DEVELOPMENT OF COMPLEXITY INDEX OF PROBABILITY FAILURE FOR INHERENTLY SAFER DESIGN

by

YUSUF ISKANDAR WAHYU SALAM

14754

Dissertation submitted in partial fulfilment of

the requirements for the

Bachelor Of Engineering (Hons)

(Chemical Engineering)

JANUARY 2015

Universiti Teknologi PETRONAS

32610 Bandar Seri Iskandar,

Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

DEVELOPMENT OF COMPLEXITY INDEX OF PROBABILITY FAILURE FOR INHERENTLY SAFER DESIGN

by

Yusuf Iskandar Wahyu Salam
14754

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,

____
(Dr. Risza Rusli)

UNIVERSITI TEKNOLOGI PETRONAS

32610 BANDAR SERI ISKANDAR,

PERAK DARUL RIDZUAN

JANUARY 2015

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.

YUSUF ISKANDAR WAHYU SALAM

ABSTRACT

In Inherently Safer Design (ISD) of a Process design, it’s goal is to eliminate or reduce a process's hazard. This paper discusses and prove on the simplification approach of ISD in reducing the failure frequency in a complexity of Independent Protection Layers (IPLs). Nevertheless challenging the concept of Layer of Protection Analysis (LOPA) that suggests that the more IPLs installed, the safer it is. On the other hand, This paper suggests total number of IPLs needed in a system can be limited into certain tolerable amount but still theoretically safe. By isolating the scope of the study to likelihood part only, the study is carried out accordingly.

ACKNOWLEDGEMENT

This project is made possible through the help and support from everyone, including: parents, lecturers, family, friends, and in essence, all sentient beings. Especially, please allow me to dedicate my acknowledgement of gratitude toward the following significant advisors and contributors:

First and foremost, the author would like to express his deep gratitude to Dr. Risza Bt. Rusli for her support, teaching and encouragement. She kindly read throughout the paper and offered invaluable detailed advices on grammar, organization, and under her supervision, the author gained a lot of experiences and knowledge.

Secondly, the author would like to show his appreciation to the most hardworking person who taking care of him along the project journey, Mrs. Mardhati Zainal Abidin, his mentor for this paper project. She is the most reliable person who teach a lot of technical knowledge while also educate the author how to independently relate to the real thing.

Finally, the author sincerely thank to the author's parents, family, and colleagues who provided the author with inspiration and support. This product of report would not be possible without all of them.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

In order to complete the study in Chemical Engineering Degree, students need to take Final Year Project (FYP) course. FYP comprises of total 6 credit hours and it is a individual project-based course. The final year project is divided into two phase; FYP1 during the 8th semester and FYP2 in the 9th semester of the undergraduate program. This project is an individual research project in connection with a special engineering problem and under the guidance of a faculty member. The purpose of the project is to develop a framework, which will enhance students' skills in the process of applying knowledge, expanding thoughts, solving problems independently and presenting findings through minimum guidance and supervision. The topic was proposed by a senior lecturer, Dr. Risza Binti Rusli and eventually will be the supervisor for the project.

1.1 Background Of Study

Inherent means existing as essential constituent or characteristic, something intrinsic. Therefore, something is inherent if it exists "as an essential constituent or characteristics." When something is inherently safer. safety is built into the process or product not added on. Hazards are eliminated not controlled, and the means by which the hazards are eliminated are so fundamental to the process design that they cannot be changed or defeated without changing the process.

In many cases, this will result in simpler and less costly plants. If extensive safety systems are required to control major hazards, they introduce complexity, along with cost, both in the initial investment for the safety equipments as well as for ongoing operating cost for maintenance and operation.

Because ISD's goal is to eliminate or reduce a process's hazards one must understand the term hazard. In this context, the definition from CCPS's (2008) Guidelines for Hazard Evaluation Procedures is used. According to this source, a hazard is " an inherent physical or chemical characteristics that has the potential for causing harm to people, environment or property." (Hendershot, 2011)

Inherently Safer Design (ISD) is a philosophy of addressing safety issues in the design and operation facilities that use or process hazardous chemicals. A facilities considering ISD will try to manage process risk within the design by eliminating or significantly reducing hazards. Where feasible, ISD provides more robust and reliable risk management, and has the potential to make the processing technology simpler and economical by eliminating the need for expensive safety systems and procedures.

Thus, it brings us to the chemical process safety strategies to achieve ISD where the first three can be characterized as engineering controls; Inherent, Passive, Active, while the last (procedural) can be categorized as an administrative control. Nevertheless a combination of ISD, engineering and administrative controls will always be required to manage all the process risks. Thus, CCPS (2009) has categorized strategies for designing inherently safer process into four groups; namely substitute, minimize, moderate and simplification.

Some issues come up from the first three; substitute, minimize and moderate having almost similar strategies where it involved directly on the materials or chemical involved in the process. Substitution involve the use of less hazardous materials chemistry and processes, minimization is the reducing of quantities of hazardous materials or size of operating equipment under hazardous condition while moderation involving the reduction of hazards by dilution, refrigeration or process alternatives that operate at less hazardous condition.

On the other hand, the last strategy, simplification require the avoidance of complexities such as multiproduct or multiunit operations or congested pipe or unit settings. Taking Bhopal tragedy for example, the not maintained well system is most likely the reason the event to be occur. the In this paper, we will be focusing on this particular simplification strategies to come up with the complexity index of probability failure.

1.2 Problem Statement

Inherent safety is a proactive approach for loss prevention and risk management. Considering the lifetime costs of a process and its operation, an inherent safety approach can lead to a cost-optimal option. Inherent safety may be achieved at any stage of process design; however, its application at the early stages of process design yields the best results. Despite being an attractive and cost-effective approach, the inherent safety methodology is not widely used. Many reasons have been attributed to this lack of widespread use, the non-availability of systematic tools for the application of inherent safety principles and index being too human bias subjective is perhaps one of the important reason. (Khan & Amyotte, 2004)

The basis of the research is that simpler plant or system provide fewer opportunities for error. This is because taking human nature as one of the factor, most people will tends to go for simpler solutions. For example, an operator who is on the task in the operational field, will have the tendencies to violate the procedures of a complex procedures and instrumentation as long as the result of the action improvised is the same. Taking Bhopal tragedy as an example, the plant was supposed to produced 1/3 of the product produced. The over yield of product to satisfy the profit that they might get and also too many safety system were shut down to lower down the operational cost made the tragedy more costly than they ever imagined. This shows how a complex system might led people to a shortcut and finally an error. How to judge the complexity of a process in a plant is what we are trying to figure out.

In a context of simplification, CCPS suggested that such added-on barriers or complex safety system have disadvantages such as the barrier can be expensive to design, build and maintain and the hazard is still present in the process, where failures of enough layers of protection can still result in an incident. Therefore, it is better applying the inherently safer concepts to the process design and chemistry by simplification at least. (Arthur, 1999,9)

1.3 Objectives & Scope Of Study

From the literature review of past researches, we come up with some objectives:

i. To develop Complexity Index using Layer of Protection Analysis (LOPA) and Fault Tree Analysis (FTA) Approach.
ii. To test the capability of the developed complexity index.
iii. To validate the result from the test with the previous work.

The scope of the study will be solely on using the simplification strategy in developing complexity index together with LOPA and Fault Tree Analysis approach on a particular system, and the complexity calculations will be focusing on the usage of Safety Instrumented System (SIS) and Basic Process Control System (BPCS) in a system as Independent Protection Layers which is all IPLs components before the Loss of Containment.

CHAPTER 2: LITERATURE REVIEW AND THEORY

Throughout this project, some literature reviews were made to gain more understanding on the subject that matters. For example, for the first five review is about the importance of applying inherently safer design with the known strategies. Some of it is about the understanding of the essentials understanding on when to apply the inherently safer design concept throughout the process life cycle. Nevertheless, discussion on misconception of inherently safer design that only deal with consequences.

During the early realization of the importance of process safety in industry, indices have been proposed from time to time for hazard identification for process safety purposes. Noteworthy among them are the Dow fire and explosion index, Dow chemical exposure index, the Mond fire, explosion and toxicity index, FTA, LOPA, QI2SD and I2SI. A few rapid ranking techniques and databases have also been proposed. (Khan, Husain, & Abbasi, 2001) The importance of quantification certain measures were the first idea on why indices and representative value are being invented.

2.1 Inherently Safer design, An Overview of Key Elements

The paper is discussing that inherently safer design is a holistic approach to safer chemical manufacture. In the paper, some overview on key elements of ISD such as minimize, substitute, moderate and simplify were discussed. Nevertheless the process's lifecycle is also considered in context of ISD to further explain the most effective use of ISD as well as other risk mitigation methods and strategies. (Hendershot, 2011)

Nevertheless, the paper discussing on categorization of chemical process safety strategies in four categories.

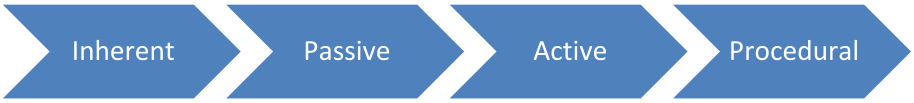


Figure 1: Chemical Process Safety Strategies

The first three can be categorized as engineering controls, while the last (procedural) can be categorized as an administrative control.

While some more categorization of strategies for designing inherently safer design was made into four groups which is substitute, minimize, moderate and simplify. Whereas, Simplification will become the highlight strategy that will be discussed later in results and discussions.

2.2 Implementing Inherent Safety throughout Process Lifecycle

In this paper the problems of implementing inherent safety evaluations and their accuracies in process lifecycle are discussed. For this purpose more closer look on what are the lifecycle phases and how the amount of the knowledge on the process will increase during the design.

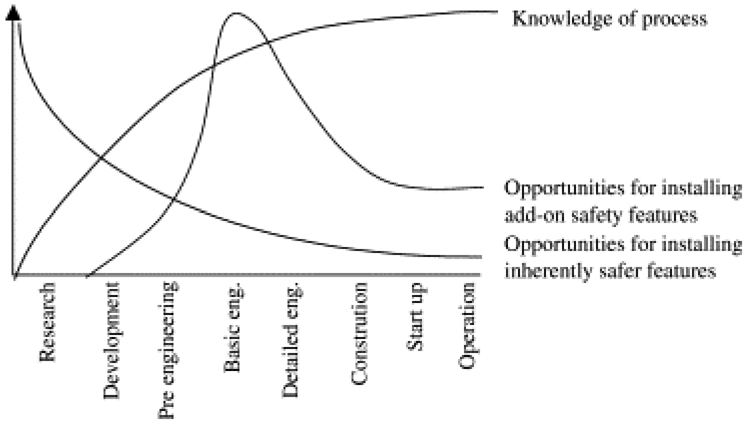


Figure 2: The design paradox and inherently safer design

The paper concluded that the major decision on process principle are done in the process development and conceptual design phases. The most crucial thing in process design concerning safety is getting the fundamentals right as early as possible. As design project proceeds, it becomes more and more costly and difficult to change the process fundamentals

2.3 Inherently Safer Design - Not Only About Reducing Consequences!

Process risk is the function of both probability or likelihood of occurrence of an incident, and also the consequences of the incident.(Hendershot, 2011)

$$Risk = Likelihood \times Consequence$$

There is common misconception that inherently safer design only focuses solely on the mitigating part by reducing or eliminating the consequences. This kind of misconception lead to increasing number of layer of protection that will cost more to reduce or to mitigate consequence instead of using prevention to reduce the likelihood of occurrence.

Some examples of ways to reducing likelihood were explained in certain conditions such as how to reduce the likelihood of reverse flow, excess feed rate to a semi-batch reactor, and using a non-reactive heat transfer fluid.

2.4 Process Intensification Safety Pros and Cons

The paper is discussing on how process intensification (PI) has the potential to be significant factor in the implementation of inherently safety. (Etchells, 2005)

PI is one way in which the inventory of such hazardous substances, and the consequences of a process failure, may be incomparably reduced. The paper also discusses the potential for PI to improve process safety, and some of the possible shortcomings, which should be studied in the light of the legal framework.

Process Intensification are best quoted by Profesor Trevoz Kletz (1991) , 'What you don't have, can't leak!'. Thus we can say, for a hazardous process that having a simpler independent protection layer will have much lesser frequency to leak rather than system with a high complexity.

Some of the potential problems form process intensification were discussed in the paper. Even though in some cases, PI will reduce capital cost and allow new or better products to be produced, some PI technologies may require high-energy inputs to achieve that. Consequently, the high -energy sources may introduce new hazards. Thus this paper suggesting that PI has the potential to be a major factor to implement inherent safety but it needs to be considered as part of the balanced risk assessment of the plant and process involved. (Etchells, 2005)

2.5 Safety Weighted Hazard Index (SWeHI)

SWeHI intents at administering a view as a whole of the industry or the desired process unit, with the regards to the hazards posed by under a given set of external forcing factors such as meteorology and social catastrophes. In the same time, it integrates this information with the safety measures.

In quantitative terms, SWeHI represents the radius of the area under moderate hazard (50% probability of fatality/damage) due to the given unit/plant considering the chemicals, operating conditions, environmental setting, etc. involved at that instant. In mathematical terms it is represented as:

$$SWeHI = B/A$$

Where, B is the quantitative measure of the damage that may be caused by a unit/plant. It is measured in terms of area under 50% probability of damage, A represents the credits due to control measures and safety arrangements made to counter the undesirable situations. (Khan, 2001)

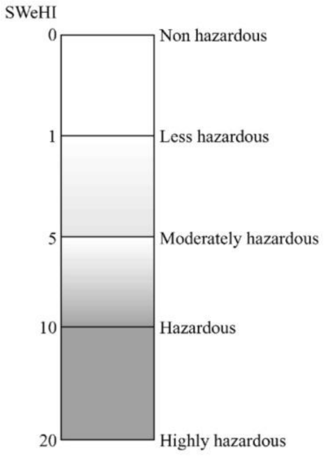


Figure 3: SWeHI Classification

2.6 Dow Fire and Explosion Index (Dow FEI)

The most widely used hazard index and is commonly referred as the Dow Index. It was first reported in 1964. Since then it has evolved into progressively more advanced versions.

The Dow FEI relies on the calculation of a fire and explosion index which is then used to estimates fire protection measures and, in combination with a damage factor, to derive the base maximum probable property damage (MPPD).

The index is calculated as follows. First, a material factor (MF) is obtained. It is a measure of the potential energy released from the material. It is determined by considering the flammability and reactivity of the material and has a range of 1 - 40. Then, two penalty factors (F1 and F2), one for general process hazards (GPHs) and one for special process hazards (SPHs), respectively, are determined. Next, the process unit hazards factor (PUHF), which is the product of these, is calculated. The Dow FEI is obtained as the product of the MF and PUHF.

GPHs are sums of the penalties due to the type of reaction/process, type of chemical handled in the process unit, and drainage and spill control factors of the chemical. SPHs account for the factors due to operation under hazardous conditions, quantity of chemical handled in the unit, and the characteristics of the chemical. Using these three parameters (MF, SPHs, GPHs), MPPD is estimated. Next, utilizing credits for hazard control strategies and safety systems, the `actual probable property damage' (APPD) is calculated. The damage radius is derived empirically from the Dow FEI by using the following equation (Khan et al., 2001):

$$\text{Damage radii} = 0.84 \times \text{Dow FEI}$$

2.7 The Mond Fire, Explosion and Toxicity Index (Mond FETI)

The Mond FETI is an extension of the Dow Index. The Mond FETI was developed at the Mond division of ICI. The Mond FETI involves making an initial assessment of hazard in a manner similar to that used in the Dow FEI, but taking into account additional hazard considerations. The potential hazard is expressed in terms of the initial value of a set of indices for fire, explosion and toxicity The material factor is determined as in the Dow method, but in addition, special material hazard factors are introduced. Again, as in the Dow method, use is made of factors for GPHs and SPHs, although some other factors are also incorporated. For example, a quantity factor, based on the inventory of material, and a layout hazard factor are introduced. There are also factors for toxicity hazard. The toxicity index is calculated using the health factor, quantity of chemical in use and the toxicological properties of the chemical. In the second edition and subsequent amendments of the Mond Index, factors which offset hazards were brought into account. These include preventive measures to reduce the frequency of incidents, and mitigation of consequences. These `offsetting factors' are used in the computation of the final values of indices. (Khan et al., 2001)

2.8 Fault Tree Analysis (FTA)

FTA is an analytical method for characterizing the occurrence of a specified, undesired event (Top Event) using a graphic model (the Fault Tree) which represents the logical combination of basic (low-level) events resulting in the occurrence of the Top Event.

The Fault Tree is a graphic "model" of the potential pathways in a complex system which can lead to a foreseeable undesired event. The pathways interconnect several kind of contributory events and conditions, using the Boolean Algebra logic symbols (AND, OR, etc.). The Fault Tree Analysis uses numerical single probabilities of occurrence of the basic events (Component reliability data, or failure data) to evaluate the propagation through the model and eventually assess the expected frequency of the Top Event. A "typical" Fault Tree is presented in figure below.

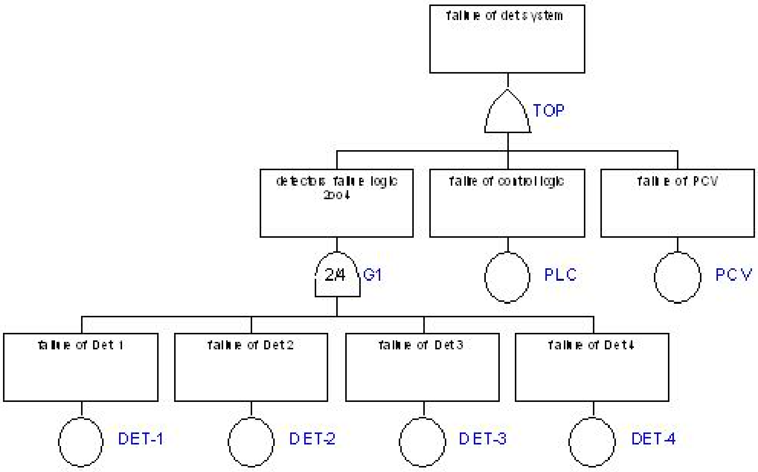


Figure 4: Fault Tree Example

2.9 Layer of Protection Analysis (LOPA) and Inherently Safer Processes

CCPS presented a model for typical layers of protection in a chemical plant (Figure 1). Each layer of protection is a barrier to prevent undesired impact events from reaching people, the environment, or equipment that could be injured or damaged. No layer of protection is perfect; every layer has some probability of failure on demand (PFD)

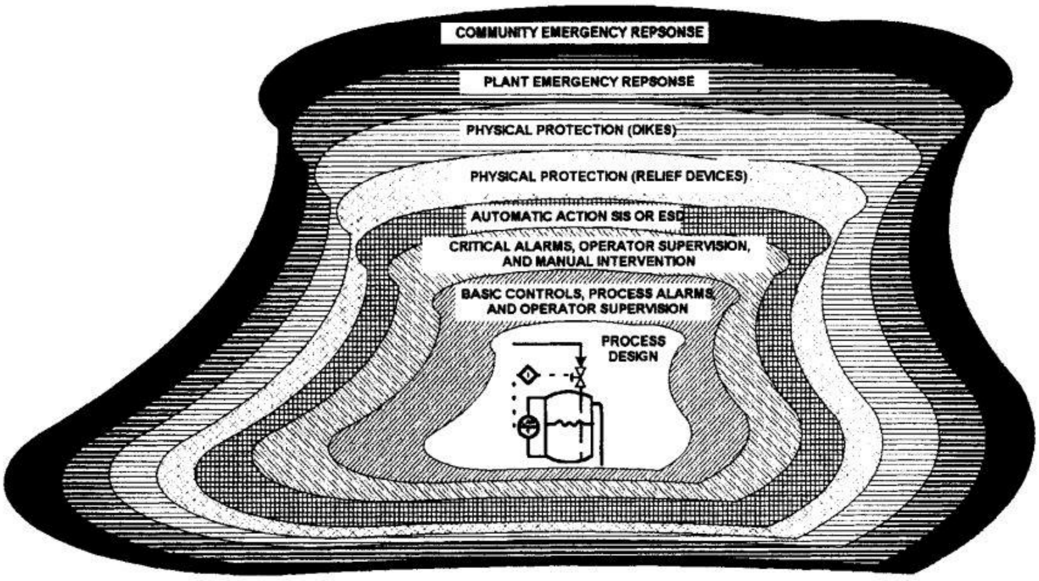

COMMUNITY EMERGENCY REPSONSE
PLANT EMERGENCY REPSONSE
PHYSICAL PROTECTION (DIKES)
PHYSICAL PROTECTION (RELIEF DEVICES)
AUTOMATIC ACTION SIS OR ESD
CRITICAL ALARMS, OPERATOR SUPERVISION, AND MANUAL INTERVENTION
BASIC CONTROLS, PROCESS ALARMS, AND OPERATOR SUPERVISION
PROCESS DESIGN

Figure 5: Layers of protection model for a chemical plant (after CCPs 1993)

LOPA concept can be summarized as:

1. Identify impact events, determine the type of impact (people, environment, property), and classify for severity,

2. List the causes for each impact event,

3. Estimate the frequency of each initiating cause

4. List independent protection layers for each

5. Determine the probability of failure on demand cause-consequence pair, (PFD) for each IPL,

6. Calculate the mitigated event frequency for each cause-consequence pair by multiplying the initiating event frequency by the PFD for each of the applicable IPLS.

7. Compare the mitigated event frequency to the criteria for tolerable risk. (Arthur, 1999)

The LOPA method was primarily developed in the context of denoting Safety Integrity Levels (SILs) for electronic/electronic/programmable electronic safety related systems. LOPA proved to make consistent decisions on the adequacy of the existing or proposed individual protection layers (IPLs) against top events or accident scenarios.

LOPA is based on the computation of single event- consequence scenarios. Started with initial event and end with consequence. Through different initiating events that can lead to the same consequence, all these events must be included to develop scenarios for consecutive assessment.

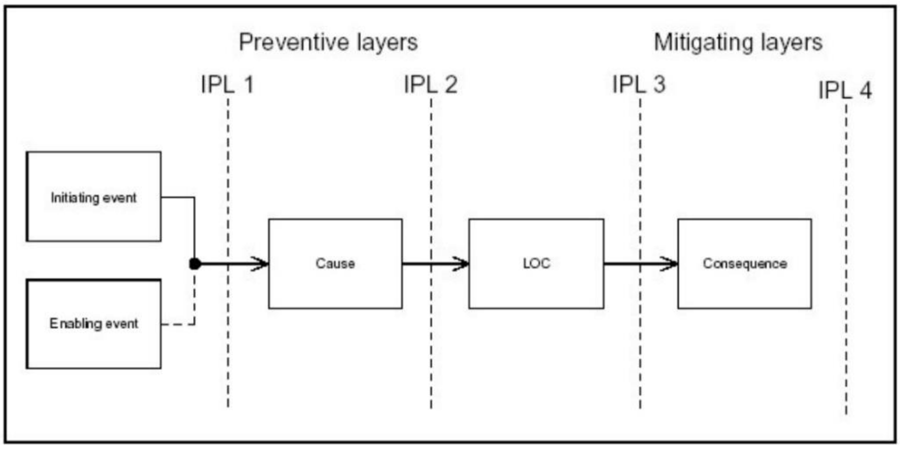


Figure 6: LOPA scenario

2.10 Quantitative Index of Inherently Safer Design (QI2SD)

QI2SD comprises of three key steps: quantify inherent hazards, evaluate inherent safety conflicts in the design alternatives which have been generated according to ISD concept and rank the ISD alternatives for decision making. (Rusli, Shariff, & Khan, 2013).

The methodology identifies potential ISD option by estimating the potential damage and evaluating hazard conflicts that could be transferred to other parts of the process after IS principles are considered. The case study shows that a micro reactor option can be considered as an inherently safer reactor for nitration of the toluene process provided that the hazard conflict levels in moderation and simplification principles have been taken into account to reduce the risk of fire and explosion. QI2SD tool is able to indicate the potential hazards and conflicts in the design based on inherent safety point of view.(Rusli et al., 2013)

2.11 Integrated Inherent Safety Index (I2SI)

The paper presented the conceptual framework of I2SI. The name integrated index was named due to the procedure, when fully developed, is intended to consider the life cycle of the process with economic evaluation and hazard potential identification for each option.

$$I2SI = \frac{ISPI}{HI}$$

As shown, I2SI is composed of two main sub-indices which are: Hazard Index (HI) and Inherent Safety Potential Index (ISPI). The Hazard index is meant for the measure of the damage potential of the process after taking into account the process and hazard control measure. The ISPI on the contrary accounts for the applicability of the inherent safety principles (or guidewords) to the process. Both ISPI and HI are range from 1 to 200. Finally after the calculations, if the I2SI value greater than unity, it denotes a positive response of the inherent safety guide word application (inherently safer option). (Khan, 2004)

From the literature reviews above, we could say the relevancy recentness and are in a good position for the project to be executed. From the paper mentioned above, the importance of inherently safer design in a process life cycle are well discussed. Nevertheless the essence of indexing of one system with numerical to denotes certain severity or acceptable criteria are as important as it is measurable.

CHAPTER 3: METHODOLOGY

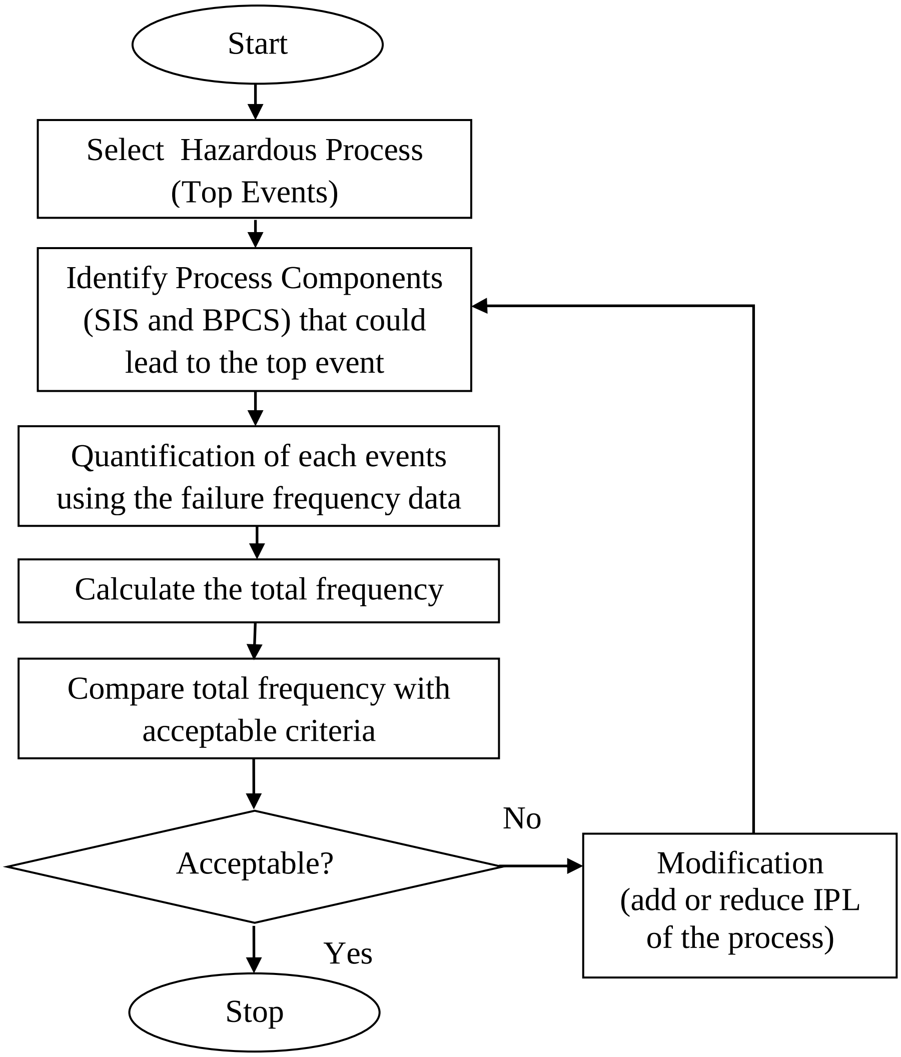

Start
Select Hazardous Process (Top Events)
Identify Process Components (SIS and BPCS) that could lead to the top event
Quantification of each events using the failure frequency data
Calculate the total frequency
Compare total frequency with acceptable criteria
Acceptable?
No
Modification (add or reduce IPL of the process)
Yes
Stop

Figure 7: Methodology

Referring the figure 2 above, the methodology will be proceed firstly by selecting hazardous process in a plant, containing hazard materials or a process that could bring hazardous result if something went wrong. From the process hazard selection, identification of present SIS and BPCS are taken into account. Next, the complexity index that will be constructed so a relationship between the present SIS and BPCS with probability taken from general Fault Tree Analysis of the hazardous process will be evaluated. The evaluation will then be compare with acceptable criteria and previous study with similar hazardous process that undergone a different index study to be compared to validate our index.

CHAPTER 4 : RESULTS & DISCUSSION

4.1 Case Study 1: Overpressure of Reactor

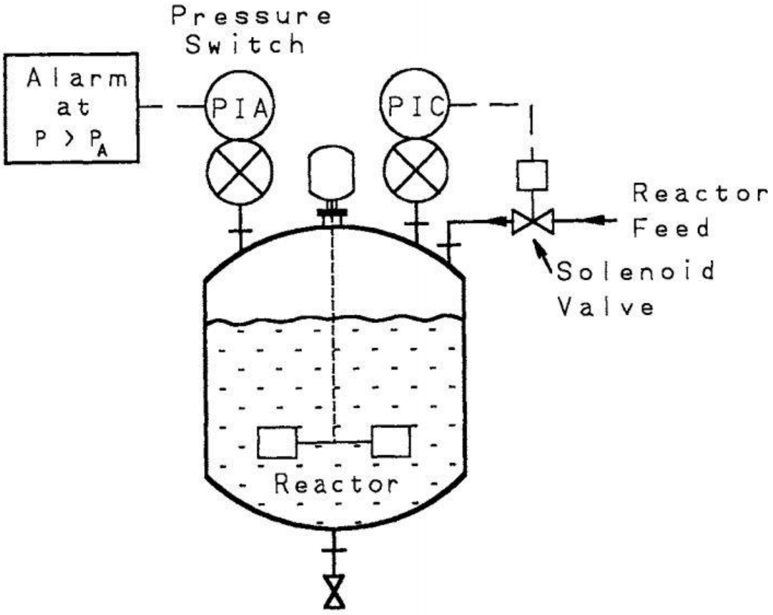


Figure 8: A chemical reactor with an alarm and an inlet feed solenoid. The alarm and feed shutdown systems are linked in parallel

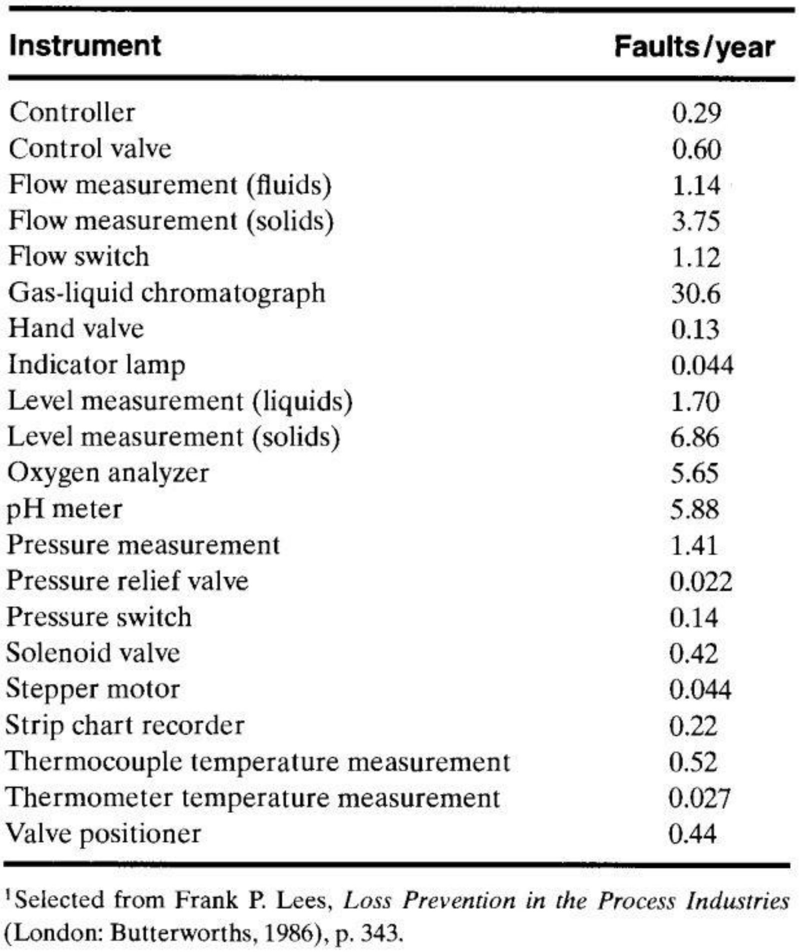
A diagram of the safety systems in a certain chemical reactor is shown in. This reactor contains a high-pressure alarm to alert the operator in the event of dangerous reactor pressures. It consists of a pressure switch within the reactor connected to an alarm light indicator. For additional safety an automatic high-pressure reactor shutdown system is installed. This system is activated at a pressure somewhat higher than the alarm system and consists of a pressure switch connected to a solenoid valve in the reactor feed line. The automatic system stops the flow of reactant in the event of dangerous pressures. (Crowl et al., 2011)

Using the table below, we calculate the reliability and failure probabilities of each component using:

$$R(t) = e^{-\mu t} ,$$

$$P(t) = 1 - R(t) = 1- e^{-\mu t}$$

Table 1: Failure rate Data for Various Selected Process Components



Instrument	Faults/year
Controller	0.29
Control valve	0.60
Flow measurement (fluids)	1.14
Flow measurement (solids)	3.75
Flow switch	1.12
Gas-liquid chromatograph	30.6
Hand valve	0.13
Indicator lamp	0.044
Level measurement (liquids)	1.70
Level measurement (solids)	6.86
Oxygen analyzer	5.65
pH meter	5.88
Pressure measurement	1.41
Pressure relief valve	0.022
Pressure switch	0.14
Solenoid valve	0.42
Stepper motor	0.044
Strip chart recorder	0.22
Thermocouple temperature measurement	0.52
Thermometer temperature measurement	0.027
Valve positioner	0.44

[1] Selected from Frank P. Lees, *Loss Prevention in the Process Industries* (London: Butterworths, 1986), p. 343.

Component	Failure Rate μ *(Faults/yr)*	Reliability $R= e^{-\mu t}$	Failure Probability $P= 1 - R$
Pressure switch 1	0.14	0.87	0.13
Alarm Indicator	0.044	0.96	0.04
Pressure switch 2	0.14	0.87	0.13
Solenoid Valve	0.42	0.66	0.34

From the case study, we identified the top events that could happened from the failure of all the components and come out with the fault tree diagram as shown below;

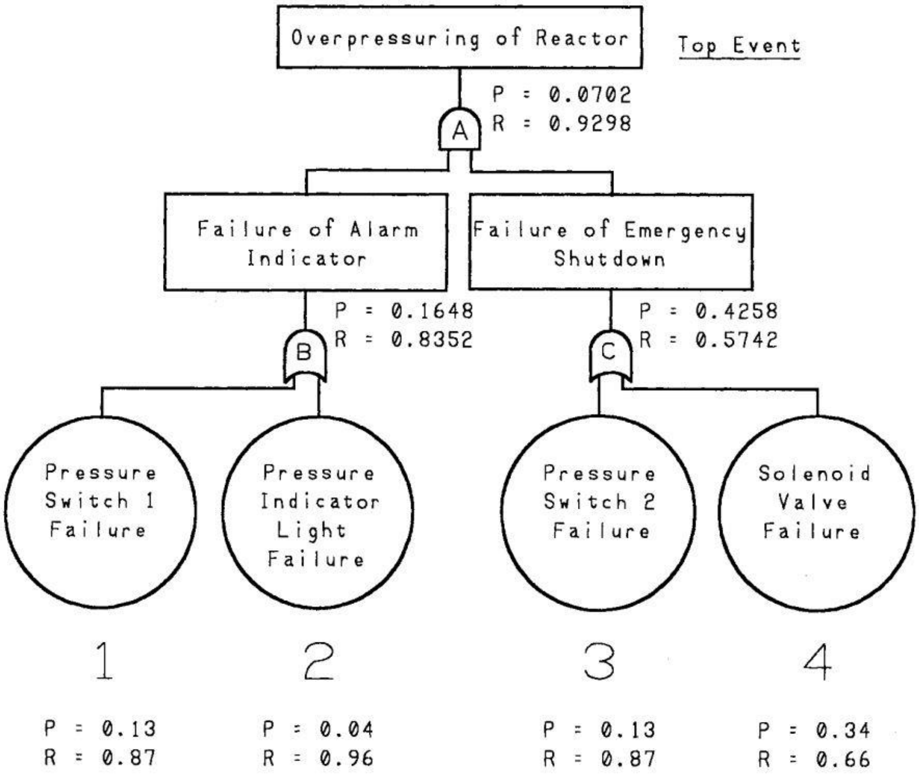

Overpressuring of Reactor
Top Event
P = 0.0702
R = 0.9298
A
Failure of Alarm Indicator
Failure of Emergency Shutdown
P = 0.1648
R = 0.8352
B
P = 0.4258
R = 0.5742
C
Pressure Switch 1 Failure
Pressure Indicator Light Failure
Pressure Switch 2 Failure
Solenoid Valve Failure
1
2
3
4
P = 0.13
R = 0.87
P = 0.04
R = 0.96
P = 0.13
R = 0.87
P = 0.34
R = 0.66

Figure 9: Fault Tree for case study

Next, a quantification of the probability will be calculated. For this case:

P(l AND 3) = (0.13)(0.13) = 0.0169

P(2 AND 3) = (0.04)(0.13) = 0.0052

P(l AND 4) = (0.13)(0.34) = 0.0442

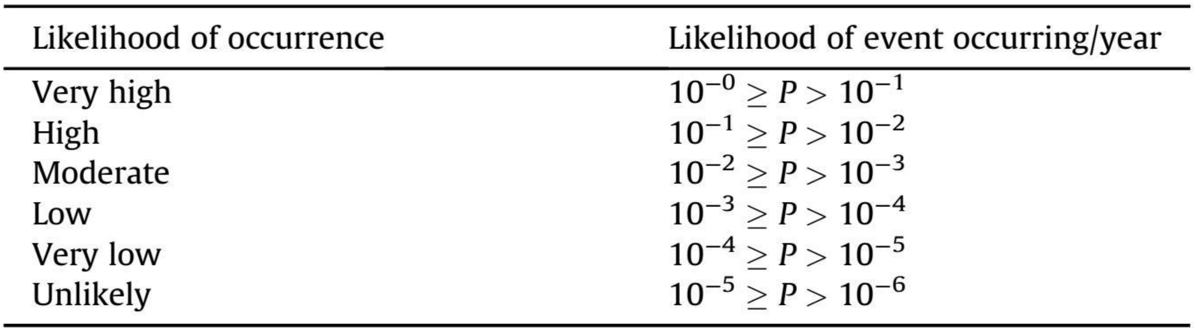
P(2 AND 4) = (0.04)(0.34) = 0.0136

Total = 0.0799

$= 7.99 \times 10^{-2}$

The next step is to compare the likelihood / total probabilities with the likelihood ratings as shown in table below:

Table 2: Likelihood ratings (US Department of Defense, 2000)



Likelihood of occurrence	Likelihood of event occurring/year
Very high	$10^{-0} \geq P > 10^{-1}$
High	$10^{-1} \geq P > 10^{-2}$
Moderate	$10^{-2} \geq P > 10^{-3}$
Low	$10^{-3} \geq P > 10^{-4}$
Very low	$10^{-4} \geq P > 10^{-5}$
Unlikely	$10^{-5} \geq P > 10^{-6}$

Referring to the table, the current likelihood is in the High likelihood of occurence.

Based on the Risk Matrix/ ALARP acceptable likelihood region, (Little, 2007-2009) moderate frequency is tolerable with add-on and safety measure, low frequency is tolerable even without add-on and safety measure while high frequency is intolerable.

From the definition above it is assumed, medium frequency which is $10^{-2} \geq P \geq 10^{-3}$ and by using equation from (Summers, 1998);

$$\textit{Probability to fail on demand} = \frac{\textit{Tolerable risk frequency}}{\textit{Process demand}}$$

Since our scope are only including likelihood of occurrence before the top event, without the consequence included, the equation become;

$$\textit{Risk Reduction Factor} = \frac{\textit{Likelihood of Occurrence}}{\textit{Acceptable Likelihood}}$$

In this case study, taking 10^{-2} as acceptable likelihood in the moderate region,

$$\textit{Risk Reduction Factor} = \frac{7.99 \times 10^{-2}}{1 \times 10^{-2}}$$

$$= 7.99$$

The essence of the calculation is, the closer the likelihood of occurrence to the acceptable likelihood, then no more addition or reducing of IPL is needed where an unnecessary complexity can be avoided. In this case study, it shows that the probability to fail is too far from the acceptable likelihood. Thus, an addition of IPL are needed until the probability is close to 1.

Table 3: Complexity Index

RRF Value	Complexity	Indications
RRF < 1	High	Reduction of IPL are needed
RRF = 1	Recommended	No further adding or reducing IPL needed
RRF > 1	Low	Additional of IPL are needed

4.2 Case Study 2: BP Texas

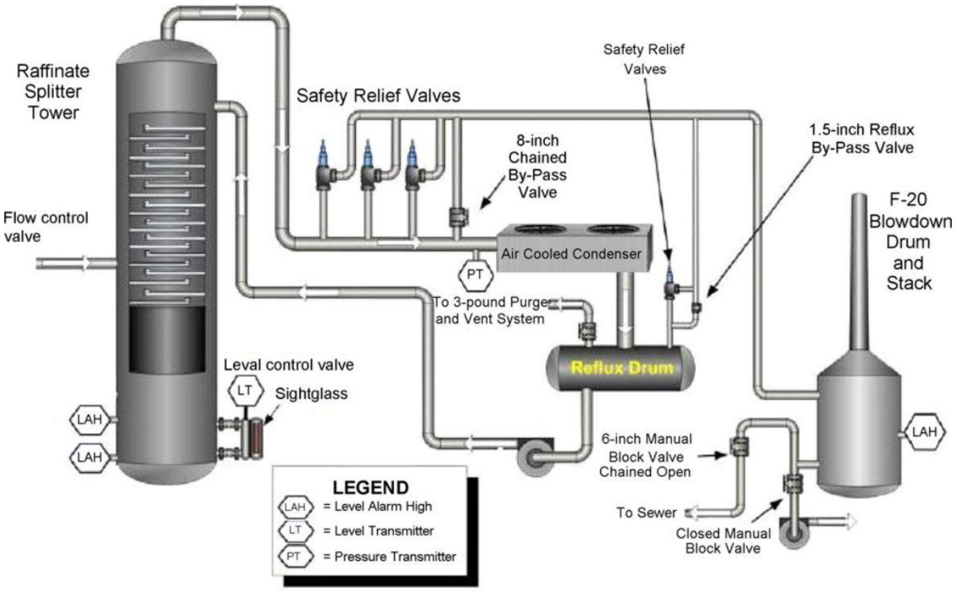


Figure 10: Raffinate Section of ISOM Unit, BP Texas (CSB, 2007)

On March 23, 2005 at 1:20 PM, The accident occurred during the start up of the ISOM unit resulting 15 fatalities, 180 injuries and $1.5 billion financial loss (CSB, 2007). A brief explanation of the accident described below.

On February 21, 2005 the raffinate section of the ISOM unit was shut down and the raffinate splitter tower was drained, gas freed and steamed out. The accident occurred during the start-up of the ISOM unit. During start up on March 23, due to faulty readings from the level transmitter ,the raffinate tower was overfilled. The release of a flammable liquid geyser from the blowdown drum which was not equipped with flare resulting from the Pressure relief devices opened overfilling the blowdown stack. The release of flammables led to an explosion and fire (CSB, 2007).

Table 4: Failure Probabilities of the ISOM unit safety barriers

No	Event description	Failure frequency (per year)	Failure frequency (per hour)
1	Excess feed loading	0.08	9.13E-06
2	Failure of level transmitter	0.01	1.14E-06
3	Failure of High Level Alarm	0.15	1.71E-05
4	Failure of level site glass	0.1	1.14E-05
5	Failure of high-high level alarm	0.15	1.71E-05
6	Failure of heavy raffinate level control valve	0.02	2.28E-06
7	Failure of manual chain valve bypassing the three relief valves	0.2	2.28E-05
8	Failure of first automatic safety valve (set at 40 psig	0.015	1.71E-06
9	Failure of second automatic safety valve (set at 41 psig)	0.015	1.71E-06
10	Failure of third automatic safety valve (set at 42 psig)	0.015	1.71E-06
11	Failure of 1.5 inch reflux bypass valve	0.02	2.28E-06
12	Failure of safety relief valve	0.015	1.71E-06
13	Failure of vent and purge valve	0.02	2.28E-06
14	Failure of 6 inch manual block valve chained open	0.2	2.28E-05
15	Failure of high level alarm	0.15	1.71E-05
16	Failure of level site glass	0.1	1.14E-05
17	Failure of Manual block valve kept closed	0.2	2.28E-05
18	Failure of ESD valve	0.2	2.28E-05

Source: Plant specific data, safety expert feedback. (Kalantarnia et.al, 2010)

From the lists of failure probabilities of the ISOM unit safety barriers, a diagram of fault tree analysis were created using the AND and OR gate as below:

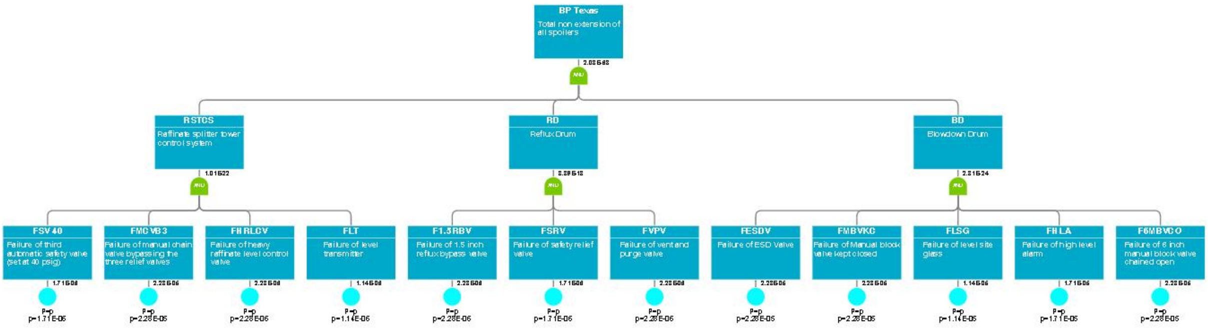
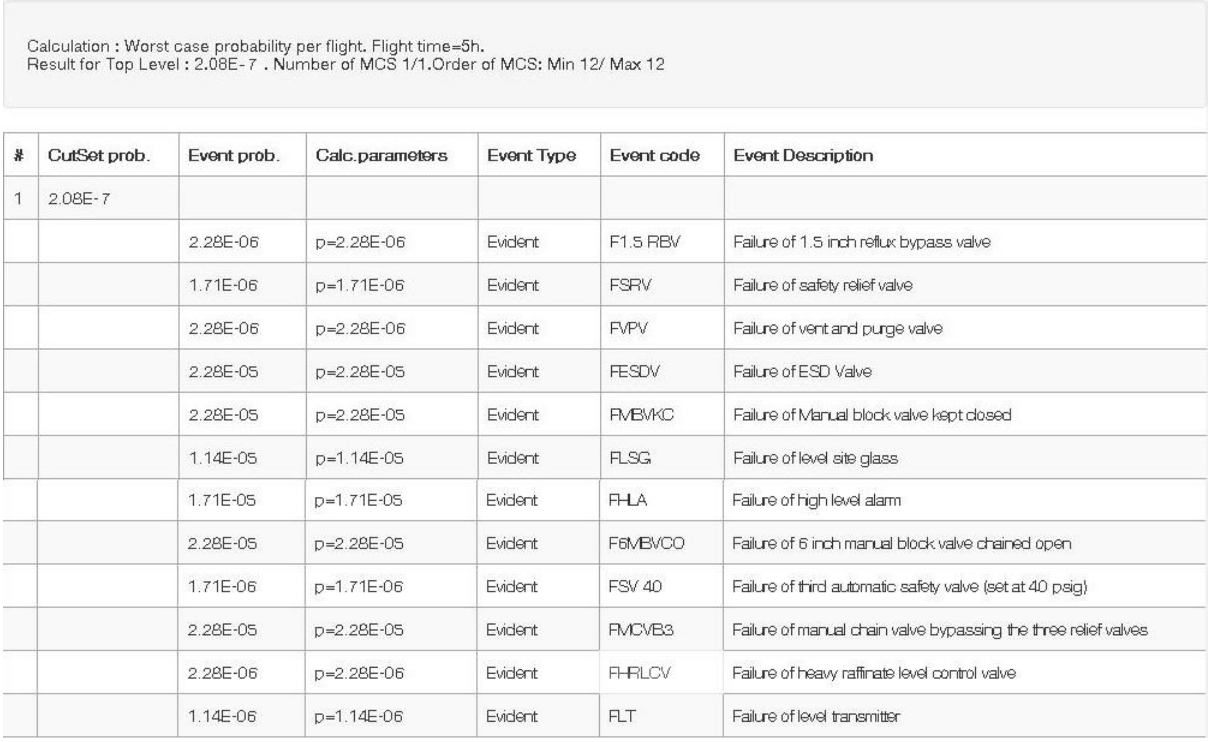

BP Texas
Total non extension of all spoilers
2.08E-63
AND
RSTCS
Raffinate splitter tower control system
1.01E-22
AND
RD
Reflux Drum
8.89E-18
AND
BD
Blowdown Drum
2.31E-24
AND
FSV40
Failure of third automatic safety valve (set at 40 psig)
1.71E-06
P=p
p=1.71E-06
FMCVB3
Failure of manual chain valve bypassing the three relief valves
2.28E-06
P=p
p=2.28E-05
FHRLCV
Failure of heavy raffinate level control valve
2.28E-06
P=p
p=2.28E-06
FLT
Failure of level transmitter
1.14E-06
P=p
p=1.14E-06
F1.5RBV
Failure of 1.5 inch reflux bypass valve
2.28E-06
P=p
p=2.28E-06
FSRV
Failure of safety relief valve
1.71E-06
P=p
p=1.71E-06
FVPV
Failure of vent and purge valve
2.28E-06
P=p
p=2.28E-06
FESDV
Failure of ESD Valve
2.28E-06
P=p
p=2.28E-05
FMBVKC
Failure of Manual block valve kept closed
2.28E-06
P=p
p=2.28E-05
FLSG
Failure of level site glass
1.14E-06
P=p
p=1.14E-05
FHLA
Failure of high level alarm
1.71E-06
P=p
p=1.71E-05
F6MBVCO
Failure of 6 inch manual block valve chained open
2.28E-06
P=p
p=2.28E-05

Figure 11: Fault Tree Analysis of the BP Texas Accident (Using Fault Tree Analysis Software.com)



Calculation : Worst case probability per flight. Flight time=5h.
Result for Top Level : 2.08E-7 . Number of MCS 1/1.Order of MCS: Min 12/ Max 12

#	CutSet prob.	Event prob.	Calc.parameters	Event Type	Event code	Event Description
1	2.08E-7					
		2.28E-06	p=2.28E-06	Evident	F1.5 RBV	Failure of 1.5 inch reflux bypass valve
		1.71E-06	p=1.71E-06	Evident	FSRV	Failure of safety relief valve
		2.28E-06	p=2.28E-06	Evident	FVPV	Failure of vent and purge valve
		2.28E-05	p=2.28E-05	Evident	FESDV	Failure of ESD Valve
		2.28E-05	p=2.28E-05	Evident	FMBVKC	Failure of Manual block valve kept closed
		1.14E-05	p=1.14E-05	Evident	FLSG	Failure of level site glass
		1.71E-05	p=1.71E-05	Evident	FHLA	Failure of high level alarm
		2.28E-05	p=2.28E-05	Evident	F6MBVCO	Failure of 6 inch manual block valve chained open
		1.71E-06	p=1.71E-06	Evident	FSV 40	Failure of third automatic safety valve (set at 40 psig)
		2.28E-05	p=2.28E-05	Evident	FMCVB3	Failure of manual chain valve bypassing the three relief valves
		2.28E-06	p=2.28E-06	Evident	FHRLCV	Failure of heavy raffinate level control valve
		1.14E-06	p=1.14E-06	Evident	FLT	Failure of level transmitter

Figure 12: FTA Calculations from www.fault-tree-analysis-software.com

From the result of the FTA calculation using www. fault-tree-analysis-software.com, it is found that the total frequency result to be: 2.08E-7 . As the basis of the calculation was using per hour, the result need to be multiplied by the number of hours in a year:

$$Final\ Frequency = \ 2.08 \times 10^{-7} \ \times \frac{8760\ hours}{year}$$

$$Final\ Frequency = 1.82 \ \times 10^{-3}$$

$$\textit{Probability to fail on demand} = \frac{\textit{Tolerable risk frequency}}{\textit{Process demand}}$$

Since our scope are only including likelihood of occurrence before the top event, without the consequence included, the equation become;

$$\textit{Risk Reduction Factor} = \frac{\textit{Likelihood of Occurrence}}{\textit{Acceptable Likelihood}}$$

In this case study, taking 10^{-2} as acceptable likelihood in the moderate region,

$$\textit{Risk Reduction Factor} = \frac{1.82 \times 10^{-3}}{1 \text{ x } 10^{-2}}$$

$$= 0.182$$

The essence of the calculation is, the closer the likelihood of occurrence to the acceptable likelihood, then no more addition or reducing of IPL is needed where an unnecessary complexity can be avoided. In this case study, it shows that the probability close to the acceptable likelihood however still less than the preferred index 1. Thus, a reduction of IPL are needed until the probability is close to 1.

CHAPTER 5 :CONCLUSION & RECOMMENDATION

In conclusion, the case study and the literature review shown are both shows the index are working. For the simpler case study of overpressure, it is proven the example is too simple thus additional of IPL so the preferable probability can be achieve. While for the second case study of BP Texas which was known as one of the accident that contributed by the high level of complexity in the instrumentations of the plant. The result and application of the index proven that the case study result shows the high complexity of the plant IPLs.

This index could help personnel and management of plant in some ways for example the installation of IPLs could be limited to only until the requirements acceptable frequency. This in a way will help to reduce the costing of a plant design or any modifications to the plant.

REFERENCES

Abedi, P., & Shahriari, M. (2005). Inherent safety evaluation in process plants – a comparison of methodologies. *Central European Science Journals, 3*(4).

BP Texas City accident report, US Chemical Safety Board,http://www.chemsafety.gov/index.cfm?folder=completedinvestigations &page=info&INV ID=52 (last checked on April 16, 2009).

Crowl, D. A. L., J.F. (2011). Chemical Process Safety Fundamentals with Applications. *Pearson Education, Inc.*

Dowell III, A. M. (1998). Layer of protection analysis for determining safety integrity level. *Elsevier Science Ltd., 37*. doi: http://S0019-0578(98)00018-4

Hoboken, N. J. W. S. (2009). CCPS. (2009) Inherently safer chemical processes: A life cycle approach.

Hendershot, D. C. (2011). Inherently Safer Design An Overview of Key Elements. *Hazardous Chemical*. doi: http://www.asse.org

Hendershot, D. C. (2011). Inherently Safer design-Not Only About Reducing Consequences! *Process Safety Progress, 30*(4). doi: 10.1002/prs

Khan, F. I., & Amyotte, P. R. (2004). Integrated Inherent Safety Index (I2SI): A Tool for Inherentl Safety Evaluation. *Proccess Safety Process, 23*(2). doi: http://10.1002/prs.10015

Khan, F. I., Husain, T., & Abbasi, S. A. (2001). SAFETY WEIGHTED HAZARD INDEX (SWeHI) A New, User-friendly Tool for Swift yet Comprehensive Hazard Identi®cation and Safety Evaluation in Chemical Process Industries. *Institution of Chemical Engineers, 79*(Part B). doi: http://0957± 5820/ 01

Rusli, R., Shariff, A. M., & Khan, F. I. (2013). Evaluating hazard conflicts using inherently safer design concept. *Elsevier Science Ltd.* doi: http://dx.doi.org/10.1016/j.ssci.2012.09.002

Summers, A. E. (1998). Techniques for assigning a target safety integrity level. *Elsevier Science Ltd., 37*. doi: S0019-0578(98)00010-X

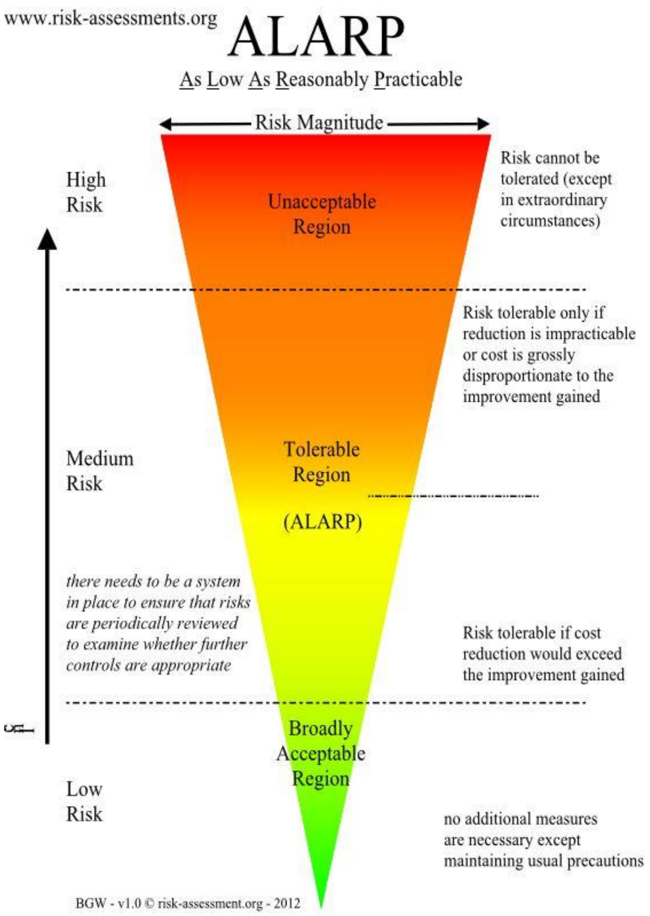
U.S. Chemical Safety and Hazard Investigation Board (CSB), 2007.Investigation Report Refinery Explosion and Fire BP Texas City Refinery, Report No. 2005-04-I-TX, March 2007.

Kalantarnia. M, K. F. (2010). Modelling of BP Texas City refinery accident using dynamic
risk assessment approach. *Elsevier Science Ltd.*, 191-199. doi: 10.1016/j.psep.2010.01.004

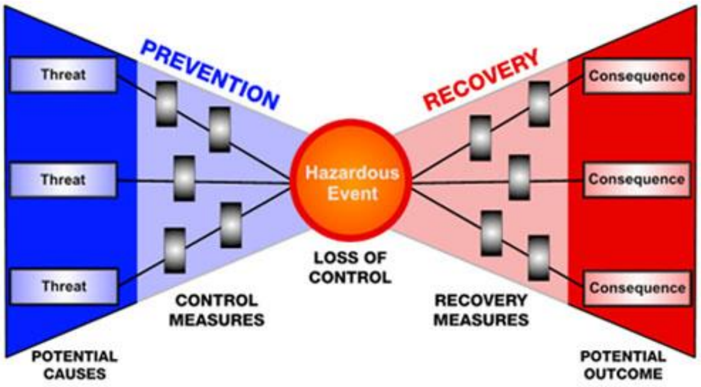
Little, A. D. (2007-2009). Little PSM performance benchmarking study.

APPENDICES

Appendix 1: Risk Matrix / ALARP Region


www.risk-assessments.org
ALARP
As Low As Reasonably Practicable
Risk Magnitude
High Risk
Unacceptable Region
Risk cannot be tolerated (except in extraordinary circumstances)
Risk tolerable only if reduction is impracticable or cost is grossly disproportionate to the improvement gained
Medium Risk
Tolerable Region
(ALARP)
there needs to be a system in place to ensure that risks are periodically reviewed to examine whether further controls are appropriate
Risk tolerable if cost reduction would exceed the improvement gained
Broadly Acceptable Region
Low Risk
no additional measures are necessary except maintaining usual precautions
BGW - v1.0 © risk-assessment.org - 2012

Appendix 2: BOWTIE Diagram on Prevention and Mitigation Barriers


PREVENTION
RECOVERY
Threat
Threat
Threat
Hazardous Event
Consequence
Consequence
Consequence
LOSS OF CONTROL
CONTROL MEASURES
RECOVERY MEASURES
POTENTIAL CAUSES
POTENTIAL OUTCOME