Comparison of a single initiating event verses a multiple initiating event approach to Layer of Protection Analysis

Dr Colin Chambers, Health and Safety Executive, Science Division, Harpur Hill, Buxton, SK17 9JN, UK

The Layer Of Protection Analysis (LOPA) technique can be implemented by evaluating a single initiating event associated with a hazardous scenario to determine the risk reduction required to meet the LOPA target frequency. This required risk reduction can then be equated to a Probability of Failure on Demand (PFD), which could be implemented by a Safety Instrumented System (SIS). Where there are multiple initiating events for the same hazardous scenario, LOPA can be applied to each of the initiating events individually, and the LOPA resulting in the most onerous requirement for risk reduction can act as the basis for determining the required SIS PFD. The single initiating event evaluation approach is presented with a suitable LOPA calculation worksheet in the Center for Chemical Process Safety (CCPS) LOPA book, which was first published in 2001(CCPS, 2001).

However, when there are multiple initiating events associated with the same hazardous scenario, this method can result in insufficient risk reduction being determined. This issue has long been understood and an approach that addresses this potential issue is widely used in the process industry. This approach takes the single initiating event evaluation method one step further by evaluating all credible initiating events associated with a hazardous scenario in a single LOPA calculation sheet and aggregates the results to give a total mitigated event frequency. This method accounts for the combined contribution of all credible initiating events to the hazardous scenario.

A LOPA calculation worksheet format that easily and unambiguously facilitates the multiple initiating event approach to LOPA is presented in the British standard BS EN 61511-3:2017, Annex F (BSI, 2017).

This paper presents and evaluates the two LOPA approaches outlined using a typical process industry example scenario and then compares the results and presents conclusions.

Keywords: LOPA, Single initiating event, multiple initiating event, risk assessment, SIS, SIL, TMEL

Introduction and background

The single initiating event versus the multiple initiating event approach to LOPA is not discussed in the author’s previous work (Chambers, 2011); (Chambers, 2009), and is a common issue where examination and discussion would be beneficial to LOPA practitioners in the process industry.

The Layer Of Protection Analysis (LOPA) technique can be implemented by evaluating a single initiating event associated with a hazardous scenario to determine the risk reduction required to meet the LOPA target frequency. This required risk reduction can then be equated to a probability of failure on demand (PFD), which could be implemented by a safety instrumented system (SIS). Where there are multiple initiating events for the same hazardous scenario, LOPA can be applied to each of the initiating events individually, and the LOPA resulting in the most onerous requirement for risk reduction can act as the basis for determining the required SIS PFD. The single initiating event evaluation approach is presented with a suitable LOPA calculation worksheet in the Center for Chemical Process Safety (CCPS) LOPA book (CCPS, 2001).

However, it is the author’s experience that for a given hazardous scenario there is likely to be more than one initiating cause. When there are multiple initiating events associated with the same hazardous scenario, this method can result in insufficient risk reduction being determined. This issue has long been understood and an approach that addresses this potential issue is widely used in the process industry. This approach takes the single initiating event evaluation method one step further by evaluating all credible initiating events associated with a hazardous scenario in a single LOPA calculation sheet and aggregates the results to give a total mitigated event frequency. This method accounts for the combined contribution of all credible initiating events to the hazardous scenario.

How can initiating events be identified?

In the author’s experience, the main reason why some LOPA practitioners evaluate a single initiating event in a LOPA study is based partly on how the initiating event is identified and partly on the original LOPA concept of analysing a single cause consequence pair without necessary consideration of whether multiple causes could lead to the same consequence.

When using Hazard Identification (HAZID) methods like Hazard and Operability study (HAZOP), the HAZOP team will evaluate each line in the HAZOP based on a given deviation and a, possibly incomplete, list of causes. As part of the HAZOP assessment an initial rough screen assessment or engineering judgement can suggest that further risk reduction might be required for that line. The relevant HAZOP lines are passed onward to assessment by other techniques such as LOPA to better determine whether further risk reduction is required. This approach has led to single initiating event LOPA assessments reviewed by the author.

Some LOPA practitioners recognise this and will look at all the LOPA studies associated with a hazardous scenario and base their requirement for further risk reduction on the most onerous of these LOPA studies, i.e. the initiating event requiring the highest risk reduction factor (lowest PFD) to meet the LOPA Target Mitigated Event Likelihood (TMEL). This approach can work, but it is likely to underestimate the required amount of risk reduction.

A better approach is that once all the lines from a HAZOP study relating to a particular process or system hazardous scenario that require further assessment are identified, an additional assessment of the hazardous scenario should be performed to see if any other credible initiating events can be identified. A suitable method called a demand tree is described in the PSLG final report (PSLG, 2009). These initiating events can then be assessed using the multiple initiating event approach to LOPA as described in Appendix 2 of the PSLG report (PSLG, 2009). The interface between HAZID and LOPA can be problematic and would benefit from further consideration, but this is outside the scope of this paper.

This paper evaluates both approaches to LOPA using a typical process industry example and compares the results.

What is LOPA?

LOPA is a method of representing and evaluating the balance between risk and risk reduction for a process or system. Layer of protection analysis is a simplified risk analysis technique that takes as its starting point a single hazardous scenario and evaluates a single outcome of that scenario, i.e. the hazardous scenario being derived from the hazard identification process. The frequency at which the hazardous scenario initiating events are likely to occur, without any risk reduction measures in place, is determined. Then, all the layers of protection and other factors that reduce this frequency are considered and evaluated using "LOPA rules" which implement the relevant clause requirements of BS EN 61511 (BSI, 2017) for each initiating event. The result is a much-reduced frequency of occurrence for the hazardous scenario. At this point the first iteration of the LOPA is complete and a decision is made, " is the Mitigated Event Likelihood (MET) equal to or less frequent than the LOPA Target Mitigated Event Likelihood (TMEL)?". If the response to the question is "yes" no further action is required and the LOPA is documented and kept for future review. If the answer is "no", consideration of further risk reduction is made. For example, by means of an additional layer of protection or by making improvements to an existing layer of protection in terms of their PFD. The LOPA is re-evaluated taking into consideration the proposed amount of further risk reduction. The new mitigated event frequency is compared to the LOPA TMEL, which should now have been met or exceeded. Good LOPA practice is to set a TMEL, sometimes referred to as a LOPA target frequency at a level that is As Low As Reasonably Practicable (ALARP), which is an expectation of UK health and safety law. Figure 2 depicts a LOPA calculation worksheet that facilitates the multiple initiating event approach to LOPA as presented in the standards BS EN 61511-3:2017, Annex F (BSI, 2017).

Where does LOPA come from?

LOPA was developed by the CCPS and several companies including the Dow chemical company in the 1990s. LOPA was used to determine the safety integrity requirements for the Safety Instrumented Function (SIF) to be implemented by a SIS, or interlocks as they were sometimes referred. Some companies developed LOPA as a screening method to reduce the number of hazardous scenarios requiring a full Quantitative Risk Assessment (QRA) (CCPS, 2001). Other companies developed LOPA simply as a means of identifying the amount of residual risk associated with a process. In general, the purpose of a LOPA was to determine whether there are enough layers of protection for a given hazardous scenario (CCPS, 2001). LOPA has proven useful in assessing the impact of existing layers of protection, and of specific initiating events (in the multiple initiating event approach) helping the analysis determine the dominant causes for a given hazardous scenario.

LOPA back ground with regard to Buncefield

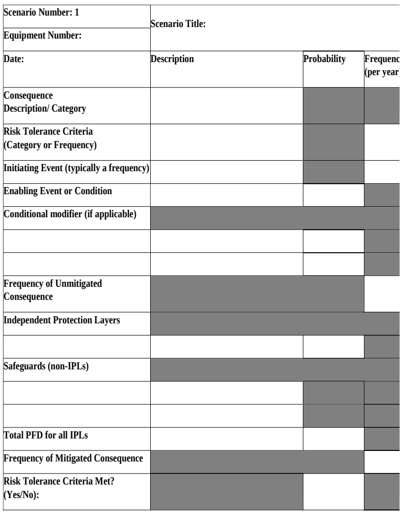
In December 2005 there was an explosion at a UK fuel storage terminal situated at Buncefield. The explosion was the result of gasoline tank overfill resulting in the generation of a significant vapour cloud that subsequently found an ignition source. The result was the biggest recorded explosion since World War 2 and lead to significant destruction at the site and damage to the surrounding buildings. The fire burned for several days and the black plume could be seen from space. The damages and costs were in the tens of millions of pounds (BSTG, 2007); (MIIB, 2007). The Buncefield Standards Task Force (BSTG) cites actions that fuel storage sites must perform to help ensure that this type of incident does not occur again. The first action requires that systematic assessment of safety integrity requirements are carried out at all relevant sites (BSTG, 2007). It was decided that LOPA would be the recommended method that all fuel storage sites could use to determine the SIL requirements for their tank overfill prevention system. The Process Safety Leadership Group (PSLG) comprising technical specialists from industry and the regulator produced guidance on key aspects of process safety associated with fuel storage sites, including guidance on LOPA. The author was a LOPA guidance subcommittee member and was also involved in reviewing the post Buncefield LOPA studies supplied to the regulator from industry (PSLG, 2009).

PSLG LOPA guidance

The PSLG LOPA subcommittee used the CCPS LOPA book (CCPS, 2001), BS EN 61511(BSI, 2017) and relevant industry practice to develop the LOPA guidance. The PSLG LOPA guidance is now widely accepted in the UK fuel storage sector and in the wider process industries. The PSLG guidance describes the multiple initiating event approach to LOPA, hence accounts for all the hazardous scenario initiating events leading to the outcomes from the bulk storage fuel tank overfill scenario and aggregates them in the same LOPA sheet (PSLG, 2009).

Single initiating event approach to LOPA

The Layer Of Protection Analysis (LOPA) technique can be implemented by evaluating a single initiating event associated with a hazardous scenario to determine the risk reduction required to meet the LOPA target frequency. There are two variants of the single initiating event. The first variant accounts for a single initiating event only, and determines the hazardous scenario mitigated event frequency and subsequently the risk reduction requirement for that hazardous scenario outcome. No other initiating events are identified or evaluated. The author has seen many instances of this approach being applied, where the single initiating event considered was taken from a single entry in a HAZOP study, without looking at other instances in the same HAZOP that were associated with the same hazardous scenario and outcome. The second single initiating event method identifies all credible initiating events, evaluates each one individually using a separate LOPA calculation sheet and then uses the LOPA with the most onerous outcome in terms of the required risk reduction. This then acts as the basis for determining the required PFD that the risk reduction measure would need to implement. Both single initiating event variants can result in underestimation of the required amount of risk reduction, as will be demonstrated in this paper. The single initiating event evaluation approach is presented with a suitable LOPA calculation worksheet in the Center for Chemical Process Safety (CCPS) LOPA book (CCPS, 2001).

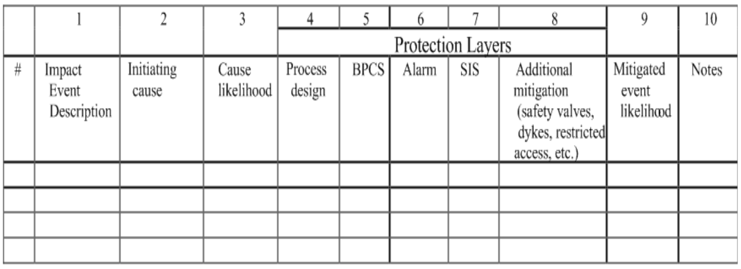


Scenario Number: 1	Scenario Title:		
Equipment Number:			
Date:	Description	Probability	Frequenc (per year
Consequence Description/ Category		▨	▨
Risk Tolerance Criteria (Category or Frequency)		▨	
Initiating Event (typically a frequency)		▨	
Enabling Event or Condition			▨
Conditional modifier (if applicable)	▨	▨	▨
			▨
			▨
Frequency of Unmitigated Consequence	▨	▨	
Independent Protection Layers	▨	▨	▨
			▨
Safeguards (non-IPLs)	▨	▨	▨
		▨	▨
		▨	▨
Total PFD for all IPLs			▨
Frequency of Mitigated Consequence	▨	▨	
Risk Tolerance Criteria Met? (Yes/No):	▨		▨

Figure 1 An example LOPA sheet used for the single initiating event approach to LOPA

Multiple initiating event approach to LOPA

When there are multiple initiating events associated with the same hazardous scenario and outcome, using the single initiating event method can result in insufficient risk reduction being determined. An approach that addresses this potential issue is the multiple initiating event approach, which is outlined here. The multiple initiating event approach takes the single initiating event evaluation method one step further by evaluating all credible initiating events associated with a hazardous scenario and outcome in a single LOPA calculation sheet and aggregates the resultant initiating event mitigated event frequency to give a combined mitigated event frequency. This approach accounts for the combined contribution of all credible initiating events to the hazardous scenario, for the overall scenario. An example will be used in this paper using data based on the author's experience of reviewing many LOPA studies over the last 20 years.



	1	2	3	4	5	6	7	8	9	10
				Protection Layers						
#	Impact Event Description	Initiating cause	Cause likelihood	Process design	BPCS	Alarm	SIS	Additional mitigation (safety valves, dykes, restricted access, etc.)	Mitigated event likelihood	Notes

Figure 2 An example LOPA sheet used for the multiple initiating event approach to LOPA

Fuel storage tank overfill scenario example

For the purposes of this paper a Buncefield type hazardous scenario will be described and used as the basis for the different LOPA approach comparisons.

A fuel storage site can typically import fuel either by ship to shore transfer, pipeline transfer or rail transfer. The fuel is typically exported by the same routes with the addition of road tanker export. This hazardous scenario considers bulk storage of gasoline received by ship to shore transfer. There is a dedicated pipeline for gasoline from the jetty to a group of dedicated bulk storage tanks via a manifold that selects which tank is used for the transfer. The average tank fill operation takes 24 hours to transfer 20 metric tonnes of gasoline from ship to the storage tank. There are approximately 50 tank fill operations per year.

Three site operators may typically be involved in the transfer operation: a jetty operator, a control room operator and a field operator, plus the ship's personnel. The ship personnel will both initiate and terminate the fuel transfer using the ship's pumps after the control room operator communicates that the transfer is complete. The tank fill operating procedure states that prior to the ship berthing, a gasoline tank with enough ullage (free space) is identified and recorded as being the tank to use for the transfer. The tank is lined up, i.e. the relevant valves that need to be opened from the jetty to the tank being used in the transfer are identified. The actual tank inlet valve is not opened until the ship is ready to initiate transfer. A representative of the product owner or from the shipping company may 'dip' the tank before and after the filling operation to verify the amount of gasoline being delivered. These measurements are compared with the tank level gauge to ensure agreement. Once transfer is initiated, and the relevant tank inlet valve is opened, fuel transfer can begin. Once the required quantity has been transferred as pre-determined by the control room operator using the automatic tank gauging system, the tank side valve is closed, and the control room operator communicates with the ship to terminate the transfer. Often, when the required amount of product is close to being transferred the ship will be informed and will slow down the transfer rate.

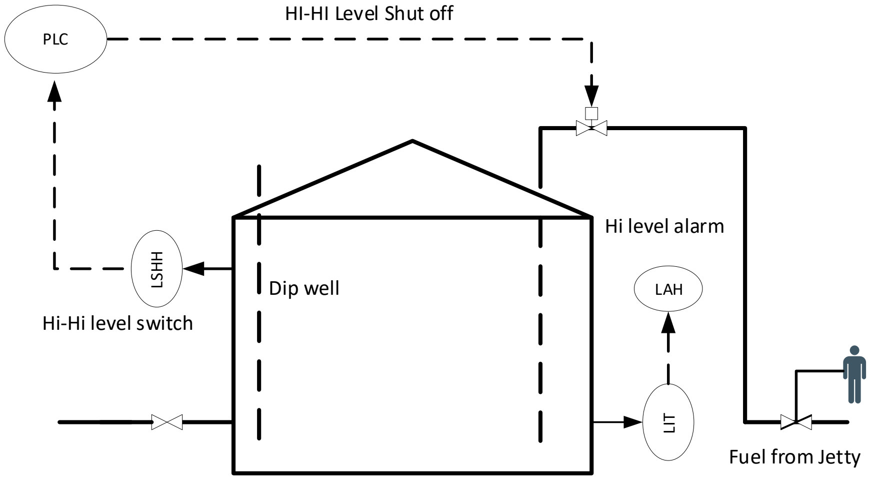


Figure 3 bulk storage tank with overfill protection systems

Hazardous scenario initiating events

Within each LOPA a single hazardous scenario and undesired outcome is considered. There is typically more than one pathway in which the hazardous scenario can be realised. Each pathway is referred to as an initiating event or initiating cause. In this paper we will use the term initiating event. An initiating event is an event that if left unchecked and with no other prevention/mitigation measures in place could result in the hazardous scenario occurring. The initiating events can be determined in several ways such as directly from a HAZOP, or similar, by systematic methods such as a demand tree, (PSLG, 2009), or preferably all the above.

The example LOPA presented in Figure 4 uses the multiple initiating event approach. Using this approach, the contribution of each initiating event can be clearly seen and hence allows evaluation of each initiating event in isolation of the others if required. Using this approach also allows evaluation of key aspects of the single and multiple initiating event approach for comparison purposes in this paper.

A LOPA should only evaluate credible initiating events, i.e. initiating events that impact on the outcome of the LOPA or that relate to key system failures that must be addressed even if they do not represent a dominant risk. In the example LOPA depicted in Figure 4, which is based on a Buncefield type hazardous scenario, initiating events typically found in LOPA studies are used. In the author's experience, there are typically 3 to 5 credible initiating events that are evaluated in a LOPA study. Additionally, the data used in this example are representative of the failure frequencies and probabilities found in LOPA studies reviewed by the author over a period of 20 years, including the Buncefield hazardous scenario LOPA studies reviewed by the author. It should be noted that the author and HSE does not endorse any of the frequencies and probabilities used in this example for use anywhere else. The operator should always determine failure probabilities and failures rates on a case by case basis and justify any assumptions they make.

The tank has an Automatic Tank Gauging system (ATG) installed, which is used to control the level of the tank during the fill operation. The ATG uses a level detection sensor to determine the fuel level in the tank and, therefore, is used to determine when to terminate the fuel transfer.

The initiating events used in this paper are as follows:

- IE1 ATG level reading sticks or reads low
    - If the ATG readout sticks or reads low then there is either no indication or an inaccurate (low) indication of the fuel level in the tank.
- IE2 line up of the wrong tank
    - If the wrong valves were opened between the ship and the tank selected for filling, the actual tank selected could already be full, resulting in potential overfill.
- IE3 incorrect calculation of ullage
    - Ullage is the space left in a tank that can be filled, if this is inadequate for the agreed amount of fuel to be transferred then overfill could occur.
- IE4 overcharge of the tank
    - An error from the ship could result in more fuel than expected being transferred thus resulting in overfill.
- IE5 tank side valve fails to danger

- If the tank inlet valve fails open, then fuel could still be transferred after the tank is full, either by failure to stop the transfer pump or by syphonic action, resulting in a tank overfill

Initiating events are expressed as an annual frequency of dangerous failure. The equipment initiating event frequencies are determined by their estimated dangerous failure rate. The Basic Process Control System (BPCS) maximum claim is a dangerous failure rate limited to <10^{-5} dangerous failures per hour, see BS EN 61511-1 clause 8.2.2. (BSI, 2017).

Human error initiating events are estimated by determining the per opportunity error probability and multiplying this by an annual demand rate, in this case equal to the number of operations per year, to determine the annual human error rate, thus ensuring correct dimensions. For example, it is estimated that the “IE2 line up the wrong tank”, error occurs 1 in 200 opportunities, therefore the per opportunity error probability is 0.005. This per opportunity error probability is multiplied by the number of times this task is expected to be performed in a year, in this case 50. Hence, for IE2 the annual human error rate is 0.005 × 50 = 0.25 per year. This means that based on IE2 only, the tank could potentially overfill once in every four years assuming no risk reduction measures were present. Human error probabilities for a given task can be estimated using analysis techniques such as Human Error Assessment and Reduction Technique (HEART) (Williams, 1990) and Technique for Human Error Rate Prediction (THERP) (Swain, 1964).

Protection layers

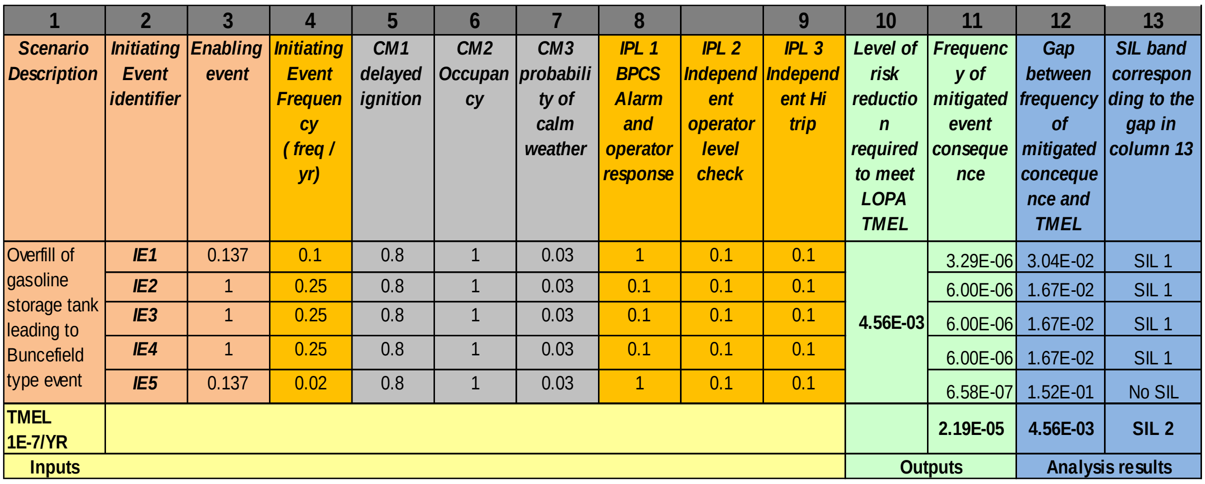
In a LOPA, a layer of protection acts to reduce the frequency of the undesired hazardous scenario from occurring. A protection layer differs from a mitigation layer, the latter acts to reduce the consequence severity of the undesired hazardous scenario, although numerically they indistinguishable in a LOPA.

What are the protection layers for this gasoline storage tank hazardous overfill scenario as described above? To determine the existing protection layers we will look at Figure 3, which depicts a typical tank used for bulk storage of gasoline. In this case it is an above ground vertical atmospheric storage tank. The ATG has a high-level alarm using the ATG level detection capability. The credit that can be claimed for the high-level alarm as a protection layer is limited to a PFD of 0.1 because the ATG does not conform to BS EN 61511 (BSI, 2017). If the ATG system fails to danger, then any associated high-level alarms will also fail. To counter this a “high high” level automatic trip system that is independent from the ATG is used, but in this case, it does not conform with BS EN 61511 and subsequently the credit that can be claimed is limited to a PFD of 0.1. An additional layer of protection employed in this case is an operator “cross check”. The requirements for an operator cross check are described in Appendix 2 Annex 6 of the PSLG final report (PSLG, 2009). The operator performing this task is independent of the control room operator and has access to a means of verifying the tank level that is independent from that used by the control room operator. The cross check is performed at predetermined intervals to both check the actual tank level and to determine if the tank level exceeds the normal maximum fill level. The field operator must be able terminate the fill operation upon detection of a high level, in this case by initiating the “high high” level trip in a timely manner that is sufficient to prevent the overfill, otherwise no credit can be claimed for this protection layer (PSLG, 2009).

The protection layers used in this example LOPA are:

- IPL1 BPCS high level alarm with control room operator response
- IPL2 Field operator level cross check
- IPL3 Independent automated high high level trip

The protection layers PFD is stated in the relevant LOPA cell in Figure 4.



1	2	3	4	5	6	7	8		9	10	11	12	13
Scenario Description	***Initiating Event identifier***	***Enabling event***	***Initiating Event Frequency (freq / yr)***	***CM1 delayed ignition***	***CM2 Occupancy***	***CM3 probability of calm weather***	***IPL 1 BPCS Alarm and operator response***	***IPL 2 Independent operator level check***	***IPL 3 Independent Hi trip***	***Level of risk reduction required to meet LOPA TMEL***	***Frequency of mitigated event consequence***	***Gap between frequency of mitigated conceqeunce and TMEL***	***SIL band corresponding to the gap in column 13***
Overfill of gasoline storage tank leading to Buncefield type event	***IE1***	0.137	0.1	0.8	1	0.03	1	0.1	0.1	**4.56E-03**	3.29E-06	3.04E-02	SIL 1
	IE2	1	0.25	0.8	1	0.03	0.1	0.1	0.1		6.00E-06	1.67E-02	SIL 1
	IE3	1	0.25	0.8	1	0.03	0.1	0.1	0.1		6.00E-06	1.67E-02	SIL 1
	IE4	1	0.25	0.8	1	0.03	0.1	0.1	0.1		6.00E-06	1.67E-02	SIL 1
	IE5	0.137	0.02	0.8	1	0.03	1	0.1	0.1		6.58E-07	1.52E-01	No SIL
TMEL 1E-7/YR											**2.19E-05**	**4.56E-03**	**SIL 2**
Inputs										**Outputs**		**Analysis results**	

Figure 4 Example LOPA for a fuel storage tank overfill scenario

Risk tolerability criterion

In this case, because the Buncefield type event has the potential to impact members of the public offsite therefore, a TMEL of 1×10^{-7}/year was chosen.

Enabling events

An enabling event is an event that needs to occur for the relevant initiating event to occur. Typically, a hazard may only be present when a process or task is performed. This is usually referred to as a "time at risk" enabling event, which based on the authors experience, is the most common enabling event used in LOPA studies. For the hazardous scenario considered in this work, a tank could only overfill at the time of being filled, assuming later tank overfill due to syphonic action or misalignment of valves could be ruled out (PSLG, 2009). Time at risk as an enabling event is only applicable to electrical or mechanical system initiating events, such as valve failure or ATG failure and is not applicable to human error based initiating events such as wrong tank line up or tank ullage calculation. This is because electrical and mechanical system failure initiating events are recorded as an annual dangerous failure rate. If the hazard is only present for part of the year then the risk can be said to be present for that part of the year only. Therefore, use of the time at risk enabling event takes this into account. However, to claimed time at risk as an enabling event, it must be shown that the equipment/system, whose failure is associated with the initiating event, does not contain a latent dangerous failure at the beginning of the time at risk period. The time at risk enabling event is expressed as a percentage of the year when the hazard is present. In this case if, it takes an average of 24 hours to fill a tank and there are 50 tank fill operations per year then this would be calculated as in Equation 1.

$$\frac{\mathbf{24\times50}}{\mathbf{8760}} = \mathbf{0.137} \qquad \textbf{Equation (1)}$$

Human error based initiating events are recorded as a per opportunity error probability, which is then multiplied by an annual demand rate to get an annual human error rate. Therefore, the time at risk enabling event is not a valid concept for human error based initiating events. Appendix 2 Annex 4 of the PSLG report contains a more detailed discussion of time at risk, (PSLG, 2009).

Conditional modifiers

Conditional modifiers are risk reduction factors that are either external to the operation of the facility or are part of the general design of the facility without being specific to the hazard scenario being considered (PSLG, 2009).

It should be noted that conditional modifiers are represented by a probability of occurrence and not as a probability of failure, which is used to represent a protection or mitigation layer.

For Buncefield type events, the main conditional modifiers represent: calm weather; ignition and explosion of a large flammable cloud; persons in the hazardous area and finally, the probability of environmental consequence, although it is recommended that environmental consequences are considered separately from safety consequences.

The probability of ignition tends towards 1 if the flammable cloud extends offsite and into an area where ignition sources are uncontrolled. Again, because of the cited offsite risk and the persons located on site, the probability of someone being in the hazardous area will be 1. The probability of calm weather is 0.03 based on Met Office data for this fictitious site.

Conditional modifiers are multiplied by the initiating event frequencies and the protection layer probabilities, so the analysis is likely to be sensitive to the values used. Therefore, care should be taken not to be overly conservative or overly optimistic (ILGB, 2002).

Comparison and analysis of single verses multiple initiating events

The LOPA calculation sheet depicted in Figure 4 has been used to document the Buncefield type example scenario described in this paper and depicted in Figure 3. The initiating event includes both equipment-based failures and operator-based failures. The values used in the LOPA are representative of LOPA studies submitted by companies in the process industries to the Health and Safety Executive (HSE) for review.

For the purposes of analysis, columns 13 and 14 in Figure 4 are of most interest. Column 13 presents the gap between the frequency of mitigated consequence from column 12 and the LOPA TMEL stated at the bottom of column 1, for each initiating event. This equates to the PFD the required risk reduction measure that would have to be implemented for the LOPA TMEL to be met. Column 14 presents the relevant SIL associated with each value from column 13.

Based on the previous description of the single initiating event approach to LOPA, the Buncefield type hazardous scenario example would have been evaluated using 5 separate LOPA sheets of the type depicted in Figure 1. Each of those 5 LOPA calculation sheets would be based on 1 of the initiating events numbered IE1 to IE5 in Figure 4.

Each of the LOPA sheets for IE1 to IE4 would require a SIL 1 SIS to meet the LOPA TMEL. IE5 would not require a SIL rated SIS to meeting the LOPA TMEL. If you take the most onerous outcome of the 5 initiating events, in this case it is IE2, IE3 and IE4 equally, all 3 require a SIL 1 SIS but with a slightly higher risk reduction factor (lower PFD) than IE1.

Taking the multiple initiating approach to LOPA and combining the frequencies of mitigated consequence, it can be seen that a SIL 2 SIS with a PFD of 4.56×10^{-3} will be required to meet the LOPA TMEL for the Buncefield type hazardous scenario presented in this paper.

This is not always the case, sometimes the worst-case single initiating event LOPA approach will determine that the required risk reduction would be close enough to that determined using the multiple initiating event approach. However, both would have to be determined to make that judgement. Even if the SIF SIL were the same using either the single initiating event approach of the multiple initiating event approach it is likely that the PFD requirement would be more onerous using the multiple initiating event approach and this could result in potential SIS architecture differences, e.g. the potential requirement for redundant architecture in the SIS.

Conclusions

Both the example LOPA for a bulk fuel storage tank overfill scenario and the author's experience in reviewing many LOPA studies for HSE indicate that both the single initiating event approaches to LOPA described in this paper have the potential to underestimate the risk gap and hence the amount of risk reduction required to meet the LOPA TMEL. The single initiating event worst case approach to LOPA is likely to underestimate the required amount of risk reduction in most, but not necessarily all, cases. The multiple initiating event approach resulted in a requirement for a higher level of risk reduction than either of the single initiating event approaches. This higher level of risk reduction is considered appropriate based on the information presented and data supplied.

Including all the relevant credible initiating events, by adding their outputs together, is analogous to including all the initiating events outcomes as inputs to an "OR" gate in a fault tree. It is concluded that all credible initiating events should be evaluated, and the risk reduction requirements associated with all the initiating events should be aggregated to account for their combined impact on the risk reduction required to meet the LOPA TMEL.

This publication and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

References

BSI, 2017, BS EN 61511-1,2,3:2017 Functional safety. Safety instrumented systems for the process industry sector. Framework, definitions, system, hardware and software requirements, British Standards Institution,

BSTG, 2007, Buncefield standards task group (BSTG), Final report, Safety and environmental standards for Fuel Storage sites, 2007

CCPS, 2001, Layer of protection analysis: simplified process risk assessment, CCPS concept book, AIChE, 2001

Chambers C. and Pearson J. A, 2011, Discussion of some common pitfalls in the application of Layer of Protection Analysis (LOPA) to the overfill of fuel storage tanks at Buncefield type sites, Hazards XXII,

Chambers, C. Wilday, J. Turner, S. 2009, A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks, HSE research reports, RR716

MIIB, 2007, Recommendations on the design and operation of fuel storage sites Buncefield, Major Incident Investigation Board 2007, www.buncefieldinvestigation.gov.uk/reports/index.htm

PSLG, 2009, Process safety leadership group, Final report, Safety and environmental standards for Fuel Storage sites, HSE books

Swain, A.D, 1964, Technique for Human Error Rate Prediction (THERP)., SC-R-64-1338, Sandia National Laboratories, Albuquerque, NM, August 1964.

Williams, J.C., 1990 Human Error Assessment and Reduction Technique (HEART)