Risk reducing outcomes from the use of LOPA in plant design and operation

Paul Feltoe

Safety Solutions Ltd

Background

Layer of Protection Analysis (LOPA) has been traditionally applied to assess scenario risk levels and determine safety function Safety Integrity Levels (SIL). In this paper, the author aims to give an appreciation of the types of situations where LOPA could be used to provide an insight into higher hazard operations in order to reduce risk, and to highlight the fact that it is not exclusively a tool for SIL assignment. The paper does not aim to give an in-depth methodology into LOPA.

Process risk can be reduced by the application of inherent safety, reducing the likelihood of human error, choosing simpler designs or adding rated safety functions. Displaying the LOPA as a bowtie, simply communicates the plant risk profile to a wide audience including external parties such as the regulator and provides meaningful actions to reduce the risk for each identified scenario. Improvements such as relocating control rooms, moving specification breaks, optimising valve arrangements to reduce the opportunity for human error and changing process designs are all possible outcomes of LOPA reviews.

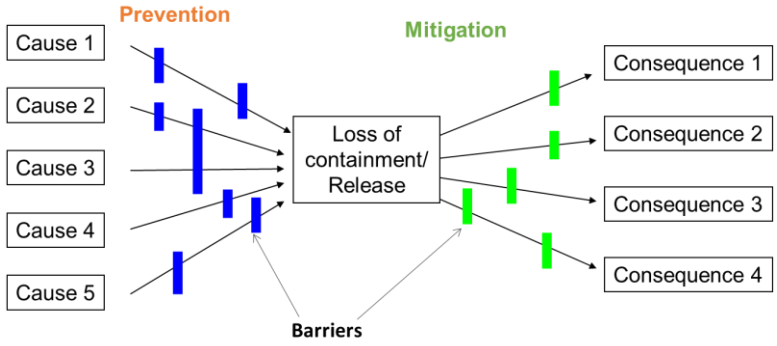
Introduction

Risk assessments have long been a means to demonstrate that process plant hazards have sufficient controls in place to ensure the likelihood of consequences being realised are within tolerable limits. There are a number of techniques utilised in industry, from simple qualitative techniques to the more complex quantitative techniques such as QRA. However, in the last 10 years, Layer of Protection Analysis (LOPA) has emerged as an additional method whereby operating companies' can assess their process hazards risks and obtain meaningful information to assist in the reduction of their risk profile.

This paper presents 5 lessons that LOPA facilitators and plant operators can apply to facility risk management.

The incident pathway and the bow-tie

Process accidents usually involve more than one cause, have several preventive barriers, and some mitigation barriers. The accident pathway can be illustrated using a bowtie such as shown below.



The aim of risk assessment

Risk assessments aim to demonstrate whether or not a hazard has sufficient controls in place to reduce the likelihood of an undesirable consequence from occurring. There are several techniques available that meet this broad requirement:

1. Risk matrix (simple and calibrated)
2. LOPA
3. Fault tree (for common cause failure)
4. QRA – e.g. risk profiling of land planning type applications

The above techniques can be supplemented by consequence modelling to improve the fidelity of the assessment.

The core aims of process safety risk assessment are:

1. From a process safety perspective, to demonstrate that the facility is safe, and identify what scenarios or hazards could make it unsafe and what are their causes. This is typically done using Hazard ID techniques such as HAZOP or PHA reviews.
2. To identify the barriers for each hazard that control the risk. Here barriers that both prevent and mitigate risk are considered.
3. To assess if these barriers are sufficiently robust, or if additional risk reduction is required.
4. To define what management systems are needed to ensure the causes and barriers are in accordance with the risk assessment assumptions.
5. To facilitate “as low as reasonably practicable” (ALARP)/ or “so far as reasonably practicable” (SFARP) assessment.
6. Communicate this to the workforce and interested parties.

The above needs are largely aligned with requirements in Australian and New Zealand's Health and Safety legislation. Table 1 highlights how, in the author's opinion, the various techniques meet these needs.

Need	LOPA	Fault Tree	Risk Graph (for SIL assessment)	Risk Matrix
Scenario cause and barrier identification	H	H	M/L	L
Systematic Barrier Assessment	M	M	L	L
Facilitates ALARP assessment	H	M	L	L
Management System/ Performance standards	Once barriers are identified, performance standards can be developed	Once barriers are identified, performance standards can be developed	n/a – not connected to risk assessment activity	n/a – not connected to risk assessment activity
Communication of risk and controls to workforce and interested parties	H	L	M	L
Team activity	H	L	H	H
Complexity (an attribute)	M	H	L	L:

H = Technique clearly meets needs, M = Technique partially meets needs, L = Technique barely addresses needs

Table 1: Risk Assessment Needs vs Techniques

Using the above approach, the author considers that LOPA is a strong tool for risk assessment, which adequately caters for the needs defined above, while striking a balance between simplicity and depth. The use of QRA has been excluded from the above as it does not meet the needs identified above. QRA in this paper refers to techniques used to generate risk profiles.

Introduction to LOPA and key issues

LOPA originally emerged in the US as an order of magnitude technique for SIL assessment that took into account:

- The causes of events and how frequently they occur
- The barriers that prevents the central event (LoC) from occurring and how effective they are.
- Mitigation factors that reduce the likelihood of the consequences being realised. These are factors such as ignition, explosion likelihood and exposure modifiers such as the time a person is in the danger zone.

The original method has evolved into a bow-tie technique for process safety risk assessment that incorporates:

- Multiple initiator aggregation - including human error, equipment and instrument failures
- Failure rates for initiators and barriers (eg SIF functions)
- Conditional modifiers that are supplemented by consequence analysis.

The application of LOPA has two variants:

1. Instrument Engineering Centric - LOPA used only for SIL assessment. The drivers for SIL assessments have historically been associated with instrument engineering groups and often the focus is the determination of the SIL level and not assessment of the hazard and the risk. The author has observed that this often assumes only one initiator.
2. Risk Centric – LOPA is used as a risk assessment tool where SIFs are only one of several barriers considered. A bow-tie is built to represent the scenario and considers all causes of the hazard including human error.

In 2009, the UK HSE Process Safety Leadership Group's (PSLG) final report into the Buncefield incident was published. Appendix 2 of this report details guidance on the appropriate use of LOPA. The PSLG's investigations into the use of protection systems on tank farms, had documented varying LOPA standards being used within industry which was leading to significantly different outcomes (required barriers, SIL levels etc). The use of advanced LOPA which includes multi-initiator aggregation of risk alongside the appropriate application of data was a core recommendation. Many organisations are now using a bow-tie to graphically depict and communicate the use of the technique.

Case Study Benefits

The following examples have been developed from real studies with similar outcomes to illustrate the types of benefits and issues that can arise. All failure rates and independence requirements were agreed by the team which involved a wide range of technical, operations and maintenance staff. Whilst not the topic of this paper, all barriers, initiators and conditional modifiers were justified and consistent with good practice norms (eg CCPS).

Case Study 1: Liquid Pipeline

Scenario: A 30+ km hydrocarbon pipeline transporting a hydrocarbon with an intermediate pump station had a number of mid line valves (MLVs) that were in need of a programmable logic controller (PLC) upgrade to replace the existing "end of life" PLCs. The PLC vendor proposed to upgrade them to safety rated PLCs at a high cost. There was no risk assessment to support this recommendation. The pumps on the pipeline were already fully fitted with an independent Safety Instrument System (SIS) trip system with functions protecting high and low pressures around the pumps.

The function of the MLV PLC's was to shut-down the pump stations should a low pressure be detected (low pressure trip upstream of the MLV) which could lead to a vapour pocket forming in the pipeline. Starting up with a vapour pocket in the pipeline would potentially rupture the pipeline, leading to a significant environmental incident.

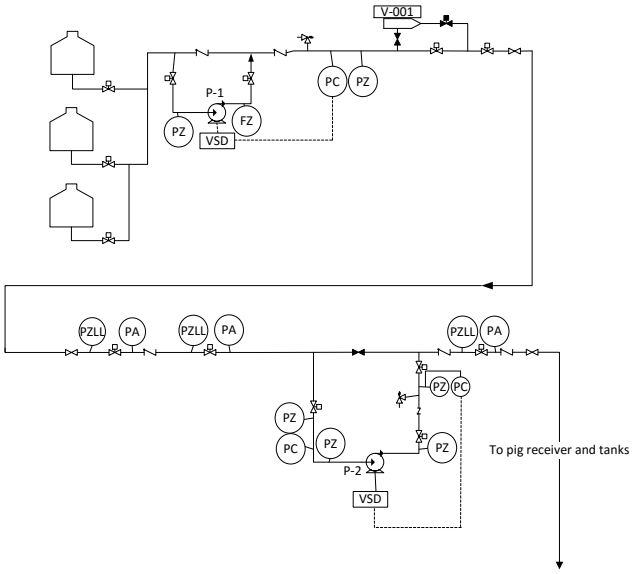


Figure 1: Pipeline PFD

The Study: A LOPA study was conducted to determine if the existing PLC safety function (low pressure trip upstream of the valve) needed to be Safety Integrity Level (SIL) rated or was non-SIL rated function sufficient. The study captured pump, valve and instrument failures as causes of a potential rupture in addition to human factor contributors. The following simplified bowtie represents the barriers and initiators. It can be seen there were multiple potential causes of the event, but also there were many independent barriers.

		Barriers 1	2	3	4	5	6	7	8	9	10			
	IE #	Limit switch	PZA HH	PZA LL	PZA	SOP1	PIC	SOP2	Interlock	PZA	PIC	Barriers PFD		Overall mitigated frequency of failure
1	MLV failure	x	x	x	x	x						0.0000001	Rupture on restart leading to large environmental incident	2.00E-08
2	XSV fail		x	x	x	x						0.000001		6.70E-08
3	MV misop		x	x	x	x						0.000001		2.00E-09
4	P1 Failure			x	x	x	x	x				0.000001		1.34E-07
5	XSV fail			x	x	x			x	x		0.0000001		1.00E-08
6	RV open			x	x	x				x		0.000001		1.00E-08
7	PIC fail			x	x	x				x	x	0.0000001		1.00E-08
8	Lineout error			x	x	x				x	x	0.0000001		1.00E-07
														1.00E-05
														3.53E-07
														Target Met

Figure 2: Pipeline LOPA Bowtie

Key outcomes from study:

1. It was determined that the liquid filled pipeline transmitted pressure very quickly along the pipeline such that protection systems several km away at the pump sites (P1 & P2) were sufficient to protect against failure of the MLV. Local protection at the MLV's were not necessary and contributed little to the overall risk profile
2. Correct operation of the restart was important to ensuring the consequences did not eventuate. Taking credit for SOPs (standard operating procedures) as LOPA barriers is not accepted by some organisation because of the reliance on a human response. The risk level was 2 orders of magnitude below the risk target and so it was not necessary to include it from a "numbers perspective", however to demonstrate ALARP, it was agreed that the SOP rigour be improved and it becomes visible within a management system. This was done by escalating it to a site critical SOP which incorporated training and assessment to ensure the barrier was credible.

<u>Case Study 2: Spray Dryer</u>

Scenario: To remove the need for external explosion venting on a spray drier, an explosion suppression system was being considered. This system detects rapid increases in pressure within the dryer chamber and injects sodium bicarbonate to suppress the explosion and protect the chamber. Additional controls on the dryer included:

- CO monitoring which detects ppm levels of CO (early onset of the Maillard reaction causing local self-heating and a source of ignition in a system which is always in the flammable range). This activates a process shutdown
- Temperature detection (2oo3) on the exhaust which activated a water deluge.

The process operation within a drier already has the fuel (powder) and the air in perfectly mixed conditions. All that is needed for an explosion, is an ignition source. This can come from either equipment failures or self-heating of the powder.

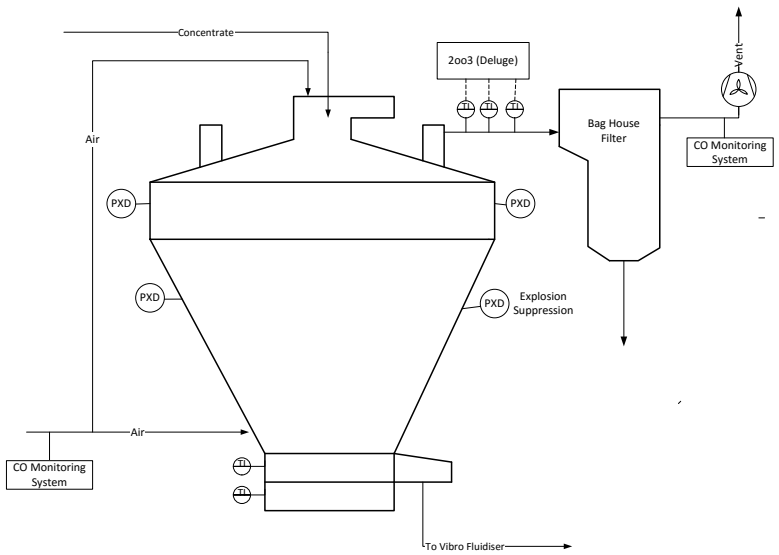


Figure 3: Spray Dryer PFD

The Study: A LOPA study was commissioned to study the overall protection of the dryer and to assess the risk of an explosion within the building. The study deemed that 2 of the existing controls were not as effective as designed. The CO monitoring system was sensitive to air intake disturbances and the 2oo3 temperature safety function on the exhaust did not have a robust and redundant final element (deluge valve). The latter was deemed only suitable to protect against a dryer fire and not an explosion. The explosion suppression system was deemed to be as reliable as vendor stipulated on the proviso that the system would be managed to the requirements listed in IEC61511.

The following simplified bowtie represents the barriers and initiators.

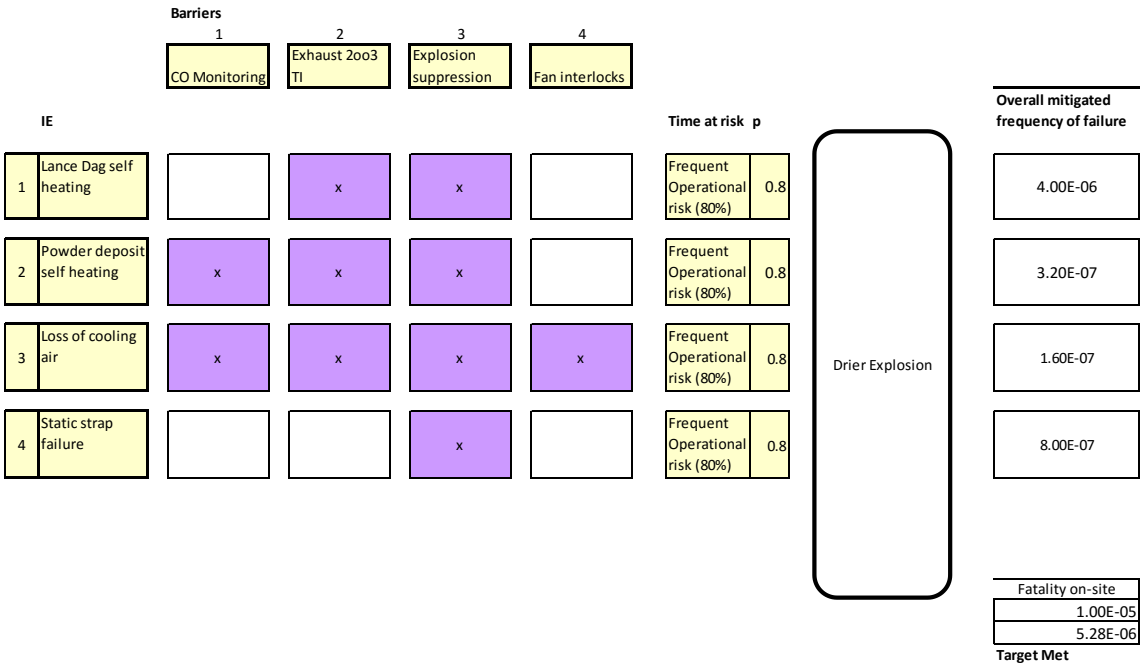


Figure 4: Spray Dryer LOPA Bowtie.

Key outcomes from study:

1. Management systems to ensure the explosion suppression system was installed, tested and maintained to IEC61511 needed to be put in place at the facility. If this could not be implemented, then external venting should be retained.
2. A review of the deluge valve installation was necessary to improve the overall effectiveness of the exhaust temperature detection protection system. The review assumed the 2oo3 function only meet the equivalent reliability requirement of a simple PLC/BPCS loop, whereas the temperature sensors were configured in a 2oo3 arrangement.
3. The effectiveness of the deluge system as a barrier needed to be verified (i.e. response time to explosion).

Case Study 3: 600# piping on inlet to gas plant

Scenario: An oil and gas facility has 2 remote well heads where the piping class reduced from 1500# to 900# to 600# downstream of the chokes. Pig launchers, receivers and various isolations exist along the pipeline and upstream of the tie-in to the gas plant. The 600# pipeline passes within 40m of the manned control room enters the plant and had the potential to rupture, should it be exposed to the shut in pressure of the wells. Each well head had 2 independent means of pressure protection and the pipeline had one.

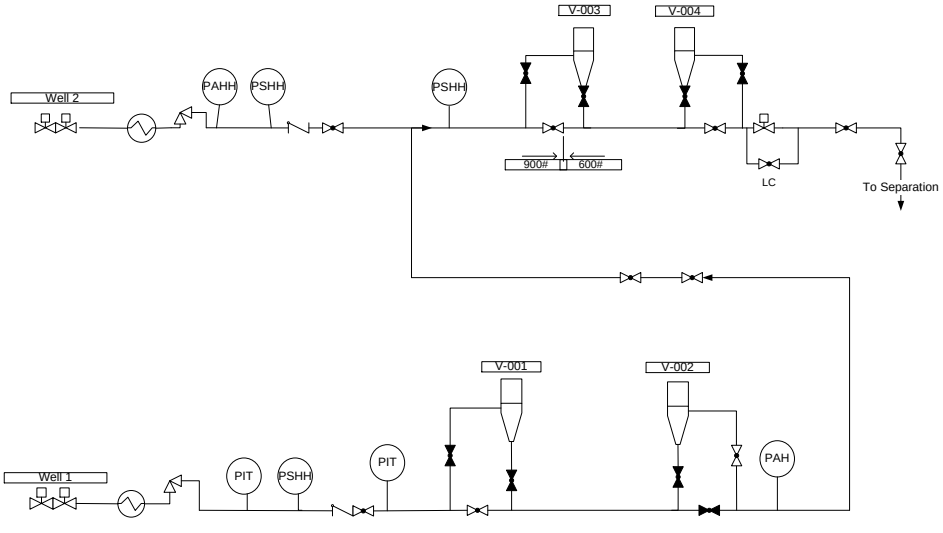


Figure 5: Gas Plant Inlet Pipelines PFD

The Study: As part of a safety case execution, 20 scenarios were assessed for the facility, all of which had the potential to cause single or multiple fatalities. The event of concern was a rupture of the 600# piping, leading to a jet fire and fatality to exposed personnel. Human error (valve movements), pigging operations and equipment failures were the main causes of the event. The risk was almost 2 orders of magnitude outside of the single fatality risk target. The study initially assumed conventional exposure levels based on operator movements around the plant, however radiation modelling of the rupture event showed that that the control room was also in the hazard zone.

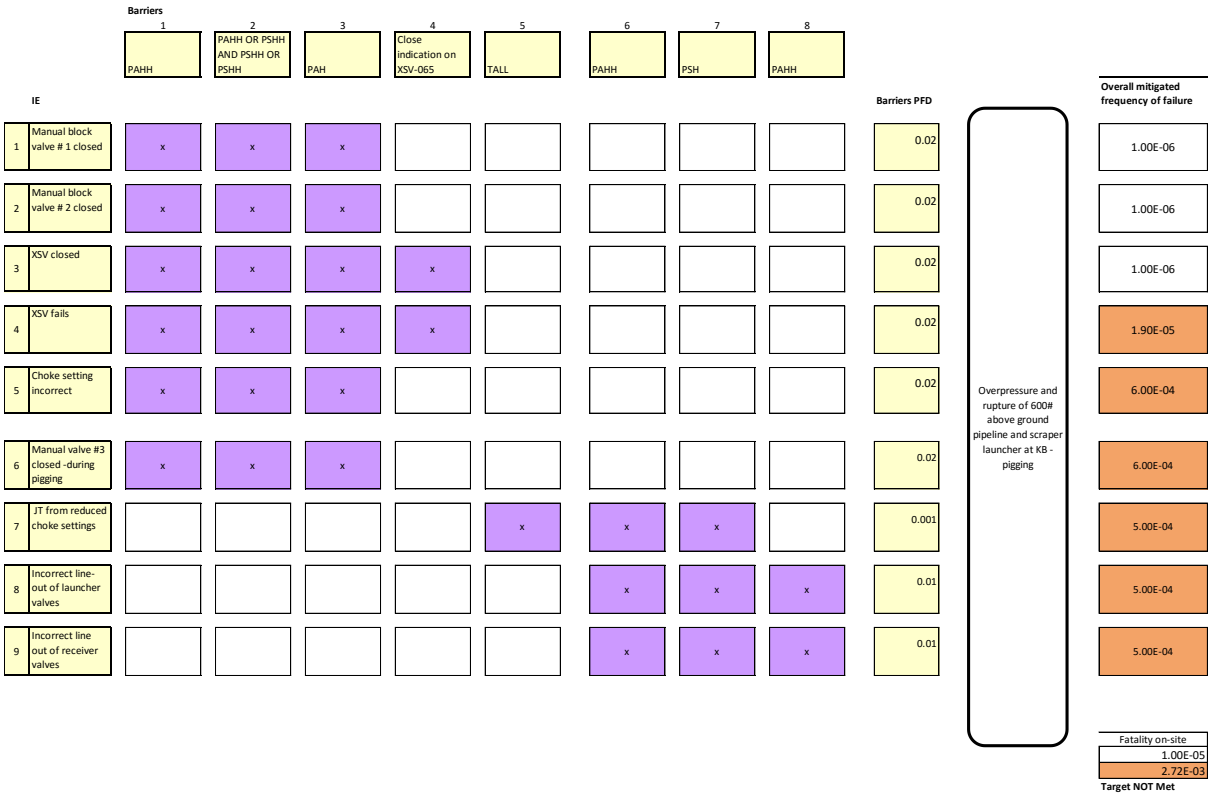


Figure 6: Gas Plant Inlet Pipelines LOPA Bowtie

Key outcomes from study:

1. The LOPA study initially assumed conventional exposure levels based on operator movements around the plant, however radiation modelling off the rupture event showed that that the control room was in the hazard zone, increasing the risk profile.
2. Various options were available to reduce the risk, including adding an SIS, uprating the piping (to 900#), putting mechanical interlocks in, however one stood out once all 20 scenarios were reviewed. This was to move the control room out of the hazard zone. This reduced the exposure levels back to “normal” levels for several scenario’s and with the addition of other controls, the risk level was deemed acceptable. The process used to evaluate the site risk profile is outlined below.

Determining a site action plan to reduce the risk

For Case Study 3, 27 potential actions were mapped against the 20 scenarios (Case Study 3 was #14). This map allowed the operator to determine at a glance which actions were qualitatively more effective (from a numbers perspective) and where they got value for money in managing the risk.

Action		Scenario																			
#	Description	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Upgrade the MCC (pressurisation and gas detection) to remove it as a source of ignition	x	x			x	x				x	x	x	x	x						
2	Relocate Control room to a safe location	x	x	x		x		x					x		x		x	x			x
3	Fully function test barber PSH's to prove trips on XSV's	x	x																		
4	Review and document operating levels of the separator during pigging. Can they be increased for short durations during pigging?			x	x						x			x		x					
5	Automate the level control on the incoming flow to prevent high levels during slugging			x							x								x	x	
...																					
27	Install gas detection around the back up generator		x				x				x		x		x						

Figure 7: Action Plan for Multiple Scenario's

This "map" allowed pre-selection of actions for all 20 scenarios. The actions were reflected in a "post action" LOPA bowtie's to determine their actual impact on risk. An ALARP test was then applied and the cycle repeated if any of the tests failed (reference Figure 8).

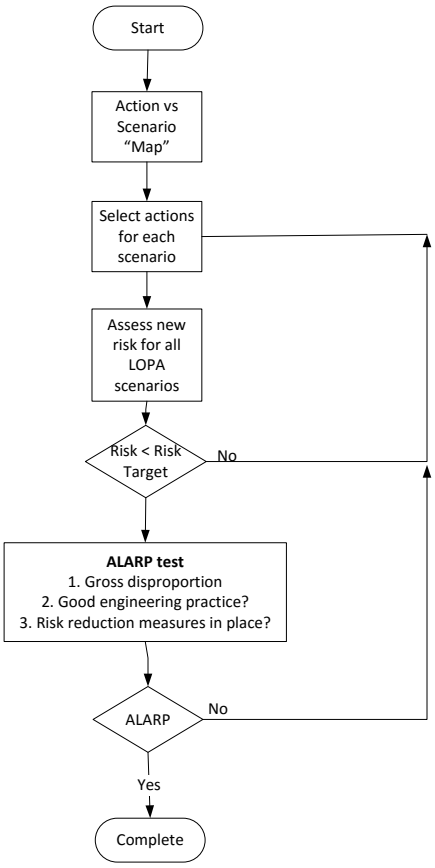


Figure 8: Determining Site Action Plan to Manage Site Risk Profile

This process enabled cost effective solutions to be determined to address the site risk profile rather than treat each scenario in isolation. Assessing scenarios in isolation can potentially lead to solutions to reduce the risk, not being considered as they may initially appear to be cost prohibitive. Actions such as removing personnel from the area by moving a control room can become easier to justify if multiple scenarios are affected by this action.

Communicating LOPA Risk

Communication is of fundamental importance in the management of process safety risk. If the technique used to assess the risk, enables participation, effective decisions about managing these risks can be made. In the author's experience, generation of a "bow-tie" to describe an accident sequence (in a review format) solicits more involvement from operations, maintenance and engineering personnel because they understand how their jobs interact with the causes and barriers that influence the accident pathway. For this reason, the advanced form of LOPA improves communication and understanding of risk if the bow-tie is generated during the review.

Conclusion

The LOPA technique is considered a strong technique in that if applied systematically meets many of the needs of an organisations risk assessment process. If applied, the following 5 learnings from these case studies can improve the decision making process and enhance an organisations response to higher risk designs and operation.

1. LOPA facilitators and plant operators should be aware that SIF assessment and design does not guarantee that the function will remain rated for the lifecycle of the facility. Operation and maintenance are equally important to show the function is meeting its design intent in reducing risk. LOPA facilitators should be aware of a company's ability to manage the lifecycle during the review as other solutions to reducing risk may be more appropriate.
2. Alternate solutions to reducing risk should be part of a review. Do not get "hung up" on looking for instrumented solutions such as SIL rated functions.
3. Consequence modelling may improve the quality of a LOPA review by improving the data used in the review particularly around exposure levels, ignition and explosion likelihoods.
4. The existence of a safety function in a brownfield installation does not mean it is actually needed. An effective risk assessment can help determine if it is required.
5. For large scale LOPA studies, such as those used for safety cases, actions can be mapped against the scenario's to determine those most appropriate to reduce risk across the facility.