event frequency relating to overpressure of the Buffer Vessel is 10^{-6} per year. This is numerically the correct answer from the LOPA, but the question the following sections seek to explore is whether this is the 'right' answer.

Examination of LOPA inputs

Risk criteria

Table 1 has shown the company risk criterion for an on-site fatality event is 10^{-6} per year (Ft). Before even selecting a numerical value, care has to be applied here to define what this frequency actually is. For example is it:

- The frequency of an individual hazardous event, or
- The risk to an individual worker.

If this is not clearly defined then there is a risk of comparing 'apples with oranges'.

Published risk criteria from the Health and Safety Executive, "Reducing Risks, Protection People", HSE Books, 2001 quotes criteria in terms of the Individual Risk of Fatality (IRF) to the worker at greatest risk. IRF is presented between the upper 'intolerable' limit of 10^{-3} per year and the lower 'broadly acceptable' limit of 10^{-6} per year. These IRF figures are often quoted directly as a LOPA risk target but it must be remembered an IRF relates to the cumulative risk to an individual person from all hazardous events to which they are exposed both process and occupational and not just a single hazardous event as portrayed in a LOPA.

The LOPA example being used here is for a single hazardous event and there is no consideration of all the other hazardous events on the same facility. So how do we know if 10^{-6} per year for the single Buffer Vessel hazardous event is a sensible LOPA target if the published risk criteria relates to cumulative risk of all hazardous events and IRF? The answer is that it is necessary to convert the published IRF criteria to an individual hazardous event frequency and apply that in the LOPA as the risk target. This requires calibration and a knowledge of the number of hazardous events that are present on a site, the number of workers at risk based on shift patterns and exposure of personnel to hazards, i.e. a calibration on the worker at greatest risk.

Typically the Target individual hazardous event frequency (Ft in the Buffer Vessel LOPA) is seen in the range 10^{-4} to 10^{-6} per year. Very often the target of choice is 10^{-6} per year, the reason is this is considered 'broadly acceptable'. Again, this is often due to confusion between IRF and hazardous event frequency. But what is the impact of a target of 10^{-6} per year for an on-site fatality. Before jumping to 10^{-6} per year let's look at some other targets:

- 10^{-4} per year – this means all hazardous events have a target frequency of 10^{-4} per year. When you start to add up the risk from all of the hazardous events on the site and then divide by the exposed work force very often this gives an IRF for the worker at greatest risk close to a level that would be considered 'intolerable'. If cost benefit were to be applied it would show that the amount of justifiable expenditure remaining even if the 10^{-4} per year target is met is substantial. For example, an individual single fatality event could justify of the order of £80,000. So although the 10^{-4} per year target is met there is potentially a lot more that could be done, so in effect the job is not finished and further risk reduction measures still need to be implemented.
- 10^{-5} per year – a similar argument in terms of IRF can be generated although the IRF is likely to be clear of the 'intolerable' risk region, but in this case cost benefit analysis would typically show for an individual on-site single fatality event the remaining justifiable expenditure is very low, of the order of £4,000. This suggests there is very little that could be engineered to further reduce the risk.

This latter point is very important because it you are aiming for a 10^{-5} per year target the cost of another engineered layer of protection to move from 10^{-5} to 10^{-6} per year is likely to be grossly disproportionate. In relation to the Buffer Vessel LOPA, the high pressure SIF has a target of SIL2 based on the 10^{-6} per year target, this suggests that SIL1 would have been appropriate if a 10^{-5} per year target was chosen. So by inference the requirement from the LOPA for a SIL2 high pressure SIF may actually incur a grossly disproportionate cost. In this case the chosen risk criterion may be forcing expenditure where it is not justified.

Failure rate data

Many pages of discussion can be given over to sources of equipment failure rate data, how it is collected and analysed and how accurate or representative it could be considered. This paper does not seek to cover this extensive subject, instead it just seeks to examine one piece of failure rate data that is used in the majority of LOPA, and that is the dangerous failure rate for a BPCS (Basic Process Control System) control loop which is invariably taken as 0.1/year as required under IEC 61511 "Functional safety of electrical/electronic/programmable electronic safety-related systems". This is a standard figure in LOPA and is routinely applied for the dangerous failure rate of a control loop that is not SIL-rated. In part this number is convenient because it means your BPCS system does not have to be SIL-rated with the functional testing requirements that would otherwise be involved.

The Buffer Vessel has only one control loop giving an initiating cause contribution of 0.1/year as shown in Table 2. However, maybe the Buffer Vessel is a small part of a much larger complex with many more control loops routed through the same BPCS. For example, across the wider complex there may be 200 control loops and then applying 0.1/year for each control loop would suggest a control loop would fail dangerously once every couple of weeks. This would seem a very unreliable operation that raises the question as to whether this actually matches operating experience. Whilst carrying out LOPA studies the author has informally analysed data on the dangerous failure rate of control loops by questioning the LOPA team and reviewing actual demand rates on individual SIF's. This is a difficult exercise as the data will vary widely between the type of plant, the process environment and many other factors. However, the inference is that 0.1/year is generally at the higher end of the ranges of dangerous failure observed.

Furthermore, a distinction has to be drawn between sudden and gradual failures. The latter tends to be more common, i.e. the gradual drift of an instrument or valve. Although the direction of failure may be dangerous there is often ample time for operations personnel to detect and correct the drift before the hazard is realised. Taking all of these factors into consideration, the frequency for a sudden dangerous failure of a BPCS control loop that leads directly to a hazardous condition can be significantly less than the 0.1/year typically used in LOPA.

So, does this mean we should be using 0.01/year as the dangerous failure rate for a BPCS control loop in a LOPA? The simple answer is 'no', as this would mean we stray into SIL-rated BPCS and all of the associated complications of this move. However, what the LOPA team should be aware is by using 0.1/year the answer from the LOPA is likely to be conservative and it is this conservatism that should be kept in mind when making decisions about further risk reduction measures. In the case of the Buffer Vessel as the LOPA stands the SIL target for PZ-123 is SIL2, but only just as a PFD_{avg} of 0.0083 is near the boundary of SIL1. So bearing in mind the potential conservatism in the analysis SIL2 maybe the correct answer numerically but SIL1 may be a more proportionate answer.

Independence of layers

A key rule of the LOPA method is that there should be a defined level of independence between initiating causes and IPL and also between IPL themselves. Very often in LOPA the 'defined level of independence' is often taken as 'complete independence'.

One of the initiating causes of the Buffer Vessel hydraulic overpressure is a dangerous failure of the BPCS level control loop (LIC-001). One of the layers of protection shown in Table 3 is the BPCS pressure control loop (PC-002) on the Buffer Vessel which upon detecting high pressure opens PCV-002 to vent the excess pressure to a safe location. Both loops are in the BPCS so applying the rule of 'complete independence' means they are non-independent and the pressure control loop cannot be claimed as an IPL. This is a conservative assessment. The question is whether this is too conservative.

If the common element, the BPCS, were to fail dangerously it is likely the majority of the plant would be impacted and probably come off-line in a major process upset so potentially the feed to the Buffer Vessel would be lost. A BPCS failure that impacts the pressure control and level control loops on the Buffer Vessel specifically is unlikely unless the controllers are located on the same I/O (Input/Output) card for example. If the controllers are on different I/O cards then a specific BPCS failure that impacts the pressure control and level control loops at the same time is extremely unlikely to the point where its contribution to the overall level of risk would be trivial. Potentially by claiming and demonstrating 'reasonable independence' such as separate I/O cards then a further BPCS layer of protection could be claimed. If the BPCS PC-002 layer of protection is now claimed it is conventional to apply no more than a risk reduction factor of 10, i.e. a PFD of 0.1 as per IEC61511, the LOPA target is now reduced from SIL2 to SIL1.

The risk reduction factor of 10 relates to an unrevealed failure of the BPCS layer, i.e. PC-002 fails to operate when a real high pressure demand occurs. If PC-002 is routinely used, for example, to vent down the Buffer Vessel once every 6 weeks as part of the normal process operations, then there is a chance a failure of this layer reveals itself under safe conditions. The operator cannot vent down the Buffer Vessel causing a delay but there is no overpressure hazard. Assuming a dangerous failure rate of 0.1/year for the pressure control loop and a maximum period of 6 weeks between venting down operations then the PFD_{avg} for the pressure control loop is numerically 0.1 x 6/52 = 0.01, which actually corresponds to a SIL1 reliability for a BPCS layer. Again this may not be claimed in a LOPA, but it does show further conservatism in the LOPA result which now moves from SIL1 to non-SIL.

Human error

A common initiating cause in LOPA is human error. In the case of the Buffer Vessel an initiating cause of hydraulic overpressure is an operator error during start-up as shown in Table 2. The assessment states that start-up is carried out twice per year, but what value for the Human Error Probability (HEP) should be used? Very often the default value is 0.1 which means once out of 10 attempts the operator will make an error. For the Buffer Vessel this means an operator makes an error 2 x 0.1 = 0.2 per year.

One of the drivers for the HEP of 0.1 is COMAH Guidance. The Human Factors Safety Risk Assessment Manual (SRAM) Appendix 12D Technical Criterion 10.2 states *'Use of generic HEP data is unacceptable unless it has been qualified to reflect the local circumstances or is more than or equal to an HEP of 0.1'*. The easiest option is to take the 0.1 which then may avoid the need to carry out a more detailed task analysis which can be time consuming. For tasks carried out several times per week or month then 0.1 may give an abnormally high initiating cause frequency which could raise the following problems:

- Human error initiating causes dominate over equipment or control failure causes.
- High initiating cause frequencies may push a SIF out of 'Low Demand' mode and into 'High Demand' mode.

In order to avoid the above problems there are some measures that can be taken. The first it to ask whether the human error frequency actually matches operating experience, the second is to carry out a numerical assessment of the HEP for which there are numerous techniques readily available such as SPAR-H (Standardized Plant Analysis Risk-Human) and HEART (Human Error Assessment and Reduction Technique). With these techniques it is relatively straightforward to numerically reduce the HEP below 0.1, however care should be taken particularly in terms of the training and competence of the user of such techniques.

In relation to the Buffer Vessel reducing the HEP from 0.1 to 0.01 does not significantly change the SIL target for PZ-123, therefore in this specific case the LOPA is relatively insensitive to the HEP.

A further observation on human error in LOPA relates to those situations where the hazardous event is based on human activity only in terms of both the initiating causes and also the layers of protection. Examples of such situations could include crane lifts over live equipment, confined space entry and purging of plant before and after maintenance. Even with numerical HEP techniques it is often difficult to robustly defend a HEP much below 0.01, and for the aforementioned situations where personnel would be always be present local to the activity, then it is very difficult to achieve a target risk criterion of 10^{-5} per year. This leaves a numerical 'risk gap', but how to close it? Take for example, purging of plant free of hydrocarbon vapour prior to entry that is carried out once per year. Applying a HEP of 0.01 with a probability of ignition of 0.5 and a person present of 1, then to achieve 10^{-5} per year target we are looking at a SIL2 risk gap, but what else can be done other than more procedural checks? It could be argued that forcing LOPA to generate a numerical answer in this case is the wrong approach, which may in turn give a misleading answer.

It is the experience of the author that one key problem in LOPA studies is failing to recognise that under certain circumstances LOPA is actually the wrong tool to use. This can be particularly apparent where a company procedure states the requirement to carry out a LOPA for all fatality events. Perhaps there are situations where a numerical tool such as LOPA is simply the wrong tool and it should not be used, other qualitative techniques may be more beneficial such as Task Analysis.

Conditional modifiers

Conditional modifiers relate to parameters such as:

- Probability of ignition
- Probability of vessel failure
- Probability person present
- Probability person injured

Take the probability of person present, in Table 3 a 0.1 probability is applied that an operator is in the area near the Buffer Vessel, thus 90% of the time the operator is away from the area and cannot be injured should the vessel rupture. So the risk of a fatality is reduced by an order of magnitude to allow for occupancy. The modifier does nothing to reduce the risk of a loss of containment or a fire with the associated plant damage and business loss, as a result they are often termed 'lucky factors'.

To remove this element of luck one approach that can be taken in LOPA is to not use 'lucky factors' at all, which means in the case of the Buffer Vessel the loss of containment will always find a source of ignition and a person will always be present. This approach means that credit is taken for only engineered layers of protection such as SIF and relief devices which can undergo formal testing and inspection routines to ensure their integrity. This will inevitably produce a more conservative result, for example in this case of the Buffer Vessel the original SIL2 SIF target is now increased to SIL3 which is likely to involve significant additional cost and may not even be practicable.

The question is whether this approach is correct. For example the Buffer Vessel may be located in a remote plant area, so an occupancy of 0.1 is sensible and it would be located in a zoned area with no obvious ignition sources so the probability of ignition may well be less than 1, so in effect using the 'no CM approach' means the real risk of fatality has been inflated by a factor of 10 to 100. Is this a problem? Well taking another common hazardous event such as internal explosion in a fired heater during start-up from cold. During start-up the worker is always at the control panel next to the fired heater and is always introducing an ignition source so occupancy and probability of ignition are always 1, so correctly no CM are applied. However, this means the Buffer Vessel has had its risk level inflated by a factor of 10 to 100 relative to the fired heater which has actually had the effect of distorting the risk profile for the site. The result of this distortion is that available capital could be spent on the Buffer Vessel first on a risk basis, whereas it could be more beneficial to spend it on the fired heater to provide a remote control panel. Applying the 'no CM approach' means the wrong decision is made.

In Table 3 the LOPA assumes a probability of rupture of the Buffer Vessel of 1 assuming the relief valve (RV-003) fails to operate on demand. The maximum pressure in the Buffer Vessel is 1.6 times its design pressure and it is also marginally above the vessel hydraulic test pressure, so as the vessel is outside of its known design envelope it is surely sensible to apply a probability of rupture of 1. However, for all pressure vessels designed to recognised codes there are inevitably design margins. For ASME code compliant vessels the design ultimate failure pressure has a significant margin above the Maximum Allowable Working Pressure (MAWP), as a result the ultimate failure pressure can be 3 to 4 times the MAWP. European code margins are generally less at 2.3 times MAWP. So it seems that overpressuring the Buffer Vessel to 1.6 times its design pressure is very unlikely to actually cause it to rupture. It could be argued the probability of rupture is of the order of 0.1 or even that a rupture would not occur at all but a probability of 1 could be applied that the vessel would suffer a joint leak instead, which may then be a lower consequence category event. So in this case assuming a more reasonable probability of rupture may mean the Buffer Vessel LOPA has over-estimated the risk of an on-site fatality event quite significantly.

So when applying CM or not, great care should be taken:

- Firstly, if CM are not used in LOPA then there needs to be an awareness that this may distort the overall risk profile of the facility with the potential to lead to incorrect decisions.
- Secondly, beware taking too much credit for CM. In a LOPA the engineered IPL should be applied first before the CM are applied, this is to avoid the situation where the LOPA risk target can be met using CM only. A final cross-check should be carried out to ensure CM do not still dominate the LOPA. For example if more than 20 to 30% of the total risk reduction to target is CM then the LOPA should be revisited.

LOPA examination summary

The Buffer Vessel LOPA as presented has applied the rules of LOPA in a sensible manner, the data used is not overly optimistic so overall the LOPA is a suitable and sufficient assessment of the risk. It has given a SIL2 requirement on the high pressure SIF based on a risk criterion of 10^{-6} per year for an on-site fatality event. Two options exist at this point, go ahead and install a SIL2 high pressure trip or alternatively review what the LOPA is telling the user and examine whether the answer from the LOPA is sensible.

As LOPA is a quantitative technique there is an understanding that the output is accurate. Consideration of accuracy is often only focussed on the quality of the failure rate data and the size of the population of equipment items or instruments over which it is collected. In effect, is the 'number' correct. It could be argued that this element of accuracy accounts for less than 10% of the overall LOPA accuracy, whereas more than 90% relates the assumption made in applying the LOPA method, in effect is the 'risk analysis' correct. This latter point is demonstrated in Table 5.

Option	LOPA inputs	On-site fatality frequency (per year) (based on SIL2 for PZ-123)
1	Applying the LOPA rules of complete independence and avoidance of all conditional modifiers	1.0×10^{-5}
2	Applying reasonable independence and appropriate use of conditional modifiers	2.5×10^{-7}
3	Applying reasonable independence and appropriate use of conditional modifiers and 0.01/year sudden dangerous failure rate for a BPCS control loop	1.7×10^{-7}
4	Applying reasonable independence and appropriate use of conditional modifiers and 0.01/year sudden dangerous failure rate for a BPCS control loop and 0.01 for HEP	2.5×10^{-8}
5	Applying reasonable independence and appropriate use of conditional modifiers and 0.01/year sudden dangerous failure rate for a BPCS control loop, 0.01 for HEP and allowing for detection of revealed failures of BPCS IPL	2.5×10^{-9}

Table 5 – Impact of applying different LOPA assumptions

What Table 5 shows is that there is a difference in risk by a factor of 4,000 between a strict LOPA (Option 1) and a LOPA that is potentially closer to the real situation (Option 5). Regardless of the actual numbers it is clear that in the case of this LOPA there is a substantial safety margin that is certainly sufficient to bring into question the cost of implementing a SIL2 high pressure SIF.

So this appears to leave us with a few questions, if the LOPA is so conservative what is its use? Should we break the rules of LOPA to get a more realistic answer? Is the Buffer Vessel LOPA wrong?

To answer this I repeat the first sentence of the LOPA summary *'the Buffer Vessel LOPA as presented has applied the rules of LOPA in a sensible manner, the data used is not overly optimistic so overall the LOPA is a suitable and sufficient assessment of the risk'*. The Buffer Vessel LOPA is perfectly adequate and even allowing for the discussion above, this paper does not suggest for a moment that the LOPA method as applied should be changed.

The most important next step is to understand what the LOPA is telling the user before any actions are taken to install additional hardware or redesign the plant. This aspect is explored in the next section.

Acting on the output from a LOPA

What to do?

What must be done is to demonstrate the risk associated with hydraulic overpressure of the Buffer Vessel is as low as reasonably practicable (ALARP). One option could be to design and install a SIL2 high pressure SIF, the event frequency is 10^{-6} per year and this can be considered ALARP. Another option is to look at what the LOPA is telling us.

The PZ-123 SIF target reliability is a PFD_{avg} of 0.0083 which is actually close to the SIL2-SIL1 boundary. Significant expenditure could be saved by claiming a PFD_{avg} of 0.01 (SIL1) with only a marginal increase in the overall calculated risk although bearing in mind there is already a substantial margin of safety in the LOPA. But on top of this it is important to complete the ALARP demonstration which applies the hierarchy of risk management and could be represented as shown in Table 6.

Without the ALARP demonstration step the LOPA team will focus on the SIL2 requirement and may not consider other options.

Guideword	Potential risk reduction measure	Feasibility of the option
Inherent	Re-rate the Buffer Vessel to withstand the maximum supply pressure.	Would require a replacement Buffer Vessel, by inspection the cost is grossly disproportionate.
Inherent	De-rate the feed pump to within 1.5 times the design pressure of the Buffer Vessel thus eliminating the rupture case.	Replacing the pump impellor could achieve this aim. Option to be progressed.
Control	Provide a BPCS function for start-up to avoid manual control of vessel level.	Feasible option to be progressed.
Prevention	Upgrade PZ-123 to SIL2.	Requires replacement of existing trip with SIL2 certified equipment. Cost benefit analysis suggests this option is disproportionate. Not required if inherent measures applied.
Mitigation	Relocate operator at start-up.	BPCS start-up function removes the operator from the vulnerable location during start-up.

Table 6 – ALARP demonstration

During a LOPA the LOPA team is analysing one hazardous event in detail, therefore it is sensible to carry out the ALARP demonstration at the same time with the same team. The ALARP demonstration has taken the focus away from the SIL2 answer, instead it looks at all aspects of the operation. The LOPA in Table 4 has shown the team that failure of LC-001 is the dominant initiating cause and Table 5 has shown the team that the Buffer Vessel will rupture at the current maximum process pressure and there is a high probability a person is present at start-up. This has the effect of focussing the teams attention on relevant risk reduction measures.

Perhaps the most interesting outcome of the ALARP demonstration is that if the inherent measure to reduce the head of the feed pump is carried out then not only is the requirement for a SIL2 high pressure SIF removed, but also the hydraulic overpressure hazardous event is eliminated. It was therefore worthwhile to wait before jumping to install the SIL2 SIF.

What not to do?

The ALARP demonstration approach described above actually means a demonstration is carried out on every individual hazardous event. This is a different approach from the conventional terms that are used to define what is ALARP which relates to the Individual Risk of Fatality (IRF) for the worker at greatest risk due to the cumulative impact of all hazardous events.

There may be a temptation to use the output from LOPA for every hazardous event on the site to calculate the IRF for the worker at greatest risk and then use this IRF value to compare directly to published criteria and decide whether the workers risk is ALARP. However, the sections in this paper have shown that LOPA as normally applied can be very conservative. In the case where a site has 100 very conservative LOPA that are then added together, the resulting cumulative IRF will be even more conservative. In simple terms if a site has 100 hazardous events each meeting their target frequency of 10^{-5} per year the IRF for the worker at greatest risk could be in the 'intolerable' risk region. This is not a feature of an unsafe plant, more a feature of using LOPA for something that it is not suited for.

Conclusions

LOPA is a time efficient and generally straight-forward technique that applies certain rules in order to calculate the frequency of hazardous events. The rules relate to the independence of protection layers, the reliability of BPCS functions and the use of conditional modifiers. This paper has highlighted that sensible application of LOPA rules can, on a case by case basis, give rise to a significant margin of safety in the results of the LOPA. The margin of safety is totally dependent on the process under consideration and a margin of safety cannot be taken for granted. If this safety margin is not recognised and analysed fully then there is a significant risk that the LOPA result can mislead.

This paper does not seek to change any rules associated with LOPA or how LOPA are generally carried out. It does however stress the need to critically review the result from each LOPA with awareness of the potential margin of safety in order to ensure that any subsequent expenditure on further risk reduction measures is allocated effectively.

All LOPA should be accompanied by a robust ALARP demonstration to support proportionate risk reduction measures.

References

Health and Safety Executive, “Reducing Risks, Protection People”, HSE Books, 2001.

IEC61511 “Functional safety - Safety instrumented systems for the process industry sector”, 2016.

Health and Safety Executive, Human Factors Safety Risk Assessment Manual (SRAM) Appendix 12D.