Application of Layer of Protection Analysis (LOPA) in Verification of Safety Integrity Level of Instrumented System

by

Mustafa Kamal Helmi Bin Mahamad Anuar

Dissertation submitted in partial fulfilment of
the requirements for the
Bachelor of Engineering (Hons)
(Chemical Engineering)

SEPTEMBER 2012

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

Application of Layer of Protection Analysis (LOPA) in Verification of Safety Integrity Level of Instrumented System

by

Mustafa Kamal Helmi bin Mahamad Anuar

A project dissertation submitted to the
Chemical Engineering Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
BACHELOR OF ENGINEERING (Hons)
(CHEMICAL ENGINEERING)

Approved by,

_____

(Azizul bin Buang)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK

September 2012

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

_____

MUSTAFA KAMAL HELMI BIN MAHAMAD ANUAR

ABSTRACT

Incomplete process hazard analysis (PHA) and poor knowledge management have been two major reasons that have caused numerous lamentable disasters in the chemical process industry. To improve the safety integrity of a process system, all risk should be reduced to a tolerable limit. One way of doing it is by adding layers of protection which include inherent safer design, basic process control system (BPCS), alarms, SIS, physical protection, and emergency response procedure. These layers however, are cost to the process industry in term of implementing it as well as maintaining the quality of the layers. Therefore, understanding the required safety integrity level (SIL) of a process is essential in order to meet the tolerable risk target as well as to optimise the cost of a safety system. Meanwhile, layer of protection analysis (LOPA) is a simplified approach to verify SIL of a process system. Nevertheless, the method is relatively new and various modifications have take place by different entities. Therefore, there is a need to maintain the consistency of the LOPA result by adhering to a standard procedure and practise as well as clear direction provided by Centre of Chemical Process Safety (CCPS). This can be done easier by developing a framework for LOPA analyst to follows as well as tailored to the company background and history.

ACKNOWLEDGEMENT

I would like to gratefully acknowledge the assistance and enthusiastic supervision by my Mr. Azizul bin Buang for this work. I thank Dr. Mohanad M.A.A El-Harbawi for his permission to continue with the work from one of his previous student. I am thankful to all my friends from Universiti Teknologi PETRONAS for their strong encouragement, support as well as feedbacks during the progress of this work. For guidelines and tips, I thank chemical engineering department specifically Dr. Nurhayati Mellon as the co-ordinator for CBB 4624 (Final Year Project II) as for her scheduled thesis writing classes and advice. I also thank all the speakers involve during this course period for their insight in accomplishing my research objective. Last but not least, I thank my family members and my roommate for their continuous encouragement in ensuring my progress throughout the research.

CONTENTS

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

1.1. Background of Study

Safety analysis is very important in industry especially in process industry. Safety analysis is basically a process where the source of risk that may cause harm to human, damage of property and degradation of environment are analysed, managed and sufficiently reduced by focusing on all the related safety lifecycle stages including the design, implementation, operation, and maintenance through to decommissioning. The minimisation of the risk to a tolerable limit is usually achieved by combination of safety protective systems including basic control process system, safety instrumented system (SIS), safety technology and external risk reduction facilities.

Among these safety protective layers, SIS manages to draw a lot of people interest for the implementation of safety analysis. SIS represents an integral part of a safety management system in order to reduce the risk of major accident hazards. In the 1990s the standards IEC 61508 and IEC 61511 emerged to provide the required action to be achieved by SIS and the required probability of failure on demand (PFD). Following the standard, layer of protection analysis (LOPA) was developed to provide guideline for companies to comply with a consistence manner. As a result, the first guideline book for LOPA was published in 2001. By 2009, it is likely more than 1 million LOPA have been performed. During the same period, many abuses of LOPA have been noted and several innovations have occurred (Bridges, 2009). Due

to this finding, many research have been conduct to develop the best method in implementing LOPA (Lassen, 2008).

1.2. Problem Statement

A few recent studies has been made to verify safety integrity level (SIL) of safety instrumented system (SIS) using layer of protection analysis (LOPA) (Lassen 2008, Zatil 2009, Fakhirin 2010, Cui et. Al 2012). However, besides LOPA other methods in determining SIL are available in industry. The methods include quantitative and qualitative analysis to verify SIL of SIS. While quantitative analysis easily gives numerical value to SIL, qualitative method will not do the same and require expert judgement to participate in resulting analysis. Meanwhile, LOPA is a semi-quantitative method using numerical categories to estimate the parameters needed to calculate the necessary risk reduction which corresponds to the acceptance criteria (CCPS, 2001). These categories are evaluated differently by different entity due different in geological and social acceptance. In brief, LOPA has been widely used but the implementation differs from one plant to another. As a result, the implementation seems to be difficult and the data obtained is inconsistent. A clear example of this inconsistency can be seen in a review of LOPA analyses of overfill of fuel storage tanks, "Buncefield incident" where seven consultants are required to produce LOPA report and difference between results are analysed (Health and Safety Executive, 2009). Thus, a simulation of LOPA analysis must be developed to give an overview on the whole analysis for a better understanding of LOPA for safety personal.

1.3. Objective

The objectives of this study are listed as follows:

- To develop a tool for conduct of LOPA to verify SIL of SIS
- To implement LOPA and SIL procedures in a practical case study.

1.4. Scope of Study

This paper will analyse the application of LOPA in determining SIL of instrumented system. The project will start by defining a few key terms which is Safety Integrity Level, Safety Instrumented System, and Layer of Protection Analysis. Development of framework or procedure of implementing LOPA will not be covered in this project, instead review on available procedures in industry will be made and simple implementation procedure will be extract. The project will emphasize more on case study already evaluated in industry using the tool developed and compare the resulting recommendation with current evaluation as well as some comparison with the method used in the current evaluation.

1.5. The Relevancy of the Project

The purpose is this project is to demonstrate method of analysing the Safety Integrity Level (SIL) of a system using Layer of Protection Analysis (LOPA) by a worksheet. Although LOPA is widely known to be able to evaluate safety integrity level, application in Malaysia is limited and the knowledge in implementing the LOPA procedures varies. Hence the procedures would be demonstrated in a simple way to be easily understood.

1.6. Feasibility of the Project within the Scope and Time frame

This project will start by collecting the reading material such as the books, journals, related website, thorough discussion with supervisor and collaboration from industrial practitioners. At the end of Final Year Project (FYP) 1, it is expected that the literature survey on LOPA have been carried out and understood. Meanwhile, for Final Year Project (FYP) 2, the study will focus on implementing the approach by collecting the information and case study from industry.

CHAPTER 2

LITERATURE REVIEW

2.1. Important Definitions

2.1.1. Safety Integrity Level (SIL)

Safety Integrity Level (SIL) is a concept introduced during the development of BS EN 61508 (BSI 2002) as a measure of the quality or dependability of a system which has a safety function (Gulland, 2004). The concept is to measure the confidence level of which the system is expected to perform its function successfully. Following its definition, the concept is the being used in BS IEC 61511 (BSI 2003) which is the process sector specific application of BS EN 61508. The standard recognises that safety function can be categorised into low demand rate safety function and high demand rate safety function. Table 2.1 shows the PFD ranges and associated risk reduction factor (RRF) ranges that correspond to each SIL.

Table 2.1: PFD ranges and associated risk reduction factor (RRF) ranges that correspond to each SIL (CCPS, 2001)

SIL	PFD Range	RRF Range
4	10^{-4} - 10^{-5}	10,000 – 100,000
3	10^{-3} - 10^{-4}	1,000 – 10, 000
2	10^{-2} - 10^{-3}	100 – 1,000
1	10^{-1} - 10^{-2}	10 - 100

As observed from the relationship between safety integrity level, probability of failure on demand and risk reduction factor in Table 2.1, higher level of SIL indicate that low accepTable failure rate and high amount of risk reduction factor.

2.1.2. Safety Instrumented System (SIS)

SIS is made up of one or more safety instrumented functions (SIF) to sense abnormal situations and automatically return the process to a safe state. This is usually achieved by performing partial or complete shutdown of the process, to prevent a hazardous event or to mitigate its consequences. If the initial risk of a process is high, the availability and integrity requirements for SIF's must be high. Requirements for SIF's are addressed in IEC 61511 and IEC 61508 which are widely accepted as the basis for specification, design, and operation of SIS's. Each SIF is specified in terms of the action to be achieved and the required safety integrity level (SIL) for the SIF.

2.1.3. Layer of Protection Analysis (LOPA)

LOPA is an engineering tool used to ensure that process risk is successfully mitigated to an accepTable level (Center for Chemical Process Safety, 2001). LOPA is basically a systematic methodology developed to allow fast, cost effective means of analysis to identify the independent protective layers (IPLs) that reduce the frequency and consequence of specific hazardous incidents. LOPA provides specific criteria and restrictions for the evaluation of IPLs, eliminating the subjectivity of qualitative methods at substantially less cost than fully quantitative techniques. LOPA can be used at any point in the lifecycle of a project or process, but it is most cost effective when implemented during front-end loading when process flow diagrams are complete and the P&IDs are under development. For existing processes, LOPA should be used during or after the HAZOP review or revalidation. LOPA is typically applied after qualitative hazards analysis has been completed, which provides the LOPA team with a listing of hazard scenarios with associated consequence description and potential safeguards for consideration. A LOPA program is most successful when a procedure is developed that sets the criteria for when LOPA is used and who is qualified to use it. A well-written procedure will also incorporate criteria for evaluation of initiating cause frequency and IPL probability to fail on demand (PFD). The development of these criteria takes time, but this cost is rapidly offset by the increased speed at which LOPA can be implemented on specific projects.

2.2. Assigning Safety Integrity Level

LOPA is not the only method in determining safety integrity level for instrumented system. Various other methods, both quantitatively and qualitatively are available in industry. In qualitative methods expert judgement is always required and the resulting end result is highly subjective. Meanwhile, quantitative methods provide numerical result and more consistent target for analysis. The methods that will be applied are different depending on the policy of the company or organisation on whether the necessary risk reduction is needed to be specified in a numerical manner or qualitative manner. Often, big scale process plant requires the assigning of the safety integrity level to be made quantitatively in order to identify basis of decision in later stage of selecting appropriate protective layers. Among the methods available include quantitative method in IEC 61511, the risk matrix, the safety layer matrix, the OLF 070 guideline, the risk graph and the calibrated risk graph.

2.3. LOPA Procedures

Over the wide time range of LOPA application, many approaches and methodologies have been presented. Dowell (1998), Summers (2003) and Ellis and Wharton (2006) have presented flowchart while IEC 61511 use a worksheet as the basis. On the hand, CCPS (2001) provide a step by step procedures which detailed explanation presented by chapters in the book. Some companies established their own procedures such as BP (2006) and Aker E&T (Nordhagen, 2007).

The essential steps that seem common are (Lassen, 2008):

- Documentation of the hazard analysis
- Development of scenario or impact event
- Identification of initiating causes
- Determination of the protection layers including the IPLs
- Quantification (cause frequency / likelihood and PFD)
- Target risk evaluation / SIL determination

From various procedures analysed, Lassen provide a preferred method which combine essential elements in LOPA procedure.

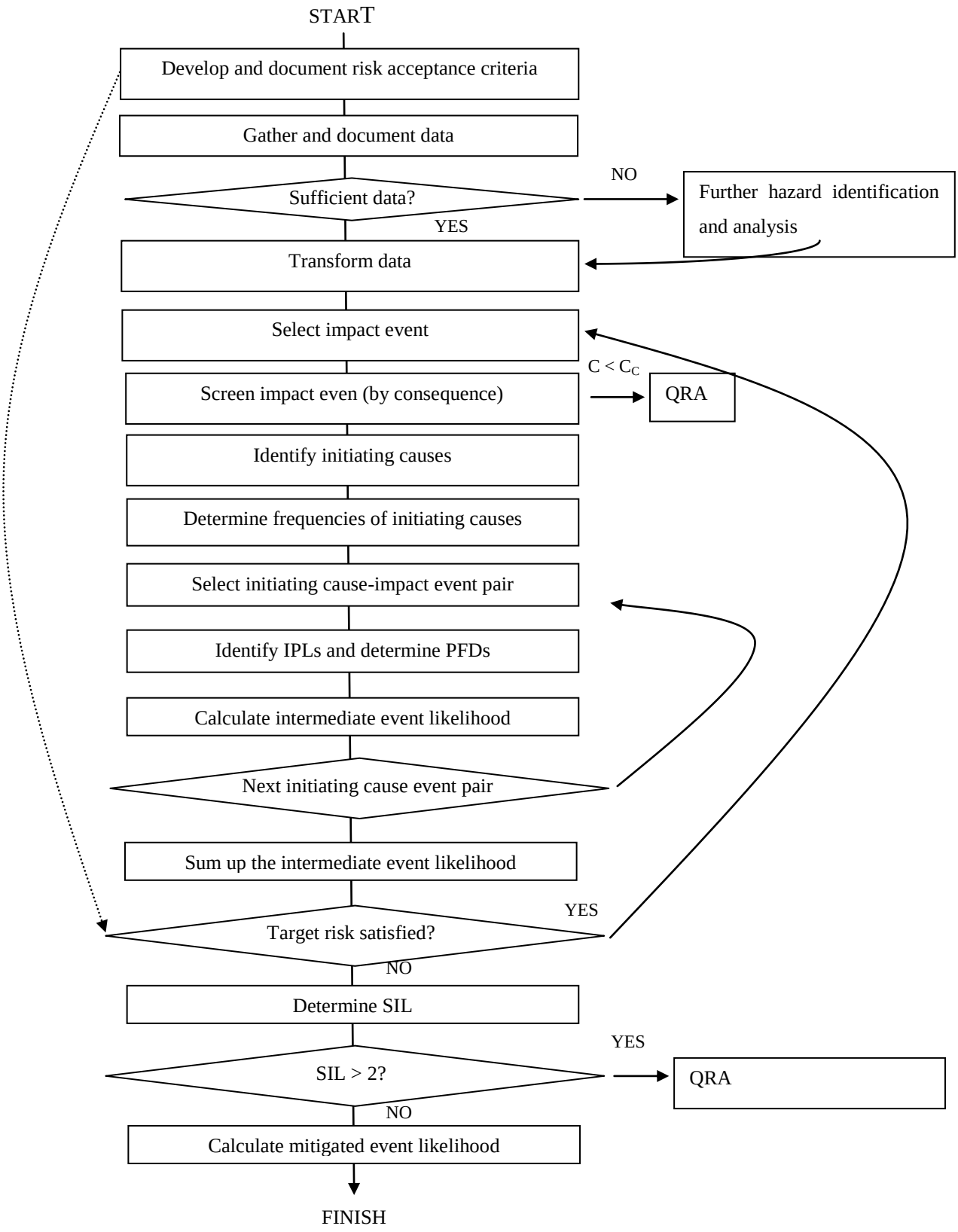


Figure 2.1: Preferred approach (Lassen, 2008)

CHAPTER 3

METHODOLOGY

This project is mainly to develop an application that would utilise layer of protection analysis (LOPA) method to verify the safety integrity level of instrumented system. The development of this application has been done using the Microsoft Excel 2007.

3.1. Selected Procedure in Implementing LOPA

As mentioned earlier in section 1.4, the project will not cover the whole procedure in implementing LOPA for the development of this tool. Instead, the core concept to run LOPA will be extracted from established procedures as describe in section 2.3. From all the procedures or approaches available, common steps and its quantitative method as suggested by Lassen is summarise as follow:

- Identify a hazardous event and assess its severity
- Identify initiating event and assess its frequency
- Identify the applicable independent protection layers and evaluate its effectiveness
- Calculate the expected frequency for the hazardous event
- Determine the need for additional layers of protection and the required SIL if SIS is recommended

3.1.1. Identify a hazardous event and assess its severity

The first mehod in applying LOPA is to identify the hazardous event under investigation and categorise the severity. From this identification, a numerical value must be able to be assigned (based on its severity) as the input for the tool and will be the basic principle for the calculation procedure later on. Often, this value will vary but not far from the established threshold frequency numbers for consequence category published by Centre for Chemical Process Safety Guideline as in Table 3.1.

Table 3.1: Threshold frequency number for each consequence category (CCPS, 2001)

Consequence severity	Max. accepTable frequency	Threshold Frequency Index, F_t
Category 5 – Catastrophic	1/10000	3
Category 4 – Major	1/1000	4
Category 3 – Critical	1/100	5
Category 2 – Minor	1/10	6
Category 1 – Negligible	1	7

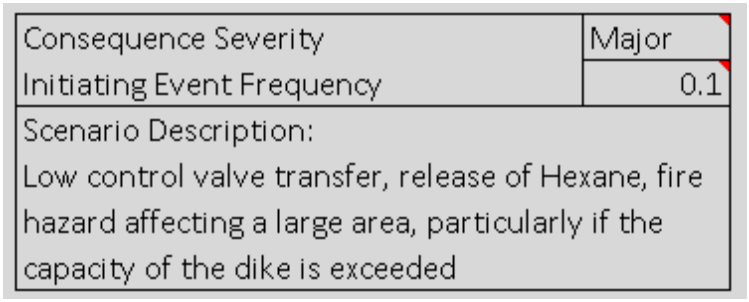


Figure 3.1: Scenario and severity input

Figure 3.1 represent the extracted information from the proposed tool where "Consequence Severity" is the input parameter required to proceed with LOPA.

3.1.2. Identify Initiating event and access its frequency

The second input data will be the the frequency of the intiating event that leads to the occurrance of the hazardous event. Often this value is obtained from the HAZOP study. Reference from literature also will be a good source of valid range of initiating event frequency. Method in determining the numerical value for the initiating event is out of scope for this project. Thus the tool will simply ask user to key in the initiating event frequency regardless how the user obtain the value. Nevertheless, in a full integrated tool development, this value is expected to be obtained from wide database and company history or record.

After the frequency of the initiating event is inserted. The proposed tool is expected to transform the data into index value which is the relative order of range of frequency in simplify form. Table 3.2 below is an example of relative relationship between initiating event frequency and frequency index.

Table 3.2: Proposed relationship of initiating event frequency and initiating index frequency

Range of IE frequency ($year^{-1}$)	Initiating Frequency Index (F_i)
0.1 – 0.01	6
0.01 – 0.001	5
0.001 – 0.0001	4
0.0001 – 0.00001	3
0.00001 – 0.000001	2

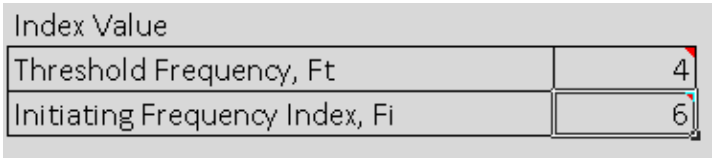


Figure 3.2: Initiating index value (automatically transformed by the proposed tool)

Figure 3.2 demonstrate the index value for both “Consequence Severity” and “Initiating Event Frequency”. Please note the value “4” is obtained from “Major” in Table 3.1 and value of “6” for F_i is obtained from Table 3.2

3.1.3. Identify the applicable independent protection layers and evaluate their effectiveness

After the severity of consequence and the frequency of the initiating event are specified, the tool must be able to evaluate the performance of the current protection provided by the independent protective layers. The purpose of this step is to identify the actual frequency of the hazardous event considering the protection by the existing safety layers. The tool is expected to transform the proabability of failure on demand (PFD) into probability of failure on demand index (S_{pfd}) as published in CCPS as in Table 3.3.

Table 3.3: Probability of Failure on demand indexes (CCPS, 2001)

Probability of failure on demand index (S_{pfd})	Probability range	Expected failure based on 1000 demand
0	1	> 10000
1	1 to 10-1	100 to 1000
2	10-1 to 10-2	10 to 100
3	10-2 to 10-3	1 to 10
4	10-3 to 10-4	0.1 to 1
5	10-4 to 10-5	0.01 to 0.1

This index value is easier to be manage and can be used in the next step in determining the reduced frequency.

3.1.3. Calculate the expected frequency for the hazardous event

Campa and Cruz-Gomez (2009) proposed that the frequency of hazardous event must take into account the number of existing protection layers. This protective layers would reduce the initiating index frequency by considering the effectiveness of all the existing protection layers. This true frequency or Reduced Frequency (F_r) is therefore summarised as follows:

$F_r = F_i - ES$ ----------Equation 1

Where:

F_r = Frequency reduction

F_i = Initiating index frequency

ES = Effectiveness of protection

3.1.5. Determine the need for additional layers of protection and the required SIL if SIS is recommended.

With the reduced frequency (F_r) obtained, the tool will make a comparison with the threshold frequency (F_t) of the selected scenario. If the the reduced frequency is lower than treshold frequency ($F_r < F_t$), no additional protection layers are required. However, if the value is higher than threshold frequency, next step will follows.

3.1.6. Determination of required SIL

Finally, the determination of the required safety integiry level (SIL) is carried out by the quantification of the S_{add} value, which is calculated as the difference between reduced frequency and threshold frequency. Relation to SIL required is suggested by CCPS as follows:

Table 3.4: Determination of required SIL from S_{add} number (CCPS, 2001)

S_{add}	Required SIL	PFD Range
4	3	$10^{-3} – 10^{-4}$
3	2	$10^{-2} – 10^{-3}$
2	1	$10^{-1} – 10^{-2}$

3.1.6.1 Comment and suggestion (qualitative judgement)

This tool also expected to provide early suggestion to the user regarding the SIL of the SIS. A qualitative suggestion that can be deduced from the value available is suggested by Campa and Cruz-Gomez (2009) as Table 3.5 below:

Table 3.5: Comment and suggestion for each condition (Campa, 2009)

Condition	Comment
$F_r \leq F_t$	Protection are sufficient for risk scenario (if $F_r << F_t$, then there is over design according to the acceptability criteria)
$F_r \geq F_t$	The protection are insufficient for the risk scenario (the combined IPLs effectiveness are not enough to reduce the initiating event frequency to the maximum accepTable frequency for the scenario. Need to establish a risk control strategy based on the required effectiveness. Frequency reduction, $S_{ADD} = F_r - F_t$. Case 1: $S_{ADD} \leq 1$ If we already have IPLs , we need to recommend improving the effectiveness of these layers (more frequent and systematized maintenance program, enhance operators response to alarms by training / emergency drill. If there are no IPL applicable, need to recommend installing a non-SIS PL. Only if no non-SIS layers can be applied, we could suggest using a SIS with SIL 1. Case 2: $2 \leq S_{ADD} \leq 4$ Non-SIS protection layers and existing protection layer improvement must be suggested if possible and reevaluated to determine if this is enough. If no non- SIS protection layers can be suggested and existing protection have been improved, we can suggest installing a SIS. Case 3: $S_{ADD} \geq 4$ The value of SADD is very high and a SIS protection would not be enough to mitigate the risk. Therefore reevaluation of the equipment or process searching for a high effectiveness solutions and second, implement several SIS and non-SIS protection layers until the risk is at accepTable level. If a SIS is recommended, the required SIL can be determined from the SADD value after considering the other non-SIS alternatives using Table 3.4.

3.2. Tool Development

In order to develop the tool required in this project, the flow for the function of the tool must be first develop. The tool is expected to:

1. Receiving initial inputs namely: Consequence Severity, Initiating Event Frequency and Probability of Failure on Demands (PFD) for the existing protective layers.
2. Compute the effectiveness of the existing protective layer and hence the amount of risk reduction achieved.
3. Determine whether the current protection layer is sufficient or insufficient and provide some recommendation.

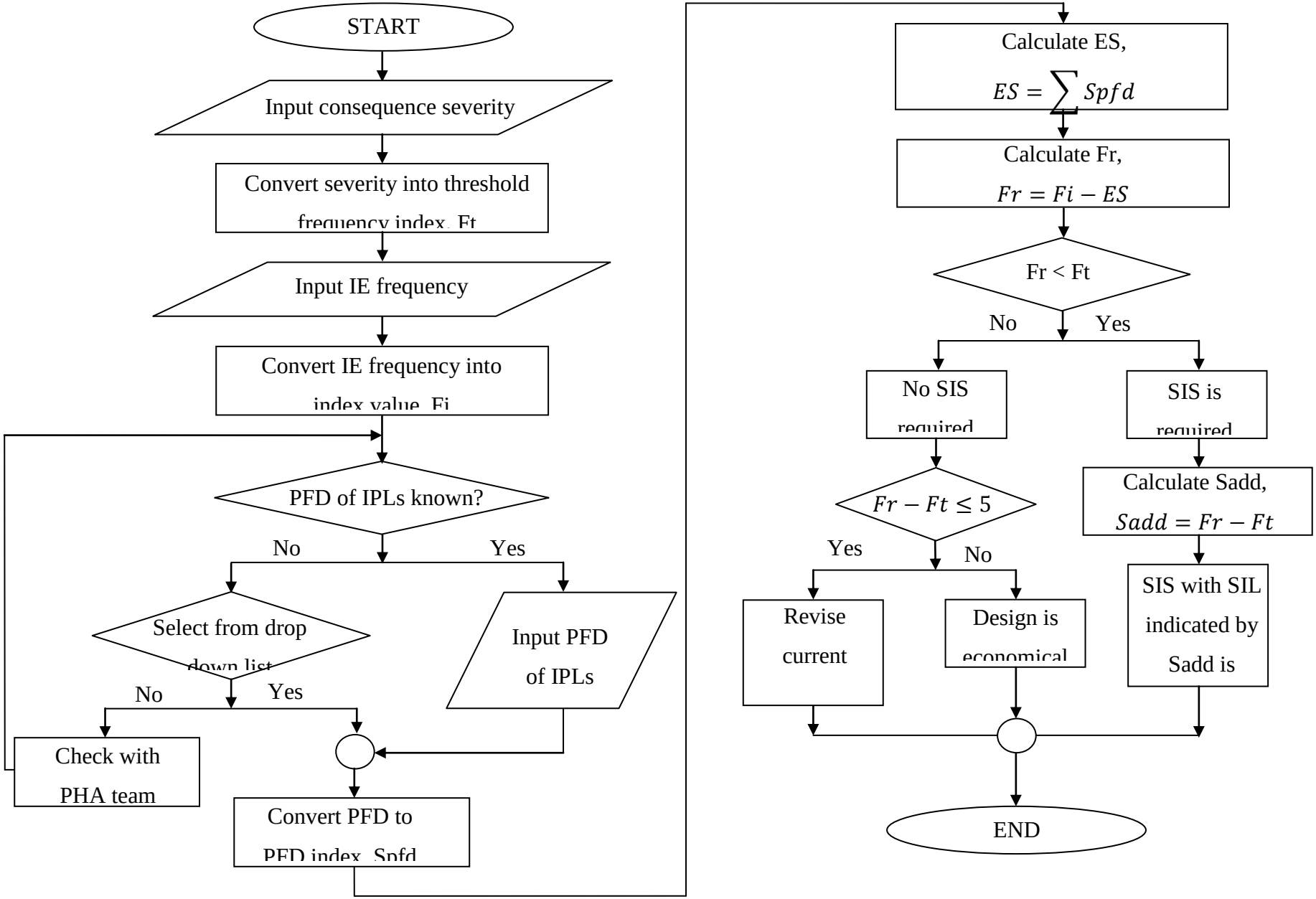


Figure 3.3: Flow chart for the proposed tool

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Results

4.1.1 Case 1: Hexane Storage Tank (Cui et al, 2012)

Case text

The Hexane Storage Tank example from the CCPS's LOPA guidance book is used here to illustrate how LOPA evaluation is being done. Hexane prior process (not shown) flows continuously into the surge tank under applied pressure. The level is controlled by a level control loop (LIC-90) that measure and throttles a level valve (LV-90) to a set value.The LIC control loop includes a high level alarm (LAH-90) to alert the operator.
Note: Tank is located in a dike with 1.5 tank capacity (120, 000 lbs)

Table 4.1: Information available after HAZOP (study node: T-401, deviation: High level)

Cause	Consequence	Safeguard	Recommendation
Low control valve transfer or fails open	High pressure in surge tank	Relieve valve – discharges to dike	
	Loss of containment (if the overpressure exceeds the tank pressure rating)		
	Release of Hexane, fire hazard affecting large area, exceed the capacity of dike	Emergency responce procedure	Consider to install SIS
		Dike of 1.5 vessel capacity	

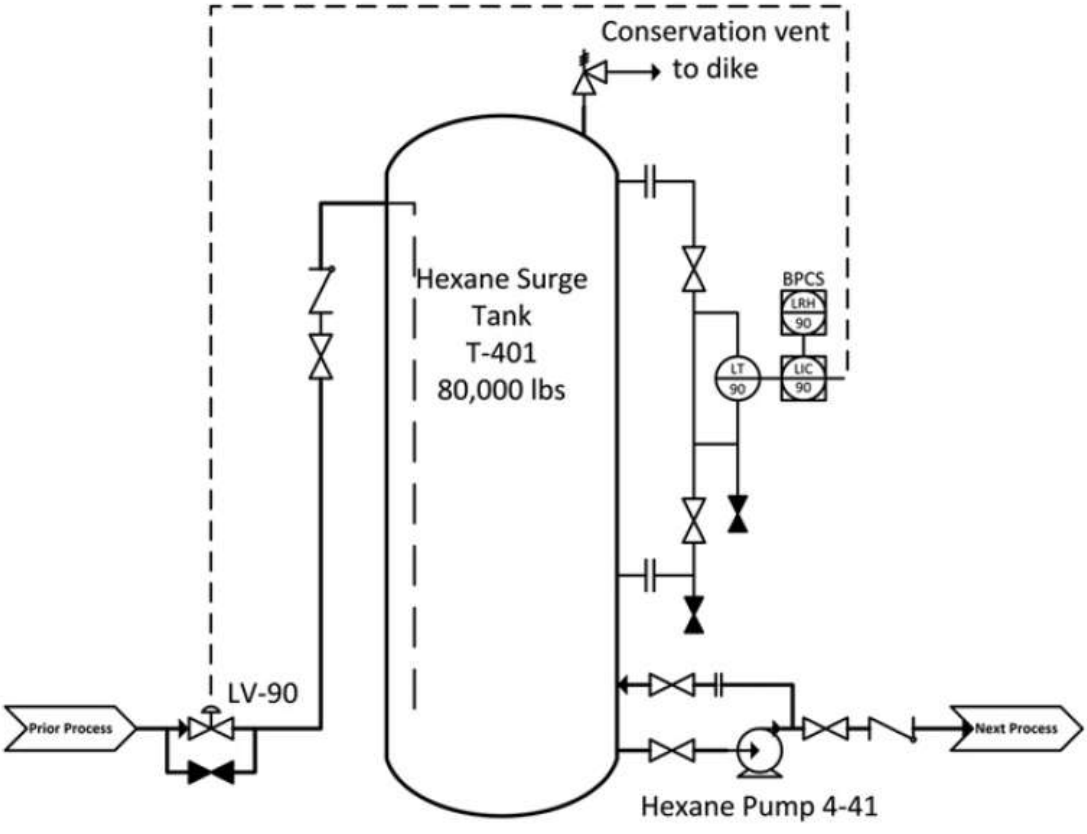
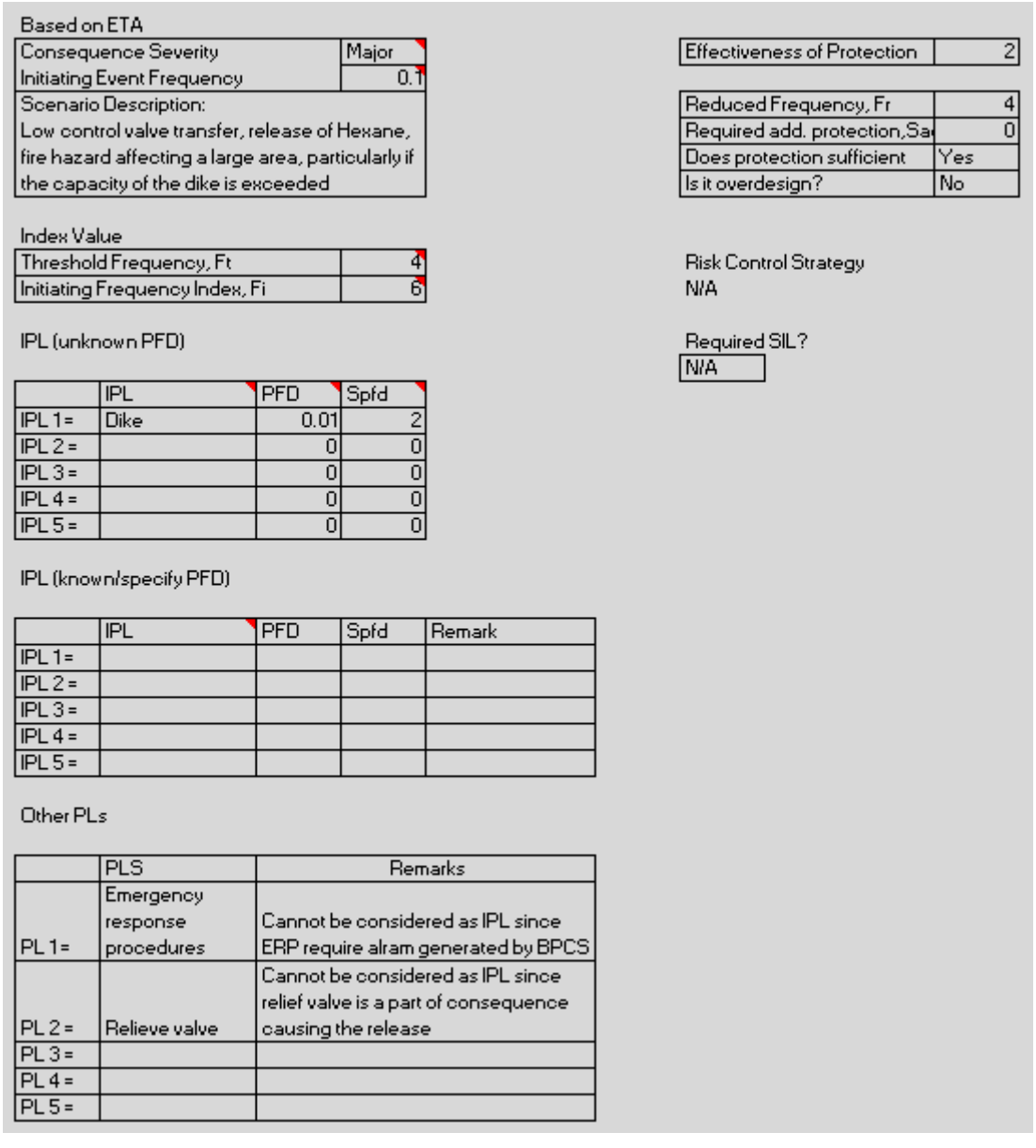


Figure 4.1: Case study node (CCPS, 2001)

Table 4.2: Input data available to continue for LOPA (Cui et al)

Consequence under study (Severity)	Release of Hexane, fire hazard (Catastrophy)
Initiating event (frequency)	BPCS LIC failure (1×10^{-1})
Tolerable Risk	1×10^{-5}
Independence Protective Layer	
Dike sized 120, 000 lbs	PFD = 0.01



Based on ETA

Consequence Severity	Major
Initiating Event Frequency	0.1
Scenario Description: Low control valve transfer, release of Hexane, fire hazard affecting a large area, particularly if the capacity of the dike is exceeded	

Effectiveness of Protection	2

Reduced Frequency, Fr	4
Required add. protection,Sa	0
Does protection sufficient	Yes
Is it overdesign?	No

Index Value

Threshold Frequency, Ft	4
Initiating Frequency Index, Fi	6

Risk Control Strategy
N/A

IPL (unknown PFD)

Required SIL?
N/A

	IPL	PFD	Spfd
IPL 1=	Dike	0.01	2
IPL 2=		0	0
IPL 3=		0	0
IPL 4=		0	0
IPL 5=		0	0

IPL (known/specify PFD)

	IPL	PFD	Spfd	Remark
IPL 1=				
IPL 2=				
IPL 3=				
IPL 4=				
IPL 5=				

Other PLs

	PLS	Remarks
PL 1=	Emergency response procedures	Cannot be considered as IPL since ERP require alram generated by BPCS
PL 2=	Relieve valve	Cannot be considered as IPL since relief valve is a part of consequence causing the release
PL 3=		
PL 4=		
PL 5=		

Figure 4.2: Computed result for Case 1

The sequence severity is assigned as Major which will depend on size of release and consequence on production and facility. Initial event frequency is assigned 0.1 for BPCS instrument loop failure. Corresponding index frequency is denoted as 6 for 0.1 likelihood per year or one occurrence every ten years.

In this scenario, emergency response procedure cannot be included as an IPL as the initiating event is BPCS which will trigger the alarm for human response. Threshold frequency is assigned by tolerable risk accepted by the organisation. From the program,

no additional protection is required as the reduced frequency with available IPL is same as threshold frequency. However, if the size of release is significantly bigger, the consequence may fall to Catastrophe with threshold frequency 3. In this case, S_{add} 1 will be obtained which signify an additional protective layer is required. Campa and Cruz-Gomez suggested that for S_{add} smaller or equal to 1, a non-SIS can be recommended or if possible simply improving the current protective layers with regular reliability maintenance to increase the S_{pfd} of the layers.

This however deviate from result calculated by L. Cui et al.

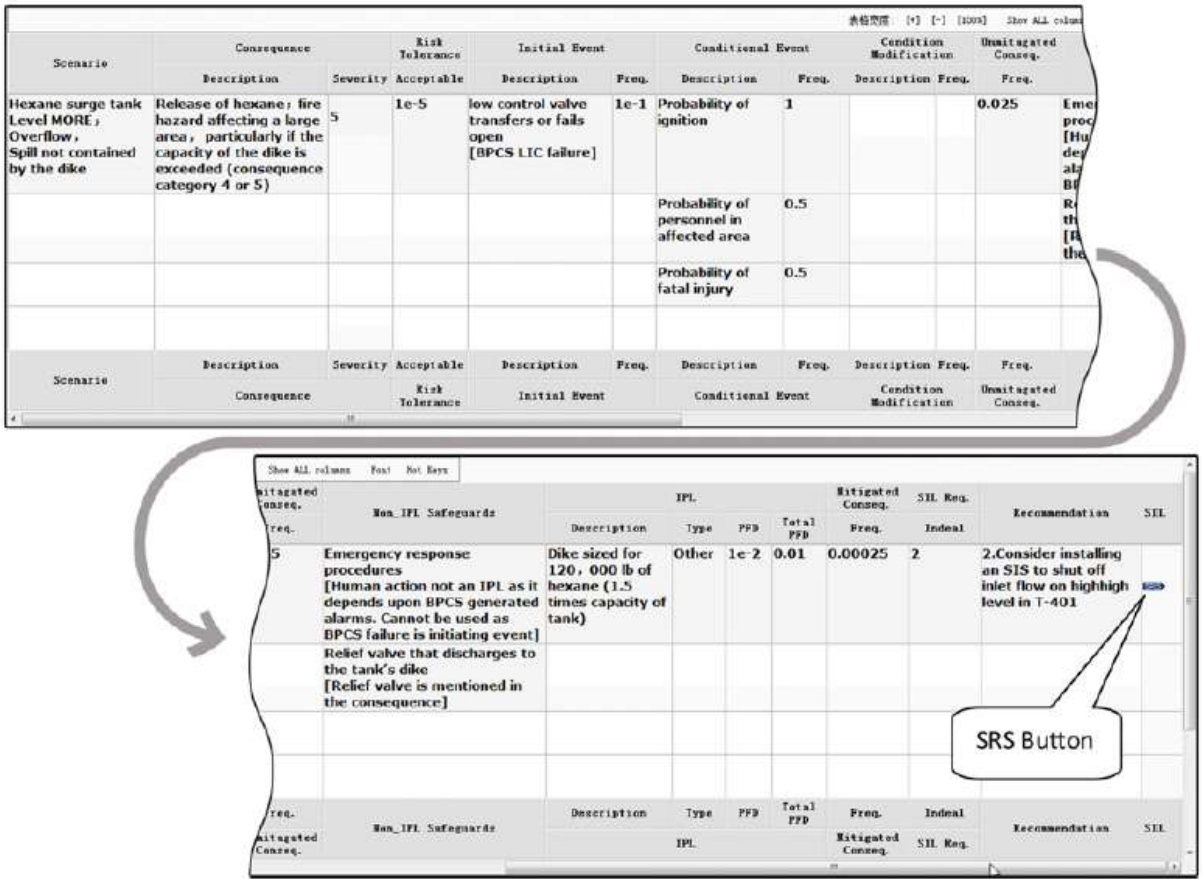


Figure 4.3: Comparison Analysis with other LOPA tools (Cui et al)

Cui, using HASILT system (using normal decimal instead of index) found that a SIF with requirement SIL 2 is required (maximum tolerable risk of 10^{-5} per year and frequency of mitigated event of 2.5×10^{-4} per year, LOPA ratio of 0.04).

It is found that results from both methods are contradicting. One of obvious parameter differentiate the result is the presence of conditional modifier in HASILT software by Cui. Conditional modifier is not necessary compulsory, however the risk under investigation for Cui method is risk towards harmful to personal or society. Meanwhile, the developed method only investigates the risk of the hazardous process. Thus including conditional modifier as an option in the tool is a valid argument since the organisation or LOPA analyst need to be able to determine SIL of both hazardous and harmful installation.

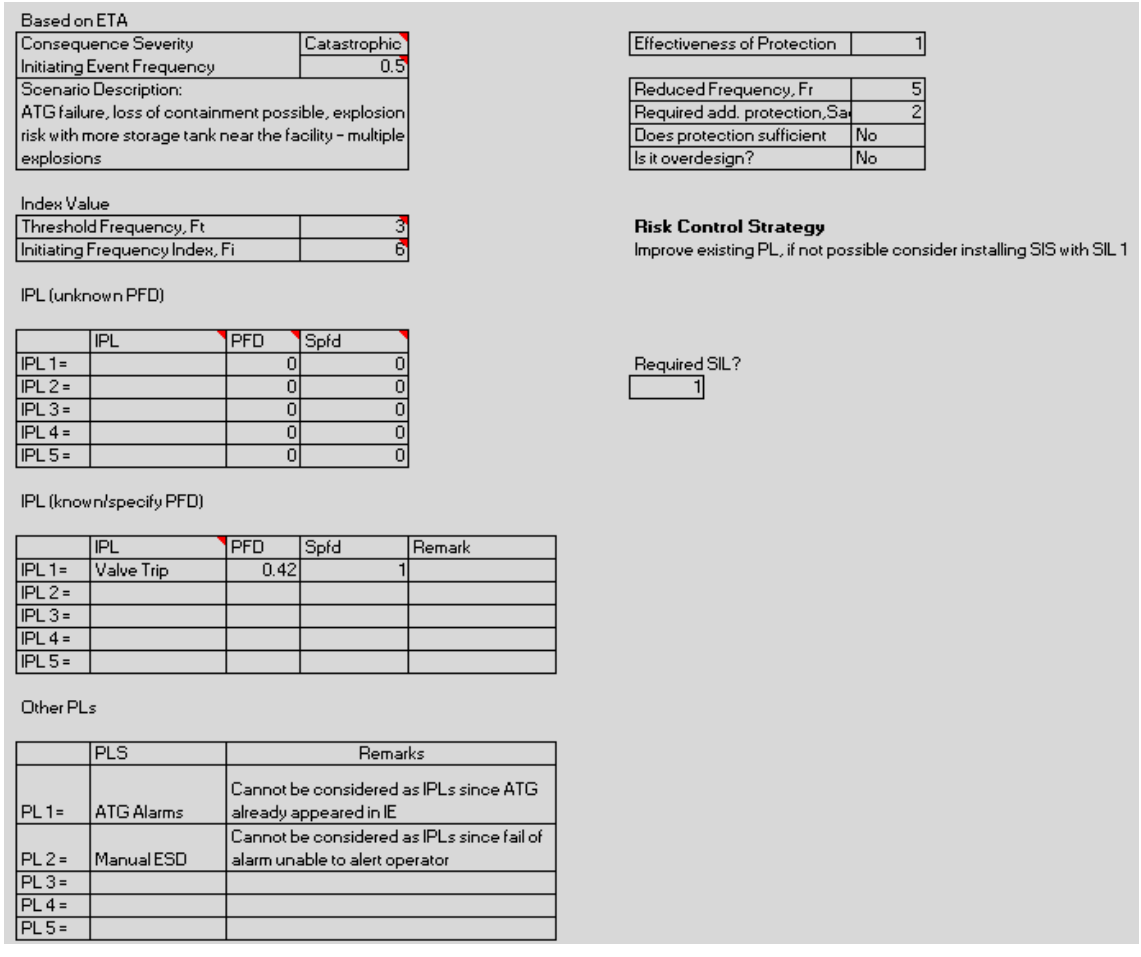
4.1.2. Case 2: Buncefield Incident, 2005

Case text

A two tanks storing a flammable substance, with properties similar to those of petrol. The tanks are filled from a main processing plant via a pipeline. Tank gauging and overfill protection are provided by Automatic Tank Gauge (ATG) and operator response; the operator is able to initiate a manually emergency shutdown (ESD) from the control room. Magnetically coupled float switches are used to initiate automatic closure of relevant plant valves. Loss of level signal, plant control valve signal or loss of air automatically closes the relevant plant valves.

Table 4.3: Input data available (Health and Safety Laboratory, 2009)

Consequence under study (Severity)	Series of explosion, Catastrophe
Initiating event (frequency)	ATG failure (0.5)
Tolerable Risk	ALARP (1×10^{-6})
Protective Layers	
Manual ESD	0.40
ATG Alarms	0.30
Valve Trip	0.42



Based on ETA

Consequence Severity	Catastrophic
Initiating Event Frequency	0.5
Scenario Description: ATG failure, loss of containment possible, explosion risk with more storage tank near the facility – multiple explosions	

Effectiveness of Protection	1

Reduced Frequency, Fr	5
Required add. protection, Sa	2
Does protection sufficient	No
Is it overdesign?	No

Index Value

Threshold Frequency, Ft	3
Initiating Frequency Index, Fi	6

Risk Control Strategy
Improve existing PL, if not possible consider installing SIS with SIL 1

IPL (unknown PFD)

	IPL	PFD	Spfd
IPL 1 =		0	0
IPL 2 =		0	0
IPL 3 =		0	0
IPL 4 =		0	0
IPL 5 =		0	0

Required SIL?
1

IPL (known/specify PFD)

	IPL	PFD	Spfd	Remark
IPL 1 =	Valve Trip	0.42	1	
IPL 2 =				
IPL 3 =				
IPL 4 =				
IPL 5 =				

Other PLs

	PLS	Remarks
PL 1 =	ATG Alarms	Cannot be considered as IPLs since ATG already appeared in IE
PL 2 =	Manual ESD	Cannot be considered as IPLs since fail of alarm unable to alert operator
PL 3 =		
PL 4 =		
PL 5 =		

Figure 4.4: Computed results for case 2

The second case is base on "Buncefield incident" where a series of explosion occurred where the main cause is the fuel storage tank overfills. The input for the LOPA procedure is obtained from a consultant report on the incident as requested by Buncefield Standard Task Group (Health and Safety Laboratory, 2009). The severity of the consequence is very high due to multiple explosions involved, therefore a "Catastrophe" category is well justified in this case. On the other hand, the ATG failure is assumed that it fails once every two years (0.5 per year) which indicate weak reliability of the ATG as the initiating event (common value is 0.1 per year). From Table 3.2, the frequency index relative to the value will be 6.

Next, from the lists of protective layers available, Automatic Tank Gauge (ATG) alarm and manual Emergency Shudtdown (ESD) fail to meet the "independence" criteria as

outlined by CCPS. Therefore, only trip valve qualify to provide risk reduction towards the initiating risk. From computed data, the reduced frequency index is still bigger than threshold frequency index and therefore additional protection is suggested.

From S_{add} value obtained, recommendation from Champa and Cruz-Gomez can be used for early risk control strategy. Therefore, this tool suggests installing SIS with SIL 1 for the process system. Table below show summary other LOPA done on the same case by various consultants for Buncefield Incident.

Table 4.4: Key Figures from the LOPA case analysis (HSL, 2009)

LOPA results presented by	Corporate risk criteria	Target SIL (Value if stated)	Calculated SIL Gap
1	1×10^{-6}	No SIL recommended	No Shortfall
2	1×10^{-6}	SIL 2	1.08×10^{-1}
3	1×10^{-5}	No SIL recommended	No Shortfall
4	1×10^{-6}	SIL 2	7.65×10^{-2}
5	1×10^{-6}	SIL 2	4.74×10^{-1}
6	1×10^{-6}	SIL 2	6.24×10^{-1}
7	1×10^{-5}	SIL 2	1.34×10^{-2}
8	1×10^{-6}	SIL 2 (initially no SIL is recommended)	5.22×10^{-4}
9	1×10^{-6}	SIL 2	3.43×10^{-2}
10	1×10^{-6}	No SIL recommended	No Shortfall
11	1×10^{-6}	SIL 2	2.25×10^{-1}
12	1×10^{-6}	SIL 2	1.09×10^{-2}
13	1×10^{-6}	SIL 2	2.91×10^{-1}
14	1×10^{-6}	SIL 2	7.21×10^{-3}
15	1×10^{-6}	SIL 2	6.54×10^{-3}

Please note that the tool developed re-evaluate LOPA presented by Company ID 8. The company initially does not recommend SIS. A revision was made after the initial report submission recommending SIS of SIL 2. The “Corporate Risk Criteria” refer to the threshold frequency, where 1×10^{-6} is value largely accepted by industry for Catastrophe consequence.

The main concern is the final recommendation from various LOPA study. Most of the LOPA consultants recommend SIL 2 for this case while the current proposed tool recommend SIL 1. The main different between the studies are that the definition of IPLs and value stated vary widely. Since the input for the tool is taken from Company ID 8 which initially does not recommend additional SIL, some of the PFD of IPLs may be revised. Nevertheless, unavailability of process flow diagram for the case under study limits identification of IPLs. The final recommendation by Health and Safety Laboratory for this incident is SIL 2 while the proposed tool only recommends SIL 1. Further study can be done to improve the result by using sensitivity analysis so that the main factor contributing to the final result is carefully re-evaluated.

4.1.3. Case 3: Failure of level transmitter (LT) indicating a false high level in a high pressure sour gas amine treatment unit (Campa and Cruz-Gomez, 2009)

Case text

Figure 3.5 shows the simplified process flow of the absorber section of a high pressure sour gas amine treatment unit. Sour gas is a natural gas containing hydrogen sulphide (H_2S). Lean amine is used to remove H_2S in absorber column, T-1. Based on HAZOP study of the process as shown in Table 4.5, the following scenario is selected (Node: High pressure amine absorber (T-1) and Deviation: high level)

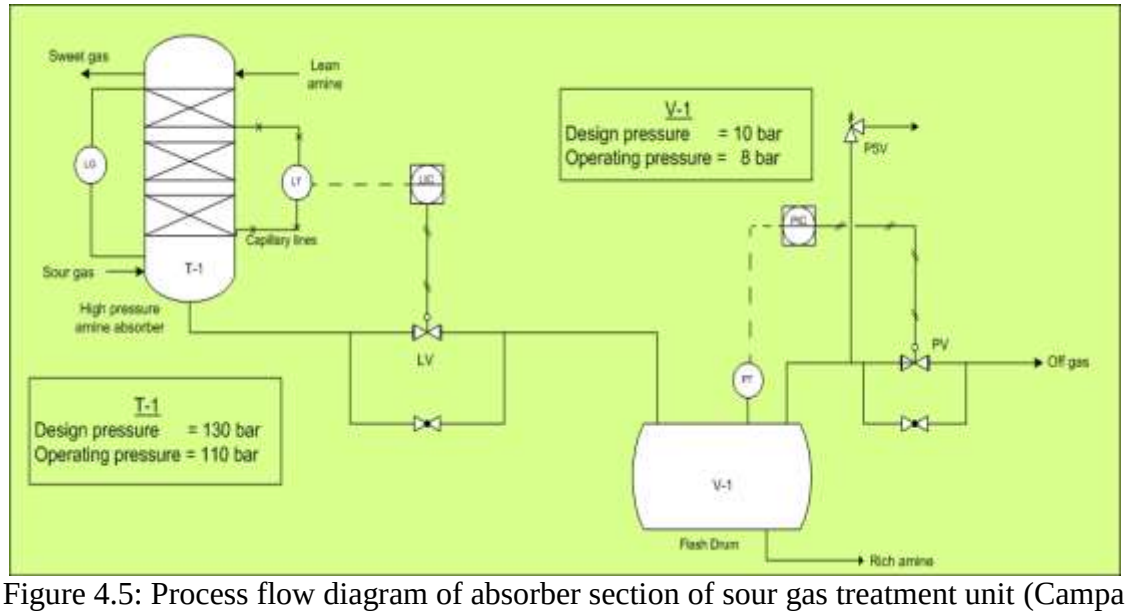


Figure 4.5: Process flow diagram of absorber section of sour gas treatment unit (Campa and Cruz-Gomez, 2009)

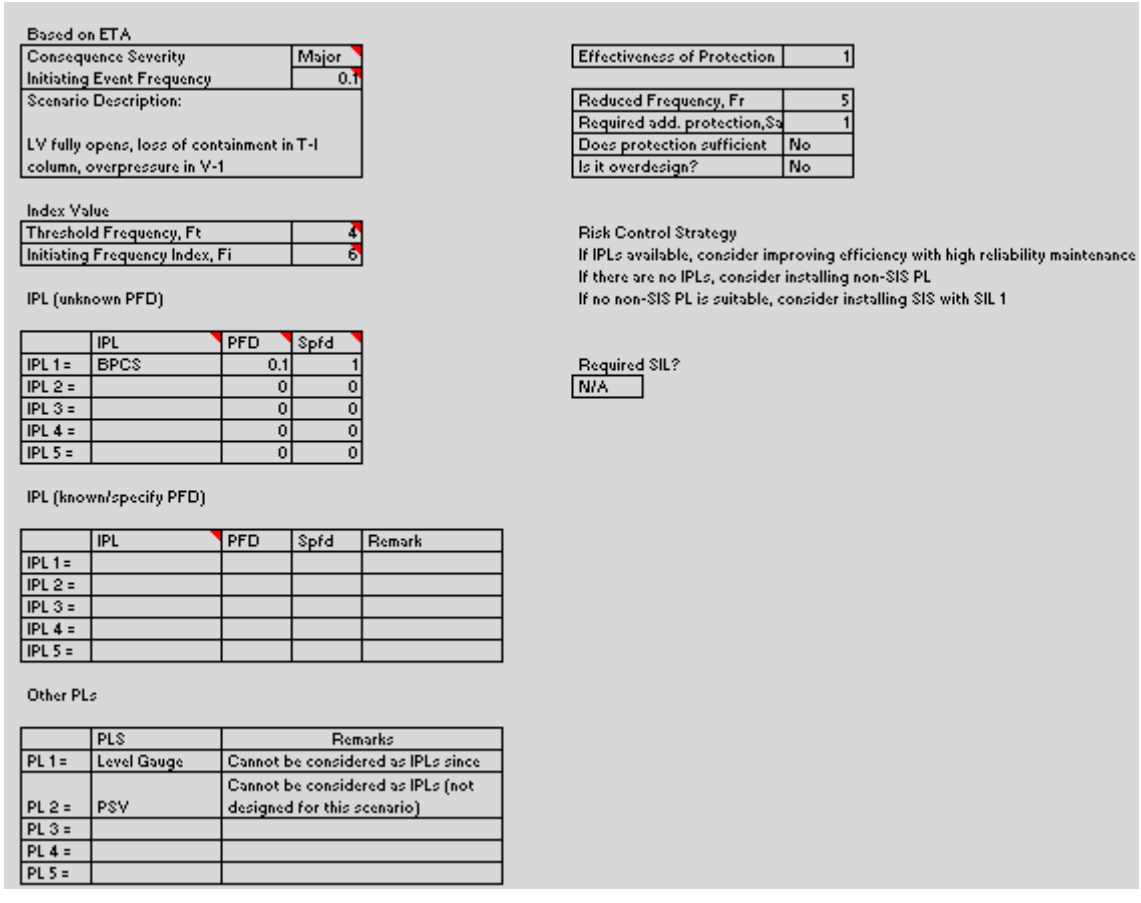
From the study node identified, HAZOP study of the process is summarise as follows:

Table 4.5: Hazards and Operability (HAZOP) study of the process

Cause	Consequence	Safeguards	Recommendations
Failure of LT indicating a false high alarm	LV fully opens, loss of liquid seal in T-1 column (LG indication is unreliable in this case)	High pressure alarm in V-1, PIC and operator responce	Consider adding a SIS and implement a SIF for this scenario
	High pressure gas flows to low pressure flash tank V-1 (not designed for this scenario)		Lock LV bypass valve in closed position
	LV bypass valve could erroneously opened in an attempt to control the 'high level' in t-1, worsening the scenario		Update emergency operation procedures with this scenario and train operator accordingly
	Potential explosion of V-1		

Table 4.6: Extracted information available for LOPA

Consequence Description/ Category	Assuming facility spacing is adequate. Personal concentrated in bunker control room at sufficient distance. Category 4: Major
Initiating event frequency	Failure of a level transmitter indicating false high level (0.1)
Independent Protection Layers	
1. BPCS alarms and Human Action	1×10^{-1}
2. Level Gauge (LG)	Cannot be considered independent since LG is part of IE
3. PSV	Not designed for this scenario



Based on ETA

Consequence Severity	Major
Initiating Event Frequency	0.1
Scenario Description:	
LV fully opens, loss of containment in T-I column, overpressure in V-1	

Effectiveness of Protection	1

Reduced Frequency, Fr	5
Required add. protection,Sa	1
Does protection sufficient	No
Is it overdesign?	No

Index Value

Threshold Frequency, Ft	4
Initiating Frequency Index, Fi	6

Risk Control Strategy
If IPLs available, consider improving efficiency with high reliability maintenance
If there are no IPLs, consider installing non-SIS PL
If no non-SIS PL is suitable, consider installing SIS with SIL 1

IPL (unknown PFD)

	IPL	PFD	Spfd
IPL 1 =	BPCS	0.1	1
IPL 2 =		0	0
IPL 3 =		0	0
IPL 4 =		0	0
IPL 5 =		0	0

Required SIL?

N/A

IPL (known/specify PFD)

	IPL	PFD	Spfd	Remark
IPL 1 =				
IPL 2 =				
IPL 3 =				
IPL 4 =				
IPL 5 =				

Other PLs

	PLS	Remarks
PL 1 =	Level Gauge	Cannot be considered as IPLs since
PL 2 =	PSV	Cannot be considered as IPLs (not designed for this scenario)
PL 3 =		
PL 4 =		
PL 5 =		

Figure 4.6: Computed results for case 3

The consequence severity is assigned as major and low initiating event frequency of 0.1. Initiating event denoted give a high probability of occurrence and therefore corresponding index frequency of 6 is denoted.

Only one of the PLs available meets the “independence” criteria which is the process alarm. Due to only one IPL, low reduced frequency is obtained and therefore resulted in insufficient protection. Therefore, it is important to view the risk control strategy for the process.

In this case, Campa and Cruz-Gomes recommendation is displayed as presented below (S_{add} required = 1):

- If IPLs already exist, improve the protection layers (more frequent and systemised maintenance program, enhance operator response to alarms by training or emergency shutdown.
- If there are no IPL applicable, need to recommend installing a non-SIS Protection Layer.
- Only if no non-SIS layers can be applied, suggesting on using a SIS with SIL 1.

As a comparison with another analysis made on the same scenario (Fakhirin, 2010), it is found that the result of the proposed tool is similar to Interlock by Fakhirin. The system is therefore can be concluded as not sufficiently protected. Improvement on the existing protective layer may be carried out before SIS can be installed.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

In the conclusion, the proposed tool managed to provide a framework to assist LOPA analyst evaluate a scenario with standard method. The idea is that within the same organisation, the employee (LOPA analyst) may retire thus carry the knowledge with them. This proposed tool provides a mean of knowledge transfer and consistency for the organisation and therefore promotes safety any of their facilities. Prior determination of SIL using LOPA, the protective layers (PLs) play the most important role. It is important to understand the concept of independence of the PL before it can qualify to be considered as an independent protective layer (IPL). Among the main rules outlined by CCPS is the importance of maintaining, testing and record-keeping for each IPL. This routine basically provides a better source of information especially the probability of failure on demand (PFD) of IPL before proceeding with the LOPA. Moreover, the PFD is also justified with proper documentation thus give a more accurate LOPA result. Another importance of the proposed tool is that as suggested by Bridges (2009), LOPA analyst must be separated from process hazard analysis team (PHA) to prevent distracting the PHA team in brainstorming for every possible situation. A sole analyst is often quote as sufficient to do LOPA and a spreadsheet framework is highly recommended to assist the analyst. Future study shall include a statistical analysis and sensitivity analysis which provide a clear indication on the best course of action that should be taken to minimise risk and maximise protection within the ALARP philosophy.

REFERENCE

Baybutt, P. (2007). An improved Risk Graph Approach for Determination of Safety Integrity Levels (SILs). *Process Safety Progress*, 26:66–76.

Bridges, W. B., & Clark, T. (2009). Key Issues with Implementing LOPA (Layer of Protection Analysis) – Perspective from One of the Originators of LOPA. *11th Plant Process Safety Symposium.* New York: AICHE.

Campa, H. J., and Cruz-Gomez, M. (2009). *Determine SIS and SIL using HAZOPS.* Mexico City: Wiley Interscience.

Center for Chemical Process Safety. (2001). *Layer of Protection Analysis:Simplified Process Assessment.* New York: Center for Chemical Process Safety.

Cui, L., Shu, Y., Wang, Z., Zhao, J., Qiu, T., Sun, W., et al. (2012). HASILT: An intelligent software platform for HAZOP,LOPA,SRS and SIL verification. *Reliability Engineering and System Safety* , 56-64.

Fakhirin, W. M. (2010). *Utilizing Layer of Protection Analysis (LOPA) in Verification of Safety Integrity Level (SIL) of Instrumented System.* Tronoh: UTP.

Gulland, W. G. (2004). Method of Determining Safety Integrity Level Requirements. *Safety-Critical System Symposium* (pp. 1-16). London: Springer-Verlag London Ltd.

Health and Safety Laboratory. (2009). *A Review of Layer of Protection Analysis (LOPA) analyses of overfill of fuel storage system.* Buxton: Health and Safety Executive.

Lassen, C. A. (2008). Layer of Protection Analysis (LOPA) for Determination of Safety Integrity Level (SIL). Snaroya: Norwegian University of Science and Technology.

Marszal, E. M., and Scharpf, E. W. (2002). *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis.* United States: Instrumentation, Systems and Automation (ISA).

Zatil, A. R. (2009). *Using Layer of Protection Analysis (LOPA) to Determine Safety Integrity Level (SIL) for Hazardous Installation,*. Tronoh: UTP.