LOPA: Friend or Foe?

Alan G King, Hazard and Reliability Specialist, ABB Consulting, Pavilion 9, Belasis Hall Business Park, Billingham, Cleveland, UK TS23 4EB

Layer of Protection Analysis (LOPA) is not easy to do well. It seems really simple and straightforward. It gives a feeling of demonstrating adequate risk reduction, but often without properly getting to grips with the overall scenario. There is a false sense of security; a false sense that "all is well".

Layer of Protection Analysis has become widely used across many parts of industry. Indeed it could be described as the method of choice for risk assessment - for deciding what integrity level is needed for instrumented protection. The problem is that its very simplicity has led to its abuse. It is not being done consistently well, but the problems are not being recognised even by practitioners.

This paper will use case study examples to demonstrate a variety of significant issues and raise understanding of the shortcomings. It will outline ways of overcoming the problems to raise the standard of output of Layer of Protection Analysis. It is well known that we learn better from studying the errors of others, than from trying to learn from our own. This paper and presentation will present ways both for practitioners to learn to recognise some of the pitfalls, and for those who participate in LOPA sessions to be able better to support the leader and the other members of the team in the development of realistic LOPA scenarios.

Keywords: SIL Determination, LOPA, Layer of Protection Analysis, IEC 61511, IEC 61508

1. Introduction

All operators of hazardous processes have an obligation to manage the risks associated with those processes. This obligation relates not only to the potential impact of those processes on people (both employees and any others who may be affected) but also to the potential impact on the environment.

Layer of Protection Analysis (LOPA) has been around as a risk assessment methodology for many years. It gained more prominence following the publication of the international standard on functional safety for the process industry sector, IEC 61511 [Ref. 1] in 2003 and IEC 61508 Ed 2 [Ref. 2] in 2010. Since then, in the process industry sector LOPA has perhaps become the favoured methodology by large parts of that industry sector. Layer of Protection Analysis now has an arguably dominant position as the risk assessment technique of choice.

The title of this paper "LOPA: Friend or Foe" invites us to consider the way in which LOPA can lead to a false sense of security; the erroneous conclusion that the analysis demonstrates sufficient risk reduction.

LOPA appears to be a quite simple methodology and gives the impression that anyone can do a LOPA assessment, regardless of their depth of experience or training. It has become apparent over time that the quality of LOPA assessments, and the records of those assessments, has been highly variable; even from those who offer to lead LOPA assessments for others.

This paper reviews some of the shortcomings seen in real LOPA assessments, and provides insight into what to look for, and how to improve the quality of LOPA assessments.

The paper then looks into some of the potential causes behind those shortcomings, and what can be done in relation to those causes. The insights in this paper will be of value not only to those who take the role of leading LOPA assessments but also to LOPA team members who can help keep the assessment on the right path.

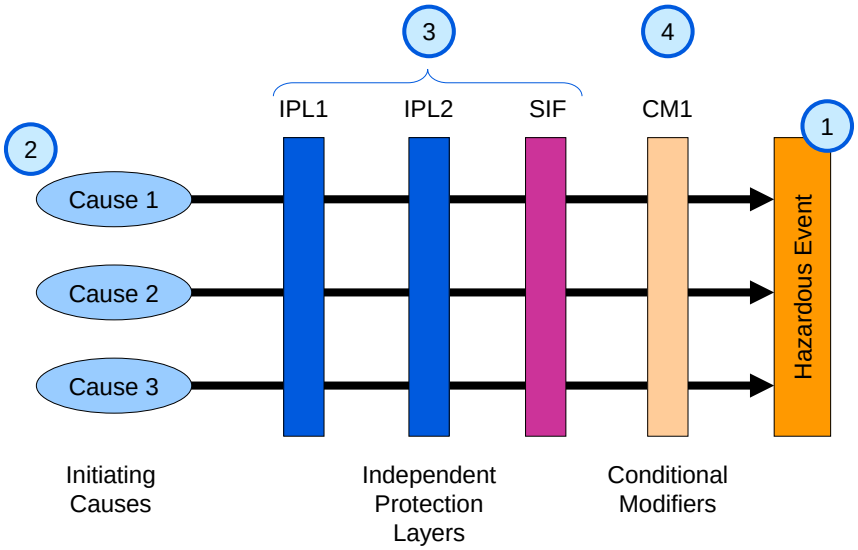
2. Background

Layer of Protection Analysis (LOPA) may be considered in its simplest form to involve four steps of identification, followed by the application of numeric values. The four steps are (1) identification of the hazardous event of concern, (2) identification of the causal failures or initiating causes, any one of which could trigger the occurrence of the hazardous event, (3) identification of those independent protection layers (IPLs), anyone of which, if working, could prevent the hazardous event from occurring, and (4) identification of any specific conditions[1] that are required for the hazardous event to occur - these factors are often referred to as conditional modifiers.

A typical hazardous event scenario is illustrated in Figure 1. The hazardous event here is shown as having three initiating causes, three independent protection layers and one conditional modifier. In Figure 1, one of the three independent protection layers is a safety instrumented function (SIF), such as a trip or an interlock function. The other IPLs may be functions also involving instrumentation or may be simple mechanical functions (such as a pressure relief valve).

[1] Conditional Modifiers can include conditions such as ignition, wind direction etc.

Figure 1 Layer of Protection Analysis (LOPA)



Once the overall scenario has been captured, fully understood and documented, the task then changes to one of applying numeric values to the features of the scenario. Figure 2 illustrates how the overall hazardous event frequency is calculated for the scenario shown in Figure 1. There is one row for each initiating cause. The first numeric cell in each row has the frequency of occurrence for the initiating cause. Each of the four subsequent cells in the row have values of probability[2] associated with the failure of each independent protection layer (IPL) or with a conditional modifier. These probabilities are multiplied along the row together with the initiating cause frequency for that row. The product for each row is noted in the final column as the intermediate event frequency contribution from that initiating cause.

Figure 2 LOPA Calculation for Figure 1

	Cause Freq. /yr.	IPL1 Failure Probability	IPL2 Failure Probability	SIF Failure Probability	Conditional Modifier Probability	Intermediate Event Frequency /yr.
Initiating Cause 1	0.1 /yr.	0.1	0.2	0.05	0.5	0.00005 /yr.
Initiating Cause 2	0.2 /yr.	0.1	0.2	0.05	0.5	0.0001 /yr.
Initiating Cause 3	0.6 /yr.	0.1	0.2	0.05	0.5	0.0003 /yr.
					Overall Hazardous Event Frequency =	0.00045 /yr.

The final task for calculation is to sum the intermediate event frequencies for each cause, to give the overall hazardous event frequency at the bottom of the right-most column. At this point, the overall hazardous event frequency may be compared with the operating company target frequency, for hazardous events of this severity, to determine whether the overall frequency is low enough to meet the target. It is also possible to leave the column for the SIF probability blank, and to determine what that SIF failure probability needs to be in order that the overall hazardous event frequency just meets the company target frequency.

However, effective Layer of Protection Analysis requires more than just the calculation. It requires documentation of the details of the overall hazardous event scenario - a description that takes the reader from the type of loss of control envisaged through to the potential consequences and the severity of those consequences. It also requires documentation of each of the initiating causes, why that cause is relevant to the overall scenario, and appropriate justification for the numeric frequency assigned to that initiating cause. A similar approach is required for each of the protection layers and the conditional modifiers - documentation of why that feature is relevant to the overall scenario, whether each feature applies equally to all initiating causes or just to some, and, if so, why. Furthermore, for each numeric probability value there needs to be appropriate justification to support the numeric value used.

[2] If for a particular initiating cause, a specific IPL or conditional modifier is not applicable, then a value of 1.0 can be put into the relevant cell and used instead for the intermediate event frequency calculation of that one initiating cause.

3. So what has been going wrong with LOPA?

As described, the LOPA methodology is straightforward enough and to many people involved with LOPA it can seem a simple approach to assessing risk. It is usually carried out by a team specifically gathered to undertake a LOPA assessment. The problem appears to be that for a number of LOPA teams and their leaders, they are not clear on the essentials. Let us explore some of the issues by looking at a number of real examples[3,4], illustrating where things have not been as good as they really need to be.

3.1. Hazardous Event Scenario Description

When it comes to the description of the overall hazardous event scenario, it is essential to be clear what the scenario actually is. Getting a good clear description can really help the team to focus. Have a look at Figure 3. Figure 3 shows a description that starts with a loss of containment. It tells us which equipment is involved but very little else. The inclusion of "Jet fire" presupposes that there will be immediate ignition rather than some form of gas release and potential for delayed ignition. As such, the description is immediately limiting the consideration of the team regarding ignition, by apparently ruling out any form of delayed ignition. It also provides no real indication of the reason for loss of containment. The description should indicate the type or class of failure that is leading to the loss of containment - telling how some form of "loss of control" of the process has occurred.

Figure 3 Hazardous Event Description - Example 1

	Description
Hazardous Event Scenario	Jet fire resulting from a Loss Of Containment (LOC) from equipment failure (start-up fuel gas heater HT-xxxx or fuel gas drum V-xxxx)

For another example, see Figure 4. This describes a leak of acetone from some pipework. However, there is, once again, no indication as to why the leak might be occurring nor, the type of failure that is being considered.

Figure 4 Hazardous Event Description - Example 2

	Description
Hazardous Event Scenario	Acetone pipework leak (continuous release through a 13mm hole of Xm3 of acetone at yy mbarg and 15°C)

Although in the example in Figure 4 there is some indication of the size of the release, there is no indication of the likely hazardous outcome that might result from the leak.

These are by no means isolated examples of poor hazardous event descriptions. They highlight some of the shortcomings that occur, and provide some understanding as to why some LOPA teams can struggle to get to grips with the scenario that they are assessing.

Figure 5 Hazardous Event Description - Example 3

	Description
Hazardous Event Scenario	1. Loss of control of level in V-2xxxx or other cause, leading to increasing level in V-2xxxx, resulting in liquid carry over to downstream gas systems 2. Production fluids begin to flow directly to the 1st stage HP suction scrubber 3. High liquid level in 1st Stage HP suction scrubbers 4. Compressor internal damage and potential loss of production

The example in Figure 5 shows some improvement. It indicates a sequence, from some form of loss of control of a feature (level), leading to liquid carryover, through to likely compressor damage. There are some tag numbers missing in relation to the suction scrubbers and compressor, but otherwise it is providing a clear sequence of events that the LOPA team can assess. This includes some broad description of what sort of loss of control has occurred.

Once the team have a clear understanding of the scenario and have a clear documented description of the sequence they are trying to assess, they can then look at identifying all the initiating causes for the hazardous event.

3.2. Initiating Causes

When it comes to identifying all the initiating causes in a systematic manner, there are various approaches that can be used. The use of demand trees has been outlined in the guidance contained in the Process Safety Leadership Group (PSLG) final

[3] Some of the examples are LOPA assessments in their final form. Others are not in their final form, but nevertheless are representative of the quality of output of the LOPA team that assembled to create them.
[4] Each example has been anonymised by amending the tag numbers or other factors that might suggest its origins.

report[5], Appendix 2, Annex 3 [Ref. 3], following the 2005 Buncefield incident. That guidance highlights the need, when identifying initiating causes, to consider all modes of operation: Normal operation, Start-up, Shutdown, Abnormal modes, Maintenance, etc. together with all classes of causal failure, including: equipment failure, failure of services, human failure, and external events, etc. Failure to conduct a systematic approach to initiating cause identification can lead to the missing of some of the initiating causes and so can lead to a serious underestimate of the overall hazardous event frequency.

For each initiating cause, it is important for the team to document why they have selected an initiating cause as relevant to the hazardous event. They also need to document the frequency that has been selected as appropriate for that initiating cause together with their thinking behind the selection. In other words, the team needs to document not just "what" they have chosen but also "why" they have chosen the initiating cause and its frequency.

Now have a look at the following LOPA entry in Figure 6:

Figure 6 Initiating Cause Description - Example 4

Description	Frequency /yr.	Justification
BPCS[6] Instrument Loop failure	0.1 /yr.	LIC8xxxx failure

In the example in Figure 6, the description is lacking the loop tag number (though part of the loop does appear in the justification box). The description is also lacking an indication of the (dangerous) failure mode that constitutes the causal failure for the hazardous event. What is needed is something more like: "Failure of BPCS Level Control Loop LC8xxxx, leading to closure of control valve LCV8xxxx causing rising level in vessel V-8zzz." It then becomes easier to see why that failure can cause the hazardous event under consideration[7]. As for the frequency used, there is no justification provided at all in Figure 6.

Now have a look at the following LOPA entry in Figure 7:

Figure 7 Initiating Cause Description - Example 5

Description	Frequency /yr.	Justification
BPCS Instrument Loop failure	0.1 /yr.	Operational experience is that this valve has not failed to open position in last five years.

In the example in Figure 7, the description is again lacking the loop tag number. The justification attempts to provide some rationale for the frequency of failure, but the text does not go far enough to provide a link to the actual numeric value used.

Here is a further LOPA entry looking at a more complex initiating cause in Figure 8:

Figure 8 Initiating Cause Description - Example 6

Description	Frequency /yr.	Justification
Manual valves HV-1234 and HV-1235 left closed in error following maintenance.	0.01 /yr.	This task is undertaken at a frequency of (1/yr.): 0.01/opportunity[8] x 1/yr. = 0.01/yr.

In the example in Figure 8, the description fails to discuss whether it really means either of the two manual valves or as the text describes the situation as "AND" implying that both valves need to be left closed to act as an initiating cause. Furthermore, the calculation does not discuss whether the operation of these two valves is sufficiently closely coupled that their operation can be taken as a single task or whether it is in fact two separate tasks and the frequency should be increased by a factor 2. A task frequency of 1/yr. has been used but there is no justification as to why 1/yr. is appropriate for this task. Is the task perhaps linked to some sort of regular activity that involves these valves? The justification should document what the maintenance activity actually is, if only so that the reader knows that, if the frequency of the activity changes, then there is an impact on the calculation for this LOPA assessment.

Too often, there is insufficient discussion of the nature of a task and the sort of error that could occur (whether a slip, lapse, or mistake) and what factors might affect the probability of error (performance shaping factors), to show that the failure and its circumstances have been properly understood. Where there is a lack of recorded detail about the task and the type of error, it suggests perhaps that the team have been simply lifting numbers from a reference table without the team really thinking about the task.

Here is a further LOPA entry looking at two interesting "initiating causes" in Figure 9:

[5] PSLG Final Report: Safety and environmental standards for fuel storage sites, HSE, 2009, ISBN: 978 0 7176 6386 6
[6] BPCS = Basic Process Control System
[7] In another totally different LOPA assessment, the initiating cause was expressed as: "Loss of Level Control (failure of LCV56zzzz)". This description also fails to recognise that any part of the level control loop can fail and lead to, in this case, "Low Water Level"
[8] Probability of 0.01 taken from LOPA reference tables provided by site operator.

Figure 9 Initiating Cause Description - Example 7

Description	Frequency /yr.	Justification
Drier leak	0.00012	See footnote [9]
Drier pipework rupture	0.000003	See footnote [10]

In the example in Figure 9, the *initiating causes* listed in the "Description" are more like consequences resulting from other causes. The frequencies shown must, by their nature, already include the effect of some risk reduction factors, but not necessarily those that apply to the plant under consideration. What is missing is any attempt to assess the actual initiating causes that could lead to a leak or rupture and then look at the relevant risk reduction factors for those causes. Furthermore, the consequence severities are likely to be different for each of the causes listed, and if so should not be in the same assessment.

It is understood that the background to those entries in Figure 9 was an attempt to use some form of quantified risk assessment report as the starting point for the LOPA. The message from this example is always to start from the hazardous event and then work back systematically to the initiating causes, as described earlier in Section 2.

3.3. Alarm Response as an IPL

Let us switch our attention to consider the inclusion of an alarm response as part of an independent protection layer. With LOPA there is a strong temptation for some LOPA teams to focus on the tag number of the alarm initiator and to insert a value of 0.1 with very little further consideration.

In Figure 10, there is a LOPA entry looking at response to an alarm:

Figure 10 Alarm and Response Description - Example 8

Description	Probability of Failure	Justification
Alarm 1	0.1	TAHxxxB. High temperature alarm. [11]

In the example in Figure 10, the tag number and description of the alarm is shown in the justification, whereas this information should be in the Description field. There is also a lack of any detail about what the operator is expected to do in response to the alarm. Probing further, it was found in the "Alarm Response Manual" for the facility that the "Corrective Action" listed for this fuel gas high temperature alarm was "Check temperature control valve in steam to heater TCV-zzz. Confirm by-pass closed. Check fuel gas flow from column." As we can see, there is nothing here that tells the operator to take some form of specific action to prevent the temperature of the fuel gas from rising further.

In addition, the "Alarm Response Manual" indicated that, although the alarm priority was classed as "High", the consequence for not responding to the alarm was listed as "Small - Commercial". Thus, we can see that reliance on this alarm for effective risk reduction does not seem reasonable; the operator is almost being led to think that the alarm is not overly important. In fact, the consequence severity for the scenario was dominated by safety considerations, and had been assessed as having the potential for up to 16 fatalities. This severity had clearly not been fed through to the alarm response manual.

There is in this assessment also no indication of how long the operator has from when the alarm is activated until any intervention by the operator will be too late to be effective. It turned out, that when the temperature rise was modelled, the time from the activation of the alarm, until the operator action of stopping the steam heating would be too late, was only a matter of a few minutes.

Overall, there is not sufficient recorded to justify the probability figure of 0.1 put in the LOPA table, and a figure of 1.0 would be more reasonable!

The point here is that, for alarm layers, it is important to think about the whole layer from the sensor though to the effective corrective action. There needs to be a clear instruction for the correct operator response, good explanation as to why the response is required, and ample time for the action to be completed once the alarm has activated. Otherwise, the operator is being "set up for failure". Furthermore, all features of the alarm layer, including the means of operator action, need to be independent from the initiating cause and from all the other layers in the scenario.

Here is another LOPA entry looking at response to alarm in Figure 11:

[9] Apparently based on reference for "partial failure of flammable vessels" - doubled for two vessels
[10] Apparently based on a reference for "rupture of pipework with a diameter greater than 100mm" and 10m of pipework.
[11] Probability of 0.1 taken from LOPA reference table provided by site operator.

Figure 11 Alarm and Response Description - Example 9

Description	Probability of Failure	Justification
Low Temperature alarm from TAL-5xxx	0.15	Alarm is independent. Assumption is that the operator has clear procedures to follow in the case of an alarm and at least 20 minutes to act before the hazard can occur. …
High Level Alarm from LAHH-5zzz - isolation of feed	0.1	Isolation of feed to evaporator …

In the example in Figure 11, there are two alarms listed. In the associated LOPA from which this example was taken, for some initiating causes, both alarms were claimed as risk reduction measures. There is no recorded discussion regarding whether these alarms go to different people and what degree of independence there would be. If the alarms are in the same control room for response by the same person, then it would be more defensible to include only one alarm.

There is no discussion as to why a larger value of failure probability has been used for the temperature alarm compared with the level alarm, nor indeed any clear justification for either numeric value. It also sounds as though the alarm response for the low temperature alarm has not, at the time of the LOPA assessment, even been defined.

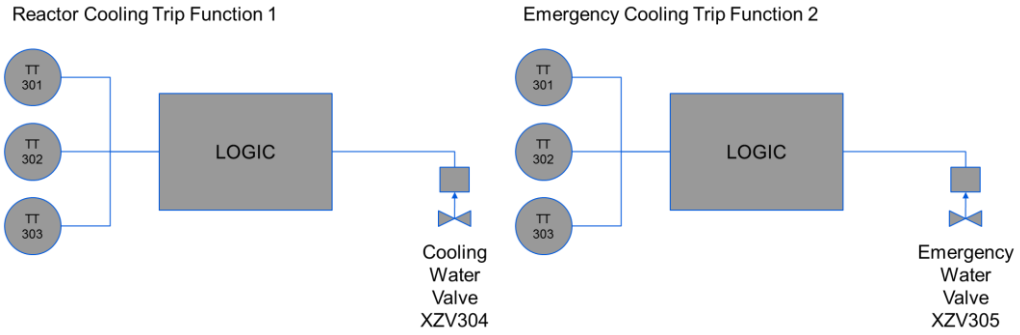
This raises the issue of ensuring that the LOPA only includes those IPLs and measures that are actually part of the design at the time of the LOPA assessment. Those which are merely "under consideration" for inclusion in the design should not go into the LOPA.

3.4. Safety Instrumented Functions

With safety instrumented functions (SIF), there is still a tendency to consider each sensor as a separate safety instrumented function and to put the sensors into the LOPA record as separate IPLs. The same applies to valves; sometimes valves can be mistreated as separate IPLs when they are really part of the same function.

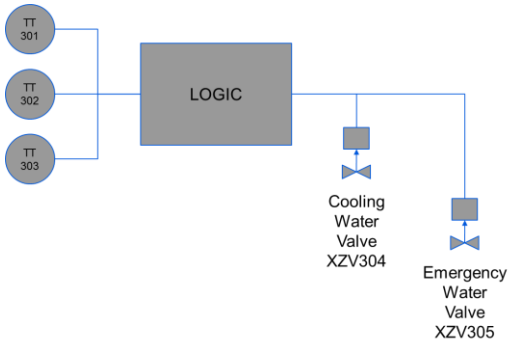
Consider the following two diagrams in Figure 12.

Figure 12 Safety Instrumented Functions?



These two examples of instrumented functionality were found as separate IPLs in a LOPA assessment. Both were credited as protection against reaction runaway[12]. Closer inspection reveals that these apparently separate functions actually use the same set of temperature sensors. All the sensors and both valves are really part of the same function and should be considered as a single IPL with an architecture as shown in Figure 13.

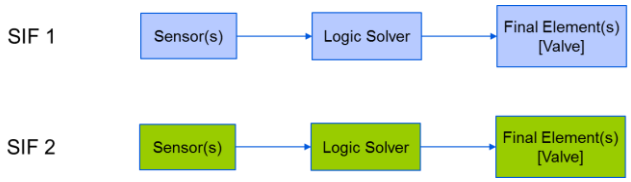
Figure 13 Single Cooling Water Trip Function



[12] It should be noted that in this example, the cooling water and the emergency water were two separate independent supplies/means of cooling.

The same confusion and over claiming can occur where there are separate sensors, but the same valve(s). It is really important that when it comes to safety instrumented functions that each function can be defined in a way that demonstrates that they are complete: the function has its own sensor(s) and its own means of creating a safe state - final element(s) - see Figure 14.

Figure 14 Separation of two Safety Instrumented Functions (SIF)



In Figure 14, separate logic solvers are shown for the two functions. However, if the two functions (SIF1 and SIF2) are intended to provide an overall level of risk reduction of, say 200, then this would be equivalent to a single function with a performance[13] in the range for Safety Integrity Level (SIL) 2. Therefore, the two functions could utilise the same logic solver provided it has been designed as suitable for SIL 2 operation.

3.5. Conditional Modifiers

Conditional modifiers are potentially a quite difficult aspect of LOPA. In many instances, they are not used well and justification for their use is often very poor. This section looks at a couple of specific modifiers and then makes some more general observations on modifiers and their combined impact.

3.5.1. Occupancy

Occupancy is a challenging aspect to consider. It relates to the probability of enough people being in the vicinity of the incident that the severity level of the safety consequence could be realised.

This example relates to a scenario where there are two initiating causes. One initiating cause is failure of a BPCS control loop during normal operation. The second initiating results from a bypass valve being left open following maintenance activities. The following table, in Figure 15, shows the Occupancy entry in the LOPA assessment.

Figure 15 Occupancy - Example 10

Description	Probability	Justification
Occupancy	0.27	Day staff are within the building during the day working 8hr per day, but only 5 days per week.

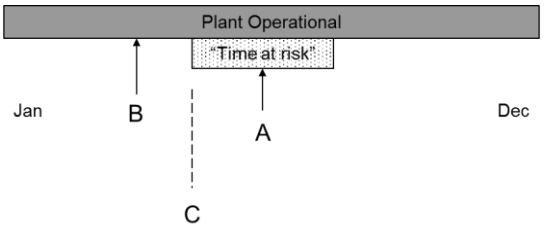
Apart from a small numeric slip[14] with the calculation of 0.27, this occupancy value appears reasonable, but it has been applied to both initiating causes. For the BPCS control failure, the occupancy figure might be reasonable. For the initiating cause associated with the bypass valve, it is not reasonable. This second initiating cause will be manifest at process start-up, and, in this case, for start-up the probability of having people around will most likely be 1.0 - people need to be present during start-up.

This example emphasises how important it is to consider conditional modifiers against each initiating cause and not to assume that one value applies to all causes[15].

3.5.2. "Time at Risk"

The conditional modifier known as "time at risk" is perhaps the most poorly understood and most abused factor in the whole of LOPA assessment process. The problem with "time at risk" is that is can be tightly linked with the initiating cause and other factors. Consider the following diagram in Figure 16.

Figure 16 "Time at risk"



[13] PFDavg = 1/Risk Reduction. PFDavg = 1/200 = 0.005. A PFDavg of 0.005 is in the range for SIL2.
[14] Calculation of 8 x 5/(24 x 7) = 0.24
[15] Some LOPA recording sheets do not allow this separation of occupancy across different initiating causes, and so lead to errors in the assessments.

Consider the plant to be operational throughout the calendar year. Consider a period of time, say 20% of the year, labelled "time at risk", during which the process is vulnerable to some sort of equipment fault or other failure as an initiating cause. Such a failure during the "time at risk" (e.g. at "A") leads to the hazardous event. If the 20% factor of "time at risk" is used in the LOPA assessment, it implies that the equipment fault occurring outside the "time at risk", for example at "B", does not lead to the hazardous event. However, the use of the 20% factor is only valid if the operation of the facility is such that it is possible to guarantee (100%) that the "time at risk" will never be entered with the fault already having happened. In other words, the operator of the facility must be able to guarantee that any fault that occurs at "B" will never be permitted to pass "C", even if the fault is unrevealed until the "time at risk". Such a guarantee is in general not realistic, and the use of the "time at risk" factor therefore becomes invalid.

Should the initiating cause failure be associated with a human task carried out in relation to the "time at risk", e.g. as part of a start-up activity, then once again the "time at risk" factor should not be used.

It is comparatively rare that the "time at risk" factor is valid as part of a LOPA assessment, and the reasoning must be documented carefully and rigorously. Even quite carefully argued justification for "time at risk" can on closer consideration be found to be flawed.

3.5.3. General thoughts on Conditional Modifiers

Conditional modifiers are a concern. If there are, for example three conditional modifiers each with a probability of 0.1, then the overall probability is 0.001. This should automatically raises cause for concern. The risk reduction from such a combination is almost equivalent to a safety instrumented function of SIL 3. The level of scrutiny and evaluation for a SIL 3 instrumented function would be considerable. The same should apply to modifiers.

The following example is taken from an actual LOPA assessment:

- Time at risk 0.0027
- Probability of vessel failure 0.1
- Occupancy 1.0
- Probability of ignition 0.5

Overall, the probability from these conditional modifiers is 0.000135 or a risk reduction factor of just over 7000. This magnitude of equivalent risk reduction should certainly trigger a very high level of scrutiny.

Pragmatically, the limiting of the overall contribution from all conditional modifiers together to a value of 0.01 might be considered more reasonable, or at least be a threshold to trigger more detailed examination. For conditional modifiers, the level of support (justification) for each should be sufficiently robust that any reviewer would be confident that the value claimed will be maintained over time.

It is also important to be sure that the conditional modifiers are truly independent of each other and independent from the initiating causes and the IPLs in the scenario.

4. What is causing some of these issues

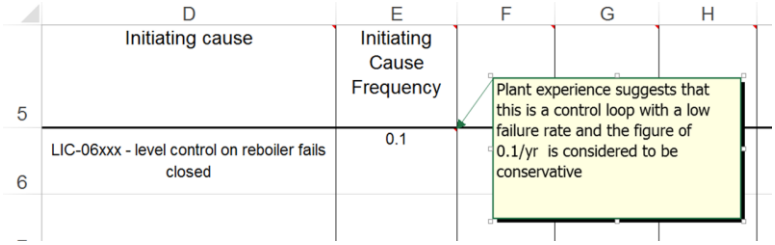
4.1. LOPA Recording Sheets - styles

There are a wide variety of styles of recording sheets used for LOPA. Some of them help the team to record all that is required and others make the work significantly more difficult than it needs to be.

4.1.1. Recording Sheet - Example A

Figure 17 shows one style that is based on a simple spreadsheet. There is space for the description of the initiating cause. However, there are no units shown for the frequency - the reader has to assume that it is 'per year'. Worse is that the justification is held as a 'Comment'; the comment only appears when the cursor hovers over the corner of the frequency cell. This means that the team are unable to see the whole story from the normal spreadsheet view. Furthermore, the comments do not appear when the spreadsheet is printed.

Figure 17 Example A - Recording Sheet



However, this style of sheet does put the layers, side by side to show the scenario development and how the intermediate event frequency is reached - see Figure 18. This feature of the layout does assist the team with understanding the scenario and how it progresses.

Figure 18 Example A - Recording Sheet (2)

		INDEPENDENT PROTECTION MEASURES					
Initiating cause	Initiating Cause Frequency	BPCS	Human Response to Alarms	Mechanical pressure relief device.	SIS (PFD_{actual})	IPL additional mitigation dikes,	Actual Mitigated Event Likelihood
LIC-06xxx - level control on reboiler fails closed	0.1						

4.1.2. Recording Sheet - Example B

The next style of recording sheet (Example B) has been generated by a commercial software package. For initiating causes, shown in Figure 19, there is plenty of opportunity to record the justification in the "Data Source" column.

Figure 19 Example B - Recording Sheet - Initiating Causes

Initiating Events			
Initiating Event	Data Source	Freq. (/yr)	Comments
1. HV-1xxx and HV-1zzz left closed in error following maintenance.	1.Taken from: ...	1.00E-02	

For IPLs, the Example B recording sheet (see Figure 20) has a column for the tag reference, a description of the IPL and any "set point" and the failure probability of the IPL. However, there is no location for recording the justification for the PFD value, other than perhaps in the "Description" column. As a result, the team omitted recording on the sheet any justification for the value used.

Figure 20 Example B - Recording Sheet - IPLs

Independent Protection Layers				
Tag #	Description	Set point	PFD	RRF
PAHH-1xxx	PAHH-1xxx located on Separator ZZZZ	30 barg	0.034	

It has another drawback in that the IPLs for the same initiating cause are shown vertically as in Figure 21, instead of side by side:

Figure 21 Example B - Recording Sheet - IPLs (2)

Independent Protection Layers				
Tag #	Description	Set point	PFD	RRF
PAHH-1xxx	PAHH-1xxx located on Separator ZZZZ	30 barg	0.034	
PSV-1zzzA/B-1 and PSV-1xxx-XXA/B Partial Load	Partial Load for operational cases with multiple wells: PSV-zzzA/B-1 located on the Separator YYYYA/B and PSV-1xxx-XXA/B	40 barg 40 barg	0.02	

This makes it more difficult than need be for the team to appreciate the scenario that they are putting together during the LOPA assessment. By contrast, the inclusion of a column for the set point is helpful, as it indicates the sequence for triggering the IPLs.

4.1.3. Recording Sheet - Example C

Figure 22 shows another form of recording sheet. This has the IPLs adjacent to each other and at the end of the row the Mitigated (Event) Frequency for that initiating cause.

Figure 22 Example C - Recording Sheet - Initiating Causes and IPLs

IE Ref	Initiating Event and Enabling Conditions	Frequency (per year)	IPL	PFD	IPL	PFD	IPL	PFD	IPL	PFD	Mitigated Frequency
A	Temperature rise in vessel due to loss of water level control - failure of TC-1xxx	0.1	High temperature alarm and response (TIA-12xx)	0.1	Low water level trip (LIZA-1zzz)	0.02					0.0002

Figure 22 has the benefit of showing the story in an easier to appreciate form. However, it has no specific column for recording the "Justification" behind the IPL and the numeric value chosen. The users of this particular style of recording sheet used a separate document for the justifications, making the overview of those aspects really difficult both for the LOPA team and for any LOPA reviewer.

4.1.4. Recording Sheet - Example D

Figure 23 shows another variation of recording sheet. This style has been used by a number of organisations. The section for initiating causes has both a Description field and a Justification field. This assists by prompting the LOPA team to put in all the information required. The same is true for Figure 24 which covers IPLs and Conditional Modifiers. Figure 25 shows the associated style of calculation grid. There is another section of the recording sheet (not shown here) that covers the scenario description and its consequences.

Figure 23 Example D - Recording Sheet - Initiating Causes[16]

#	Description	Frequency /yr.	Justification
A	BPCS Instrument Loop failure. LC-5224. Level control valve in closed state.	0.1 /yr.	Operational experience is that this valve has not failed to open position in last five years.
B	Manual valves HV-1234 and HV-1235 left closed in error following maintenance.	0.01 /yr.	This task is undertaken at a frequency of once a year (1/yr.): 0.01/opportunity x 1/yr. = 0.01/yr.

Figure 24 Example D - Recording Sheet - IPLs[17]

#	Description	Probability of Failure	Justification
1	Low Temperature alarm from TAL-5xxx	0.2	Alarm is independent. Operator has clear procedures to follow in the case of an alarm and at least 20 minutes to act before the hazard can occur. …

Figure 25 Example D - Recording Sheet - Calculation Grid

PFDavg Calculation						
Initiating Cause	Freq. (/yr.)	Independent Protection Layers				Intermediate Event Frequency (/yr.)
		1	2	3	4	
A	0.1	0.2				0.02
B	0.01	0.2				0.002
					Total Event Frequency Fe/yr.	0.022
					PFDavg for Additional Safety Instrumented Function, Ft/Fe	0.0045
					Safety Integrity Level =	SIL 2

The bottom two rows in Figure 25 are optional features for situations where a SIF has not been included as an IPL and it is desired to assess the integrity requirements for that SIF.

[16] These tables are populated to show what information normally goes in which field. It is not intended that the populating of these tables illustrates best practice in recording of such information.
[17] These tables are populated to show what information normally goes in which field. It is not intended that the populating of these tables illustrates best practice in recording of such information.

Example D represents one of the better recording sheet options available.

4.2. LOPA Recording Sheets - Pre-population

From time to time, the topic of pre-population of LOPA recording sheets arises. This is where someone, ahead of any LOPA team meeting, enters on the recording sheet the description of the hazardous event scenario, together with descriptions, frequencies or probabilities, and perhaps the justifications for initiating causes, and IPLs etc.

Initially, pre-population seems a good idea - it is seen as saving time and giving the LOPA team a ready prepared recording sheet for each scenario. It has even been suggested that someone does the whole LOPA assessment before the team meeting and simply presents the result to the team for their approval.

The problem with pre-population of LOPA recording sheets is that it has the effect of disabling the thinking process for the LOPA team. Initiating causes already entered are less likely to be challenged or removed. The team are also less likely to look for additional initiating causes. The team is quite likely to accept the assessment exactly as presented to them without critical challenge. This is not what is required for a rigorous analysis.

Whilst it is reasonable to enter the outline of the hazardous event scenario on the recording sheet as a starting point for the LOPA team, the team should be expected to develop the assessment themselves. That is surely the whole reason for gathering a LOPA team together - to have the relevant range of experience and expertise around the table and so ensure that the LOPA scenario is realistic, rigorous and complete.

4.3. Teams and leaders

What constitutes competency for teams and for leaders? Clearly from the observations described in this paper, there are significant competency issues. Those leading teams need to be thoroughly aware of the LOPA methodology AND especially its limitations. It is to be encouraged that team leaders are not only trained and experienced with LOPA, but also have experience that goes beyond that to embrace Event Tree Analysis and Fault Tree Analysis. The leader is then able more easily to recognise when the assessment is too complex for LOPA, and to go for a more suitable methodology.

It is also important for the team members to have a clear understanding of the LOPA methodology - either by attending a separate training course, or to have a session at the beginning of the LOPA assessment meeting, led by the LOPA leader, to provide an introduction for them.

Most LOPA assessments will make a list of the members present and their role in the team. The core team roles will typically include:

- Process Engineering
- Control and Instrument Engineering
- Operations (someone with direct experience of operating the process being discussed or a similar process)
- Process Safety Engineering

However, if the equipment involves rotating machines (compressors and pumps etc.) then having a specialist machines engineer present is exceedingly helpful. Without such specialist input, the LOPA team will be tempted to “guess” or “estimate” what might happen - inevitably leading to mistakes. The same is true for packaged equipment - get one or preferably two vendor representatives to be present for the LOPA sessions. If the scenario involves low temperature embrittlement, then get a materials specialist to attend the LOPA meeting, but make sure that you provide them with adequate information to allow thorough preparation before the meeting. Failure to have all the relevant specialists present can easily lead to the LOPA team reaching the wrong conclusion.

It is good practice at the meeting to record not only who is present for each assessment, and their roles within the team, but also the experience that each person present has. This is to record the justification why a person is able to fulfil the role assigned to them.

It is also important that there is commitment from the team members; someone busy doing email or other non-LOPA activity during a meeting is just not acceptable.

4.4. Information and Conditions

4.4.1. Information

It is important that the information made available to the team is up-to-date. There have been occasions when it is apparent that major changes have been made to the equipment but not reflected in the drawings and other documentation. One LOPA assessment is remembered where the drawing showed four tanks and the team admitted that two had been removed six months previously, but there was disagreement as to which two of the four tanks on the drawing remained.

It is also important to have printed copies of the documentation (such as P&IDs) for each team member. Team members will often check on information individually during the LOPA assessment and pick up on different issues before raising them with the rest of the team.

4.4.2. Conditions

LOPA assessments are usually held in some form of meeting room. It is important to provide a good environment for the team. Facilities should include: refreshments (tea/coffee/water even biscuits and fruit), natural light (if at all possible), space to get up and walk around, comfortable seating, good projection facilities (even with dual screens), wall-space for putting up drawings or other reference diagrams, network or internet access for additional information, etc. It is all about creating the conditions for getting the best out of the whole team.

One key aspect that is often overlooked is that of team fatigue. Trying to undertake LOPA from 9am to 5pm, 5 days a week for several weeks, can sooner or later lead to *burn-out*. Keeping the sessions shorter: start at 09:30 and run until 16:30 with breaks mid-morning and mid-afternoon can help improve the quality of the LOPA assessments. Limiting the LOPA sessions to Tuesday to Thursday (3 days) can actually improve productivity - it allows time for gathering additional information at the beginning of the week ready for the LOPA sessions. At the end of the week there is time for reviewing the work that has been done.

5. Conclusions

While LOPA is often seen as a simple, straightforward technique, this paper has shown that LOPA routinely suffers from poor application. Indeed it is a significant challenge for a LOPA team to develop and record a realistic, rigorous, and complete scenario for each hazardous event of concern.

The paper has discussed a variety of aspects of LOPA assessments where the performance and the quality of assessments has been less than optimal. It has focused on a number of shortcomings, and provided appropriate comment and guidance for improvement.

It is vitally important that the application of LOPA is improved and the quality of the assessments rises so that the issues highlighted in this paper become things of the past. The responsibility for the improvements lies not only with LOPA leaders but with the whole team. Anyone in the team can see where the record is missing tag numbers, or has a less than clear description of a function, or poor justification to support a numeric value. All those present should fully commit to achieving quality.

In summary, what has been missing from many of the LOPA assessments has been sound logic. The records have also lacked clear and unambiguous records of WHAT the LOPA team concluded, but more crucially they have lacked the very detail to explain WHY the LOPA team decisions were made - the justification and support for the statements made.

6. Acknowledgements

The author would like to thank colleagues and others who have shared insights into LOPA and provided the opportunity to discuss and review aspects of LOPA assessments.

7. References

1. International Electrotechnical Commission, 2003, IEC 61511 Functional safety – Safety instrumented systems for the process industry sector, Parts 1 – 3, Geneva, Switzerland
2. International Electrotechnical Commission, 2010, IEC 61508 Ed 2 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 – 7, Geneva, Switzerland
3. “Safety and environmental standards for fuel storage sites”, Process Safety Leadership Group, Final report, HSE, 2009. ISBN 9780717663866