CHAPTER ONE
INTRODUCTION

1.0 BACKGROUND

1.1 Definition

Safety Integrity Level (SIL): is an analysis to establish the target safety level or target risk level and provide guidelines to evaluate the process risk and implement safety systems of the required integrity in order to achieve the established target risk levels

Layer of Protection Analysis (LOPA): is a semiquantitative tool for analyzing and assessing risk. LOPA is an analysis tool that typically builds on the information developed during a qualitative hazard evaluation, such as a process hazard analysis (PHA).SIL and LOPA can be used in process safety and both are widely used in some developed companies.

1.2 History of LOPA

There has been much discussion about the number of and strength of protection layers. This sometimes made using subjective arguments, emotional appeals and persistence of an individual. LOPA answer the key questions using rational, objective, risk-based approach. The individual protection layers provided are analyzed for their effectiveness in LOPA. Then, the combined effects of the protection layers are compared against risk tolerance criteria. The genesis of this method was suggested in two publications:

- In the late 1980s, the Chemical Manufacturers Association published the *Responsible Care® Process Safety Code of Management Practices* which included “sufficient layers of protection” as one of the recommended components of an effective process safety management system (American Chemistry Council, 2000).

- In 1993, CCPS published its *Guidelines for Safe Automation of Chemical Processes.* Although it was called the risk-based SIS integrity level method, LOPA was suggested as one method to determine the integrity level for safety instrumented functions (SIFs). “Interlock” is an older, imprecise term for SIF. The method used was not as fully developed as the LOPA technique described in this book. However, it did indicate a path forward, which was pursued by several companies independently.

The initial development of LOPA was done internally within individual companies, in some cases focusing on existing processes. However, once a method had been developed and refined, several companies published papers describing the driving forces behind their efforts to develop the method, their experience with LOPA, and examples of its use. In particular, the papers and discussion among the attendees at the *CCPS International Conference and Workshop on Risk Analysis in Process Safety* in Atlanta in October 1997 brought agreement that a book describing the LOPA method should be developed. In parallel with these efforts, discussions took place on the requirements for the design of safety instrumented functions (SIF) to provide the required PFDs (probability of failure on demand). United States [ISA S84.01, (ISA, 1996)] and international standards [(IEC 61508, (IEC, 1998)] and [IEC 61511, (IEC, 2001)] described the architecture and design features of SIFs. Informative sections of the ISA and IEC standards suggested methods to determine the required SIL (safety integrity level), but LOPA was not mentioned until the draft of IEC 61511, Part 3 appeared in late 1999. These issues were summarized in the CCPS workshop on the application of ISA S84.01. In response to all this activity, CCPS assembled in 1998 a team from A. D. Little, ARCO Chemical, Dow Chemical, DuPont, Factory Mutual, ABS Consulting (includes former JBF Associates), International Specialty Products, Proctor and Gamble (P&G), Rhodia, Rohm and Haas, Shell (Equilon), and Union Carbide to tabulate and present industry practice for LOPA in this book.

1.3 Problem Statement

Many practical issues need to be addressed in order to arrive at risk based solution. Some of the related issues include identification of target risk levels, identification of the hazardous events associated with the process under consideration, establishing the existing risk associated with the process, and selection of the appropriate non-instrumented safety systems to meet the target risk. Thus, a methodology is required to establish the requirements of the safety instrumented system and the safety integrity levels (SIL). Establishing the target risk levels are based on national and international standards and regulations, corporate policies supported by good engineering practices or input from concerned parties. Losses such as injuries and fatalities to employees or the public, damage to the environment, or financial losses are the terms to express the target risk levels. The target risk levels can be defined for a process, a plant or a corporation.

LOPA can be effectively used at any point in the life cycle of a process or a facility. LOPA is used in research, process development, process design, operations, maintenance, modifications and decommissioning. Those are the important reason why LOPA is needed.

In April 2009, Petronas Penapisan Melaka (Malaysia) Sdn. Bhd (PP(M)SB) planned to establish Layer Of Protection Analysis (LOPA) Procedure and train our own LOPA analysts. Current guideline that PP(M)SB had only general data of Initiating Event Frequency (IEF) and Probability Failure Data (PFD) that are given from CCPS LOPA. Therefore, current IEE and PFD are not related to the company experience (i.e. historical data, operator experience). The general data is not always true especially in case of ‘infant mortality’ and ‘old age’.

1.4 Objectives

The objectives of this project are:

- To determine the Safety Integrity Levels (SIL) for hazardous installation by using Layer of Protection Analysis (LOPA).
- To implement LOPA procedure in the real situation. An industry plant operation will be the case study in this project.

1.5 Scope of the Study

This project will be started with gathering information and theoretical knowledge on Safety Integrity Levels (SIL). The methods that can be used in determining the SIL will be listed out. One of the listed methods will be used as the technique to determine SIL. In this case, Layer of Protection Analysis (LOPA) will be used as the risk assessment technique to determine SIL for hazardous installation. The related information on LOPA will be defined as LOPA will be used to complete this project. This method will be applied in the real application in industry as a real case study. Meanwhile, further research on this project will be continuously practiced as it is important to ensure the effectiveness of this project.

CHAPTER TWO
LITERATURE REVIEW

LOPA is a simplified form of risk assessment. LOPA typically uses order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layers (IPLs) to approximate the risk of a scenario. LOPA is an analysis tool that typically builds on the information developed during a qualitative hazard evaluation, such as a process hazard analysis (PHA). LOPA is implemented using a set of rules.

2.1 Selecting Safety Integrity Levels

2.1.1 Introduction

The purpose of a safety instrumented system (SIS) is to reduce the risk that a process may become hazardous to a tolerable level. The SIS does this by decreasing the frequency of unwanted accidents. The amount of risk reduction that an SIS can provide is represented by its *safety integrity level* (SIL), which is defined as a range of probability of failure on demand. The method organizations use to select SILs should be based:

- Their risk of accident
- An evaluation of the potential consequences and likelihoods of an accident
- An evaluation of the effectiveness of all relevant process safeguards

Selecting an SIL, should involve considering relevant laws, regulations, and national and international standards.

2.1.2 Safety Integrity Level

SILs are categories based on the probability of failure on demand (PFD) for a particular safety instrumented function. The SIL is the key design parameter specifying the amount of risk reduction that the safety equipment is required to achieve for a particular function in question. If an SIL is not selected, the equipment cannot be properly designed because only the action is specified, not integrity. To properly design a piece of equipment, two types of specifications are required:

- A specification of what the equipment does
- A specification of how well the equipment performs that function.

The SIL addresses this second specification by indicating the minimum probability that the equipment will successfully do what it is designed to do when it is called upon to do it. Selecting SIL involves giving a numerical target upon which subsequent steps in the safety life cycle based. Thus SIL selection offers an important guide when you are selecting equipment and making maintenance decisions.

2.1.3 SIL Selection and Risk

The reason of an organization should use a systematic methodology, which includes layer of protection analysis (LOPA), to select SIL is to make the choice that best reduces risk. To make the best decision about SIL, designer needs to completely understand not only the potential likelihood of an unwanted event, but also the possible consequences of that event. Once the risk is known, one must determine hoe to reduce that risk to a tolerable risk. The amount of risk that an organization is willing to tolerate will determine the amount of risk reduction is needed.

2.2 Purpose of LOPA

The primary purpose of LOPA is to determine the sufficient layers of protection against an accident scenario. The layers of protection of a scenario depend on the process complexity and potential severity of the consequences.

2.3 Overview of LOPA

LOPA is a simplified form of risk assessment. LOPA typically uses order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layers (IPLs) to approximate the risk of a scenario. LOPA is an analysis tool that typically builds on the information developed during a qualitative hazard evaluation, such as a process hazard analysis (PHA). LOPA is implemented using a set of rules.

The primary purpose of LOPA is to determine if there are sufficient layers of protection against an accident scenario. A scenario may require one or many protection layers depending on the process complexity and potential severity of a consequence. Only one layer must work successfully for the consequence to be prevented. However, since no layer is perfectly effective, sufficient protection layers must be provided to render the risk of the accident tolerable.

LOPA provides a consistent basis for judging whether there are sufficient IPLs to control the risk of an accident for a given scenario. If the estimated risk of a scenario is not acceptable, additional IPLs may be added. Alternatives encompassing inherently safer design can be evaluated as well. LOPA does not suggest which IPLs to add or which design to choose, but it assists in judging between alternatives for risk mitigation. LOPA is not a fully quantitative risk assessment approach, but is rather a simplified method for assessing the value of protection layers for a well-defined accident scenario.

LOPA provides a risk analyst with a method to reproducibly evaluate the risk of selected accident scenarios. A scenario is typically identified during a qualitative hazard evaluation (HE). LOPA is applied after an unacceptable consequence, and a credible cause for it, is selected. It then provides an order of magnitude approximation of the risk of a scenario. In many applications of LOPA, the goal of the analyst is to identify all cause–consequence pairs that can exceed the organization's tolerance for risk.

2.4 When to use LOPA

LOPA is typically applied after a qualitative hazard evaluation using the scenarios identified by the qualitative hazard review team. However, LOPA can also be used to analyze scenarios that originate from any source, including design option analysis and incident investigations. LOPA can also be applied when a hazard evaluation team:

- Believes a scenario is too complex for the team to make a reasonable risk judgment using purely qualitative judgment, or
- The consequences are too severe to rely solely on qualitative risk judgment.

LOPA can also be used as a screening tool prior to a more rigorous quantitative risk assessment method. When used as a screening tool, each scenario above a specified consequence or risk level will first go through LOPA analysis, and then certain scenarios will be targeted for a higher level of risk assessment. The decision to proceed to CPQRA is typically based on the risk level determined by LOPA or based on the opinion of the LOPA analyst.

2.5 Implementing LOPA

LOPA is most effective when an organization adopts a consistent approach to LOPA and sets criteria for when to use LOPA and who is qualified to use it. LOPA can be applied in a team setting to identify accident scenarios. LOPA can also be applied by a single analyst; in this case, the scenarios have typically already been identified for the analyst.

2.6 Benefits of LOPA

LOPA has many benefits that justify investment by company management and risk analysts. As with most new tools, however, the benefits often cannot be fully appreciated until LOPA is applied to everyday problems. Some general benefits of LOPA include:

- LOPA requires less time than quantitative risk analysis. This benefit applies particularly to scenarios that are too complex for qualitative assessment of risk.
- LOPA helps resolve conflicts in decision making by providing a consistent, simplified framework for estimating the risk of a scenario and provides a common language for discussing risk. LOPA provides a better risk decision basis compared to subjective or emotional arguments based on “the risk is tolerable to me.” This is particularly beneficial for organizations making the transition from qualitative to more quantitative risk methods.
- LOPA can improve the efficiency of hazard evaluation meetings by providing a tool to help reach risk judgments quicker.

- LOPA facilitates the determination of more precise cause–consequence pairs, and therefore improves scenario identification.
- It is more accurate than purely qualitative estimates.
- Its tools and data are commercially available and inexpensive

CHAPTER THREE
METHODOLOGY

LOPA includes the method that falls between qualitative and quantitative methods. There are several steps involve in developing this analysis. Below is the summarization of the steps or methodologies that to be used in for the whole project:

- Step 1: Identify the consequences to screen the scenarios
- Step 2: Select an accident scenarios
- Step 3: Identify the initiating event of the scenario and determine the initiating event frequency (events per year)
- Step 4: Identify the IPLs and estimate the probability of failure on demand of each IPL.
- Step 5: Estimate the risk of the scenarios by mathematically combining the consequences, initiating event, and IPL data

The above description of the methodologies will lead in determining the SIL for hazardous installation. Below is the summary of the methodologies to be used in implementing LOPA.

STEP 1: ESTIMATING CONSEQUENCES AND SEVERITY

In LOPA, the consequences are estimated to an order of magnitude of severity. There various types of consequence analysis used in LOPA. Consequences are the undesirable outcomes of accident scenarios. Consequence evaluation is an integral part of any risk assessment methodology. The risk associated with the accident scenarios, and the risk assessment methodology adopted by the organization, and the resources the organization is willing to expend to refine the estimate are the factors of what consequences should be evaluated and how rigorously the consequences are evaluated. The different types of consequence evaluation are:

- Release size/characterization
- Simplified injury/fatality estimates
- Simplified injury/fatality estimates with adjustments
- Detailed injury/fatality estimates

The method used for consequence categorization:

Method 1: Category Approach without Direct Reference to Human Harm

This method typically uses matrices to differentiate consequences into various categories. It avoids estimating the number of potential injuries or fatalities, thereby:

- Avoiding any overt appearance that injuries and fatalities are tolerable
- Helping the team make more accurate judgments about relative risk, since it is very difficult to estimate qualitatively the number of people who might be harmed and how severe the harm might be. A toxic release can result in one or more fatalities or no harm at all, depending on the proximity of people to the release point and the time and capability they have to escape.

The advantages of this method:

- The method is simple and easy to use because the size and properties of the release are relatively easy to assess. No case-by-case modeling is required. A release of a certain size is assigned a certain consequence value independent of the eventual effect (fire, explosion, toxic release, injury, fatality, etc.). The criteria for loss of production are similarly simple to assess.
- When combined with a matrix showing the organization’s risk tolerance criteria, the method allows visual assessment of where a given risk lies in relation to the organization’s guidelines.

Method 2: Qualitative Estimates with Human Harm

This method uses the final impact to humans as the consequence of interest, but arrives at the value using purely qualitative judgment. For each scenario, the human consequences are estimated directly by the LOPA analyst, using past experience, previously generated look-up tables, or knowledge of prior detailed release modeling of similar releases.

The advantages of this method are:

- ***Simplicity of understanding*****:** Many people tend to better understand consequence in terms of harm rather than expressing risk in terms of release size.
- ***Direct comparison with corporate guidelines*****:** Many companies already have established guidelines for risk of a fatality/injury, or for risk of a certain monetary loss.

The disadvantages of this method are:

- Implicit assumptions for the probability of ignition for flammable releases, for the probability of injury, and the probability that a person is present in the area may over- or underestimate the risk of fatality.
- Look-up tables are even less precise (more subjective) than release categorization tables.
- The estimation of the consequence severity may vary between different analysts, unless some guidance is provided across the company.

Method 3: Qualitative Estimates with Human Harm with Adjustments for Post Release Probabilities

Alternatively, the LOPA analyst can initially estimate the magnitude of a release "qualitatively" similar to Method 2 and then later adjust the event frequency by the probability that:

- The event will result in a flammable or toxic cloud;
- For a flammable cloud, an ignition source will be present;
- An individual will be present in the area when the event occurs;
- The individual will experience a fatal (or injurious) consequence.

The advantages of this method:

- ***Simplicity of understanding*:** People tend to better understand consequence in terms of harm rather than expressing risk in terms of release size.
- ***Direct comparison with corporate guidelines*:** Many companies already have established guidelines for risk of a fatality or injury.
- ***Frequency adjustments*:** The frequency adjustments may give a better estimate of the risk of human harm.

The disadvantages of this method:

- The simplifications made in assessing the probabilities of the events subsequent to the release. The results of real-world events have proven to be both significantly less and significantly greater than those calculated by analysts. However, if consistent approaches are used, it is reasonable to expect that this method will highlight scenarios with relatively higher risk.
- Extra parameters for the probability of reaching the stated impact or outcome must be included in the risk calculation and these may change over time (e.g., the number of people or their location changes).
- The estimation of the consequence severity may vary between different analysts, unless some guidance is provided across the company.
- This method would need to be augmented to address business impact or economic risk.

Method 4: Quantitative Estimates with Human Harm

This method is similar to the qualitative estimates with human harm method (Method 3), but uses detailed analyses in determining the effects of a release and its effects upon individuals and equipment. This method involves the use of mathematical models to simulate the release itself (also called "source term" modeling), the subsequent dispersion, and the toxic or blast/thermal effect. The advantages of this method:

- A greater degree of certainty concerning the predicted consequences.
- Direct comparison with corporate guidelines.

The disadvantages of this method:

- Although the modeling programs are much more sophisticated than the estimation methods, the results of real-world events have been both significantly less and significantly greater than those calculated by analysts. Modeling results are strongly affected by the exact release conditions, atmospheric stability, wind direction, time to ignition, etc. There are thousands of possible permutations to consider. Inevitably only a few "representative" cases can be chosen.
- The level of sophistication required for modeling the consequence of a scenario is disproportionate to that used to estimate the order of magnitude frequency of the scenario with LOPA.
- The training, experience and effort required to perform the modeling can be prohibitive, and such analysis is usually only applied to scenarios that have already been judged to have potentially fatal results.

STEP 2: DEVELOPING SCENARIOS

A scenario is an unplanned event or sequence of events that results in an undesirable consequence. Each scenario consists of at least two elements:

- An initiating event that starts the chain of events and
- A consequence that results if the chain of events continues without interruption.

Each scenario must have a unique initiating event/consequence pair. If the same initiating event can result in different consequences, additional scenarios should be developed. In some cases many scenarios may spring from a common initiating event and separate scenarios should be developed for individual sections of the plant. In addition to the initiating event and consequence, a scenario may also include

- Enabling events or conditions that have to occur or be present before the initiating event can result in a consequence
- The failure of safeguards (which may be IPLs)

Methods that use consequence end-points of fatalities, or harm to business or the environment, may also include some or all of the following factors, or outcome modifiers, in the scenario:

- The probability of ignition of a flammable material (liquid or vapor release)
- The probability of a person being present in the area affected by the event,
- The probability that a fatal injury will result from exposure to the effects of the fire, explosion, or toxic release—includes evacuation or protective action
- The probability that an estimated financial loss to the facility of a certain magnitude will result.

The most common source of information for identifying scenarios is hazard evaluations (HE) developed and documented for existing processes and performed during the design of new and modified processes. The purpose of an HE is to identify, assess and document the hazards associated with the process. Other sources for identifying candidate scenarios for LOPA are:

- Issues related to plant operation. This could involve unexpected behavior, or operating conditions outside normal ranges, etc.
- Incidents in the process, or from other processes, which reveal an initiating event or scenario not previously considered or which was not considered credible

- The requirement to change the process, which could involve new or modified scenarios
- Interlock reviews to assess whether the safety instrumented function (SIF)—interlock—is required and, if so, the type of SIF required meeting the corporate risk guidelines.

Once a scenario has been identified, it must be developed and documented to the level where a basic understanding of the events and safeguards is achieved. The scenario may not be initially understood completely and may undergo revisions. New scenarios may also be revealed that must be analyzed separately. Once the initiating event is identified for a specific scenario, the analyst must determine whether any enabling events or conditions are required for the initiating event to lead to the consequence. The next step is to confirm that the consequence is stated using the same criteria as the LOPA method.

STEP 3: IDENTIFYING INITIATING EVENT FREQUENCY

For LOPA, each scenario has a single initiating event. The frequency of the initiating event is normally expressed in events per year. Some sources use other units, such as events per 10^6 hours. Initiating events are grouped into three general types: external events, equipment failures, and human failures. Prior to assigning frequencies to initiating events, all causes from the scenario development step should be reviewed and verified as valid initiating events for the consequence identified. Any causes that are incorrect or inappropriate should be either discarded or developed into valid initiating events. Frequency estimation also involves in this stage. This frequency estimation measures the failure rate data which consists of sources, selection of failure rates, failure rates in LOPA, derivation of initiating event frequency from failure data, time at risk, adjustment of frequency rates and high demand mode.

STEP 4: IDENTIFYING INDEPENDENT PROTECTION LAYERS

An IPL is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario. In order to be considered an IPL, a device, system, or action must be

- **Effective** in preventing the consequence when it functions as designed,
- **Independent** of the initiating event and the components of any other IPL already claimed for the same scenario
- **Auditable;** the assumed effectiveness in terms of consequence prevention and PFD must be capable of validation in some manner

The basic requirements of effectiveness, independence and audit ability for an IPL are determined by several methods. The simplest is to use a written design basis, or IPL summary sheet, which must be available for review by the LOPA team or analyst.

STEP 5: DETERMINING SCENARIO FREQUENCY

The following is the general procedure for calculating the frequency for a release scenario with a specific consequence endpoint.

$$f_i^C = f_i^{\mathrm{I}} \mathrm{\ x\ } \prod_{j=1}^{j} \mathrm{PFD}_{\mathrm{ij}}$$

$$= f_i^{\mathrm{I}} \mathrm{\ x\ } \mathrm{PFD}_{\mathrm{i1}} \mathrm{\ x\ } \mathrm{PFD}_{\mathrm{i2}} \mathrm{\ x\ } \ldots \mathrm{PFD}_{\mathrm{ij}}$$

Where

f_i^C is the frequency for consequence *C* for initiating event *i*

f_i^{I} is the initiating event frequency for initiating event *i*

PFD_{ij} is the probability of failure on demand of the *j*th IPL that protects against consequence *C* for initiating event *i*.

The above equation is applicable for low demand situations—that is, f_i^{I} is less than twice the test frequency for the first IPL.

STEP 6: MAKING RISK DECISIONS

Three basic types of risk judgment are used in conjunction with LOPA:

- The predominant method is to **compare the calculated risk** with predetermined risk tolerance criteria through use of various methods.
- The second type is **expert judgment** by a qualified risk analyst, which as noted above, is not recommended by the authors but is included for completeness.
- The third type is **relative comparison among competing alternatives** for risk reduction, using either of the methods described above.

Cost–benefit analysis is often also used to compare the value of competing options. This technique supplements the basic risk judgment approaches. For the comparison calculated risk to scenario risk tolerance criteria type of risk decision making, the calculated risk from is compared to a risk criteria that relates to some measure of maximum risk per scenario that the company will tolerate. Types of methods to be used:

- **Matrix Method:** Risk matrices are a generalized method of visually showing the frequency tolerable for a scenario based on the consequence severity (Chapter 3) and the scenario frequency
- **Numerical Criteria Method (Maximum Tolerable Risk per Scenario):** Develop risk criteria based on a maximum tolerable risk per scenario, based on a variety of consequence categories
- **Number of IPL Credits:** Embedded the tolerable risk criteria in tables which specify the number of IPL credits for scenarios of certain consequence levels and frequency.

CHAPTER FOUR
RESULTS AND DISCUSSION

In this stage, student has managed to complete her project until determination of scenario frequencies and making risk decision. Completing this stage includes:

- Step 1: Estimating Consequences and Severity
- Step 2: Developing Scenarios
- Step 3: Identifying Initiating Event Frequency
- Step 4: Identifying Related IPLs
- Step 5: Determining Scenario Frequency
- Step 6: Making Risk Decision. Determine SIL

Student has estimated the undesirable outcomes of accident scenarios. Then, student has developed the scenarios or sequence of events that results in an undesirable outcomes. Each scenario consists of two elements which are the initiating event that starts the chain of events and a consequence that results if the chain of events continues without interruption.

After developing the scenarios, student identified initiating event frequency and related Independent Protection Layers (IPLs). There are 26 initiating events that have been listed in order to proceed with LOPA, refer to Table 4.1. The data for IPLs PFD also has been collected. There are passive IPLs and active IPLs, refer to the table 4.2 and 4.3 below.

No	Initating Causes	Likelihood of Failure (/yr)
1	BPCS Instrument Loop Failure	1 x 10^{-1}
2	Regulator Failure	1 x 10^{-1}
3	Fixed Equipment Failure	1 x 10^{-2}
4	Pumps & other Rotating Equipments	1 x 10^{-1}
5	Cooling Water Failure	1 x 10^{-1}
6	Loss of Power	1 x 10^{-1}
7	Human Error (Routine task, 1 per day opportunity)	1 x 10^{-1}
8	Human Error(Routine Task, Once-per-month opportunity)	1 x 10^{-2}
9	Human Error ((Non-Routine Task, Low Stress)	1 x 10^{-1}
10	Human Error (Non-Routine Task, High Stress)	1 x 10^{-0}
11	Pressure Vessel Residual Failure	1 x 10^{-6}
12	Piping Residual Failure-100m-Ful Breach	1 x 10^{-5}
13	Piping Leak (10% section)-100m	1 x 10^{-3}
14	Atmosphere Tank Failure	1 x 10^{-3}
15	Gasket/Packing Blowout	1 x 10^{-2}
16	Turbine/Diesel Engine Over speed w/casing Breach	1 x 10^{-4}
17	3rd Party Intervention	1 x 10^{-2}
18	Lightning Strike	1 x 10^{-3}
19	Safety Valve Opens Spuriously	1 x 10^{-2}
20	Pump Seal Failure	1 x 10^{-1}
21	Unloading/Loading Hose Failure	1 x 10^{-1}
22	Small External Fire (aggregate causes)	1 x 10^{-1}
23	Large External Fire (aggregate causes)	1 x 10^{-2}
24	LOTO Procedure *Failure (*overall failure of a multiple-element process	1 x 10^{-3} per opportunity
25	Operator Failure (Routine procedure, well-trained, unstressed, not fatigued)	1 x 10^{-2} per opportunity

Table 4.0.1

Passive IPLs

IPL	**Comments** *Assuming an adequate design basis and adequate inspection and maintenance procedures*	**PFD from literature and industry**	**PFD used in this book** *for screening*
Dike	Will reduce frequency of large consequences (widespread spill) of a tank overspill/rupture/spill etc	1×10^{-2} - 1×10^{-3}	1×10^{-2}
Underground Drainage System	Will reduce frequency of large consequences (widespread spill) of a tank overspill/rupture/spill etc	1×10^{-2} - 1×10^{-3}	1×10^{-2}
Opent Vent (No Valve)	Will prevent overpressure	1×10^{-2} - 1×10^{-3}	1×10^{-2}
Fireproofing	Will reduce rate of heat input and provide additional time for depressurizing/firefighting etc	1×10^{-2} - 1×10^{-3}	1×10^{-2}
Blast-wall/Bunker	Will reduce frequency of large consequences of an explosion by confining blast and protecting equipment/buildings etc	1×10^{-2} - 1×10^{-3}	1×10^{-3}
"Inherently Safe Design"	If properly implemented can significantly reduce the frequency of consequences associated with a scenario. NOTE: The LOPA rule for some companies allow inherently safe design features to eliminate certain scenarios (e.g, vessel design pressure exceeds all possible high pressure challenges)	1×10^{-1} - 1×10^{-6}	1×10^{-2}
Flame/Detonation Arrestor	If properly designed, installed and maintained these should eliminate the potential for flashback through a piping system or into a vessel or tank	1×10^{-1} - 1×10^{-3}	1×10^{-2}

Table 4.0.2

Active IPLs

IPL	**Comments** *Assuming an adequate design basis and adequate inspection and maintenance procedures*	**PFD from literature and industry**	**PFD used in this book** *for screening*
Relief Valve	Prevent system exceeding specified overpressure. Effectiveness of this device is sensitive to service and experience	$1 \times 10^{-1} - 1 \times 10^{-5}$	1×10^{-2}
Rupture Disc	Prevent system exceeding specified overpressure. Effectiveness of this device is sensitive to service and experience	$1 \times 10^{-1} - 1 \times 10^{-5}$	1×10^{-2}
Basic Process Control System	Can be credited as an IPL if not associated with the initiating events being considered	$1 \times 10^{-1} - 1 \times 10^{-2}$ ($>1 \times 10^{-1}$ allowed by IEC)	1×10^{-1}
Safety Instrumented Function (Interlocks)	See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for lufe cycle requirements and additional discussion		
SIL 1	Typically consists of: Single sensor (redundant for fault tolerant) Single logic processor (redundant for fault tolerant) Single final element (redundant for fault tolerant)	$\geq 1 \times 10^{-2} - < 1 \times 10^{-1}$	This book does not specify a specific SIL level. Continuing examples calculate a required PFD for o SIF
SIL 2	Typically consists of: "Multiple" sensor (for fault tolerant) "Multiple" channel logic processor (for fault tolerant) "Multiple" final element (for fault tolerant)	$\geq 1 \times 10^{-3} - < 1 \times 10^{-2}$	
SIL 3	Typically consists of: Multiple sensor Multiple channel logic processor Multiple final element	$\geq 1 \times 10^{-4} - < 1 \times 10^{-3}$	

Table 4.0.3

4.1 Event Tree Analysis

After gathering all data and information, the scenario frequency could be determined. In this case, student used Event Tree Analysis method to develop the scenarios of each initiating events. These are the developed event tree for several initiating events:

BPCS Instrument Loop Failure (0.1)

Safety Function (IPL)	Inherently Safe Design	Operator Response	SIF	Dike
Identifier	B	C	D	E
PFD	0.01	0.1	0.01	0.01

Table 4.1.1

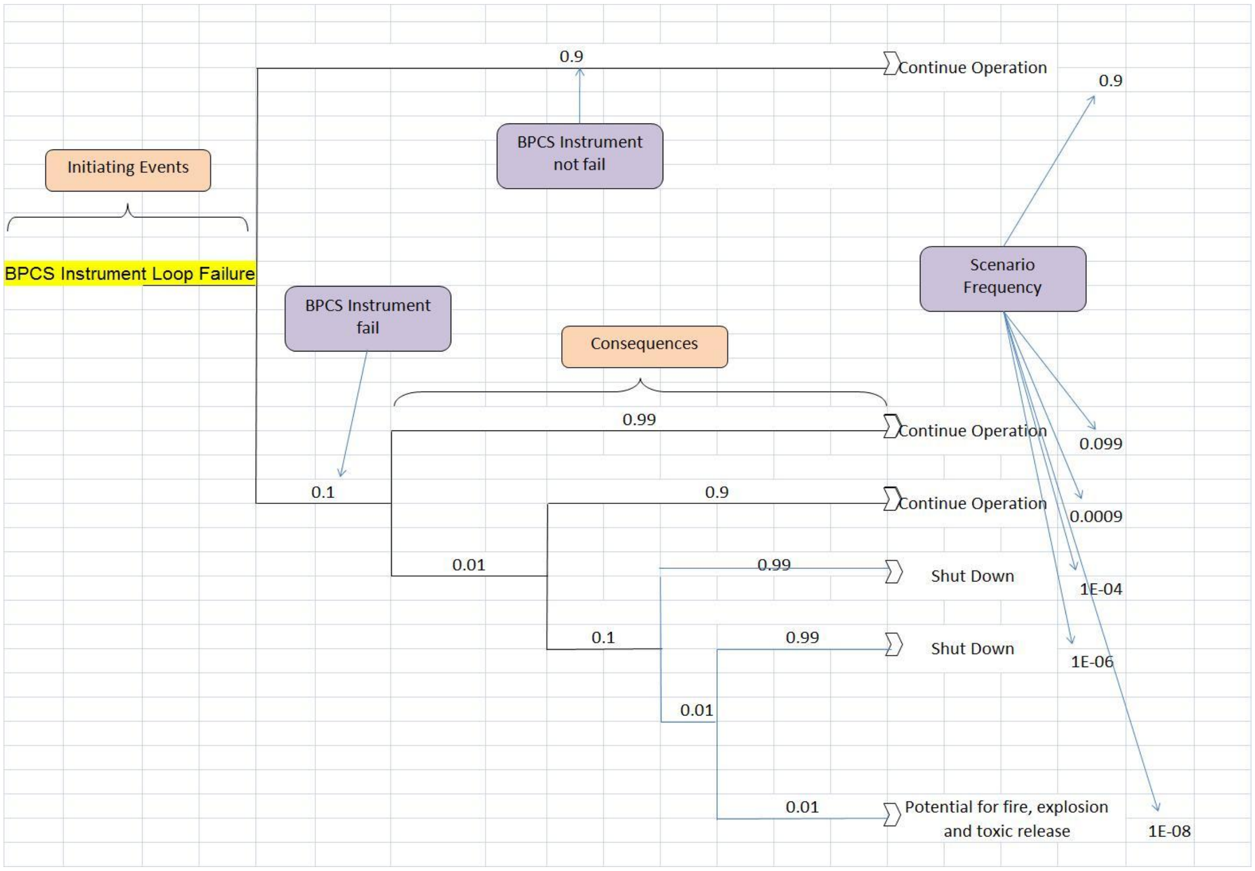


Figure 4.1.1

From Figure 4.1, the initiating cause is Basic Process Control Systems (BPCS). BPCS is designed to maintain the process in the safe region. Failure of BPCS will cause trouble to the plant itself. There are four Independent Protection Layers (IPLs) to prevent the undesirable outcomes to occur in this system. First protection layer is inherently safe design. Safe design, if properly implemented can significantly reduce the frequency of consequences associated with a scenario. Generally, all equipments in a plant are safely designed. Here, the frequency of the failure of safer design is 0.01. So, 0.09 is the frequency if the design is not properly safe. Operator response and alarm could be the second protection layer if the safer design is not properly functioned. The frequency for operator response failure is 0.1. Then, Safety Instrumented Function (SIF) should be third protection layer after operator response where it will function if the operator response is failed. SIFs are state control functions, sometimes called interlocks and safety critical alarms. Each of the SIFs will have its own PFD value based on:

- The number and type of sensors, logic solvers and final control elements
- The time interval between periodic functional tests of system components

The failure frequency of this SIF is 0.01. The last layer is dike where dike will reduce the frequency of large consequences. The failure of dike function could lead to the potential undesirable outcomes. From the event tree above, potential fire, explosion and toxic release could happen if all of the IPLs are not functioned. The frequency of this scenario is 0.00000001.

Pressure Vessel Residual Failure (0.000001)

Safety Function:	Inherently Safe Design	Critical Alarms & Human Intervention	Safety Instrumented Function (SIF)	Relief Valve
Identifier	B	C	D	E
PFD	0.01	0.1	0.01	0.01

Table 4.1.2

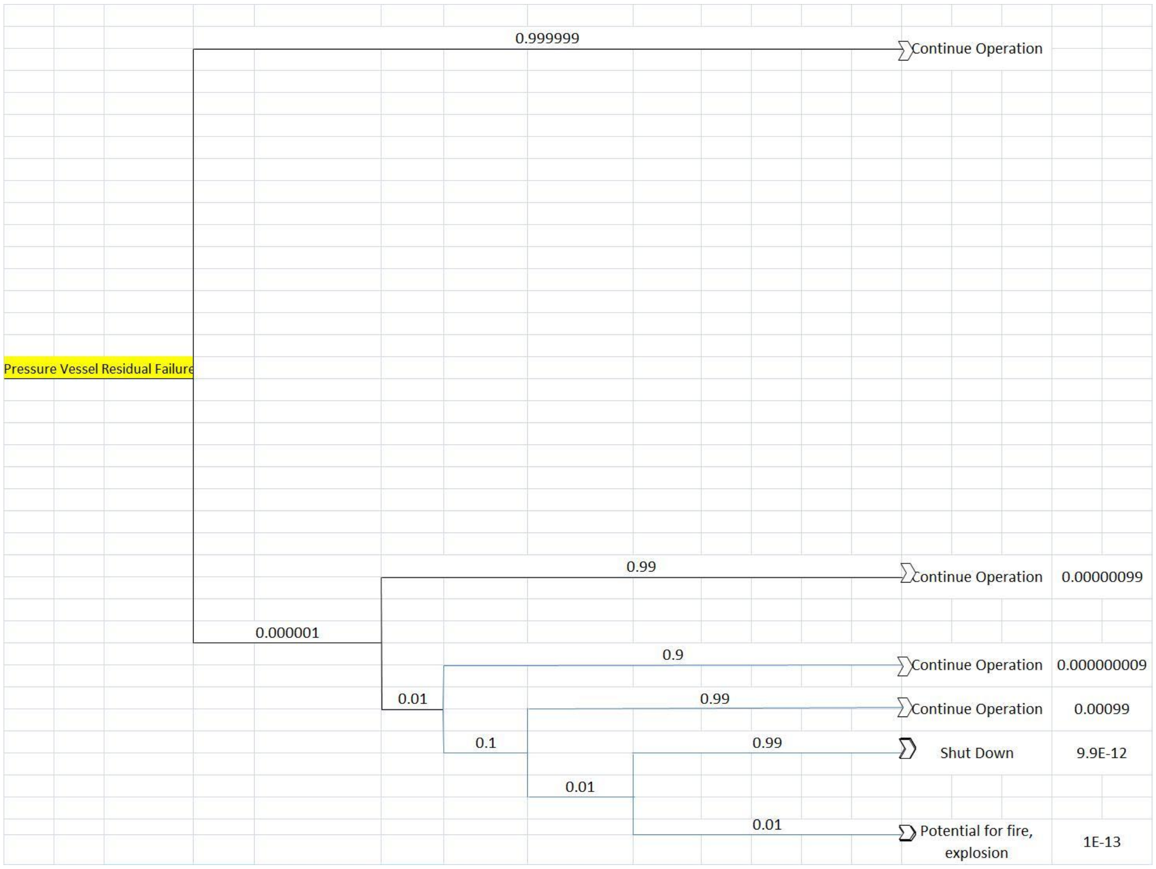


Figure 4.1.2

Above shows the scenario resulting from pressure vessel residual failure initiating cause. The failure frequency of this initiating event is 0.000001. There are four Independent Protection Layers (IPLs) to prevent the undesirable outcomes to occur in this system. First protection layer is inherently safe design. As mentioned before, safe design, if properly implemented can significantly reduce the frequency of consequences associated with a scenario. In this case, the frequency of the failure of safer design is 0.01. Critical alarm and human intervention will be the second protection layer if the safer design is not properly functioned. The frequency for critical alarm and human intervention failure is 0.1. Then, Safety Instrumented Function (SIF) will be third protection layer after operator response where it will function if the operator response is failed. The failure frequency of this SIF here is 0.01. The last layer is relief valve where relief valve prevent system exceeding specified overpressure. Effectiveness of this device is sensitive to service and experience. Relief valve fail to function could lead to the potential undesirable outcomes. From the event tree above, potential fire, explosion and toxic release could happen if all of the IPLs are not functioned. The frequency of this scenario is 1E-13.

Pump Seal Failure (0.1)

Safety Function:	Inherently Safe Design	Operator Response
Identifier	B	C
PFD	0.01	0.1

Table 4.1.3

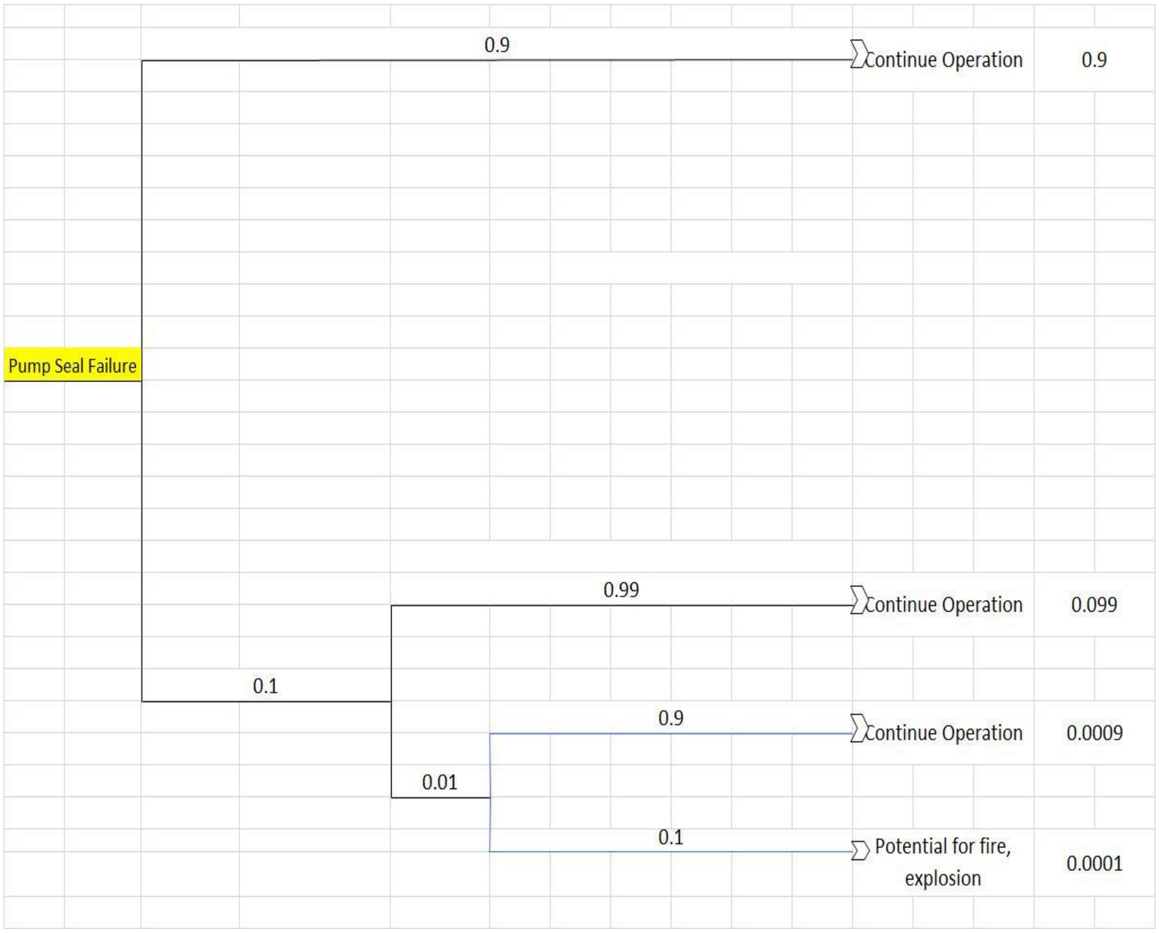


Figure 4.1.3

Above shows the scenario resulting from pump seal failure initiating cause. The failure frequency of this initiating event is 0.1. Two Independent Protection Layers (IPLs) involve in this system. First protection layer is inherently safe design. The frequency of the failure of safer design is 0.01. Operator response will be the second protection layer if the safer design is not properly functioned. The frequency for operator response failure is 0.1. From the event tree above, potential fire, explosion and toxic release could happen if all of the IPLs are not functioned. The frequency of this scenario is 0.0001.

Small External Fire (0.1)

Safety Function:	Inherently Safe Design	Operator Response	Pressure Relief Valve	Dike
Identifier	B	C	D	E
PFD	0.01	0.1	0.01	0.01

Table 4.1.4

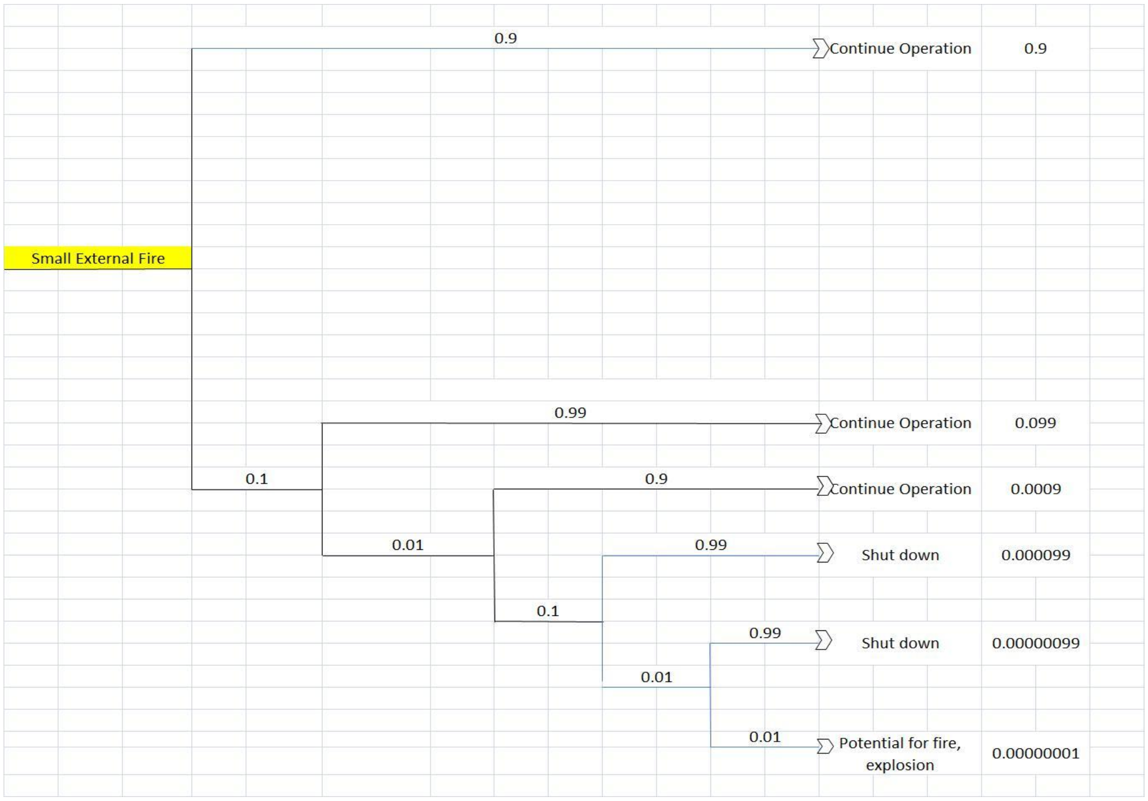


Figure 4.1.4

That even tree shows the scenario resulting from pressure vessel residual failure initiating cause. The failure frequency of this initiating event is 0.1. There are four Independent Protection Layers (IPLs) to prevent the undesirable outcomes to occur in this system. First protection layer is inherently safe design. In this case, the frequency of the failure of safer design is 0.01. Operator response will be the second protection layer if the safer design is not properly functioned. The frequency for operator response failure is 0.1. Then, the third layer is relief valve where relief valve prevent system exceeding specified overpressure. The frequency of relief valve failure is 0.01. The last layer of protection is dike. Frequency of dike to fail per year is 0.01. From the event tree above, potential fire, explosion and toxic release could happen if all of the IPLs are not functioned. The frequency of this scenario is 0.00000001.

<u>Loss of Power (0.1)</u>

Safety Function:	Inherently Safe Design	BPCS	Alarm & Operator Response	SIF	Relief Valve
Identifier	B	C	D	E	F
PFD	0.01	0.1	0.1	0.01	0.01

Table 4.1.5

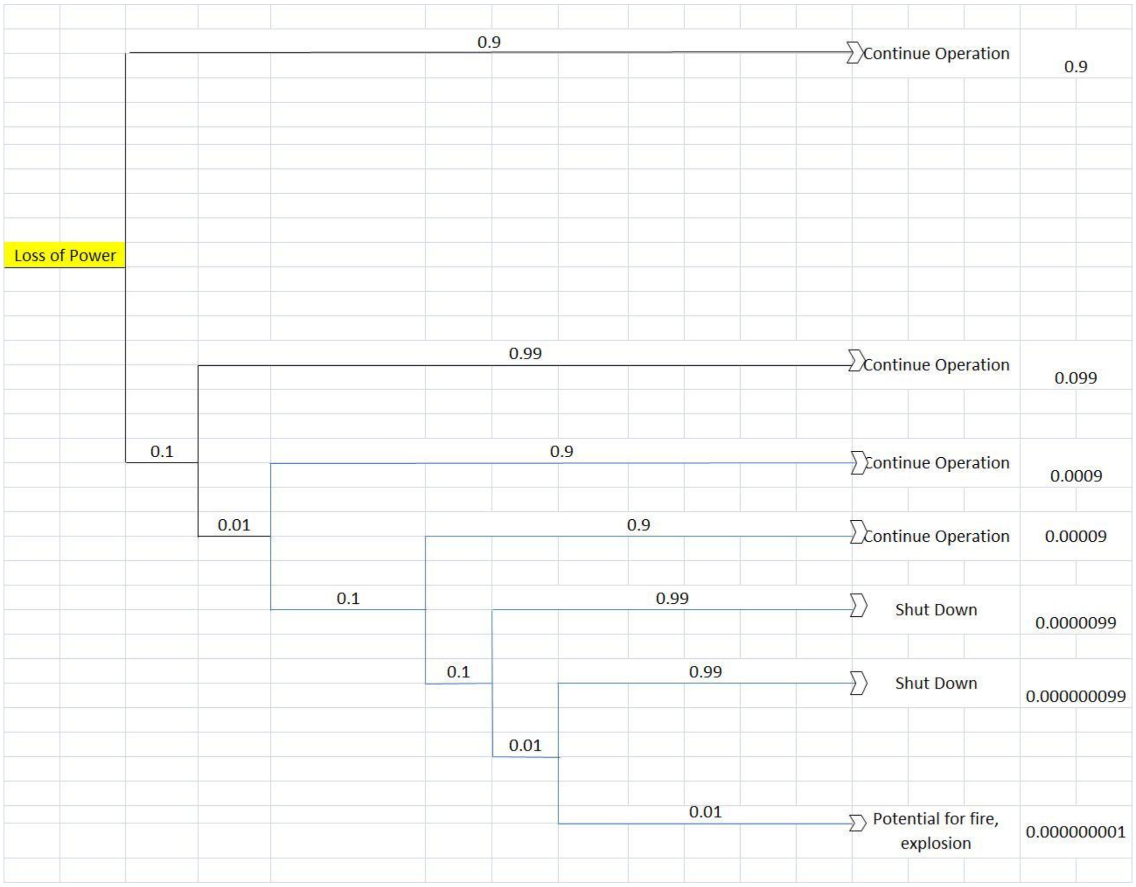


Figure 4.1.5

Above shows the scenario resulting from loss of power initiating cause. The failure frequency of this initiating event is 0. 1. There are four Independent Protection Layers (IPLs) to prevent the undesirable outcomes to occur in this system. First protection layer is inherently safe design. In this case, the frequency of the failure of safer design is 0.01. Basic Process Control System (BPCS) will be the second protection layer if the safer design is not properly functioned. The frequency for BPCS failure is 0.1. When considering using the BPCS as an IPL, the analyst must evaluate the effectiveness of the access control and security systems as must evaluate error can degrade the performance of the BPCS. Then, alarm and operator response will be third protection layer after operator response where it will function if the operator response is failed. The failure frequency of alarm and operator response is 0.1. Then, SIFs will be next protection layer after alarm and operator response where it will function if the before protection layer is failed to respond. The failure frequency of this SIF here is 0.01. The last layer is relief valve where relief valve prevent system exceeding specified overpressure. Relief valve fail to function could lead to the potential undesirable outcomes. Frequency of relief valve failure in this case is 0.01. From the event tree above, potential fire, explosion and toxic release could happen if all of the IPLs are not functioned. The frequency of this scenario is 0.000000001.

From the results above, we can see that an event tree includes the initiating events, the consequences which are the safety function and the possible outcomes. All of them will combine to form scenario consequences which will represent in event tree analysis form. For scenario frequency calculation, the equation below is used:

$$\boxed{\begin{aligned} f_i^C &= f_i^{\mathrm{I}} \text{ x } \prod_{\mathrm{j=1}}^{\mathrm{j}} \mathrm{PFD_{ij}} \\ &= f_i^{\mathrm{I}} \text{ x } \mathrm{PFD_{i1}} \text{ x } \mathrm{PFD_{i2}} \text{ x } \ldots \mathrm{PFD_{ij}} \end{aligned}}$$

Where

f_i^C is the frequency for consequence C for initiating event i

f_i^{I} is the initiating event frequency for initiating event i

PFD_{ij} is the probability of failure on demand of the jth IPL that protects against consequence C for initiating event i.

The above equation is applicable for low demand situations—that is, f_i^{I} is less than twice the test frequency for the first IPL.

4.2 Making Risk Decision

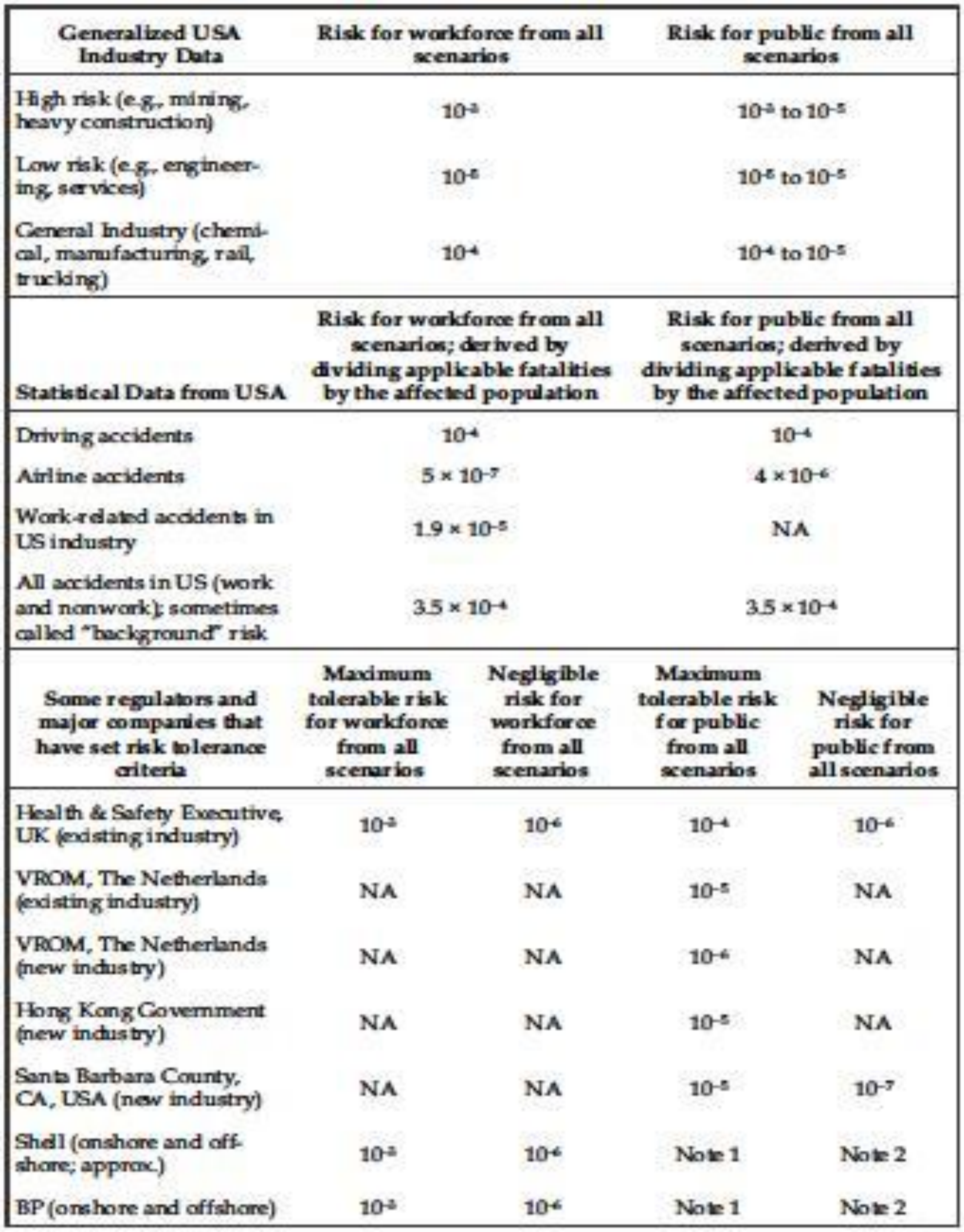
In making risk decision, tolerance risk frequency will be the benchmark to the calculated risk frequency. So, the calculated risk frequency will be compared to the tolerance risk frequency. In LOPA, LOPA ratio has to be calculated to make risk decision. The calculated ratio will determine whether the system is reliable or not reliable In general, LOPA ratio is used to make judgment whether the IPLs or safeguards available in the system is applicable to prevent undesired outcomes. To calculate LOPA ratio, the equation below is used:

$$\boxed{\textit{LOPA Ratio} = \frac{\text{Tolerance Risk Frequency}}{\text{Scenario Frequency}}}$$

Tolerance risk frequency can be obtained from historical data, a company itself and expertise. Scenario frequency is the frequency that was calculated above. Below are the criteria for LOPA ratio:

- If LOPA ratio ≥ 1.0, no need to add other IPLs
- If LOPA ratio ≤ 1.0, has to add other IPLs (SIL), and determine SIL

In the calculation to determine LOPA ratio, the frequency of SIF is not included. This is to determine the level of safety integrity (SIL).

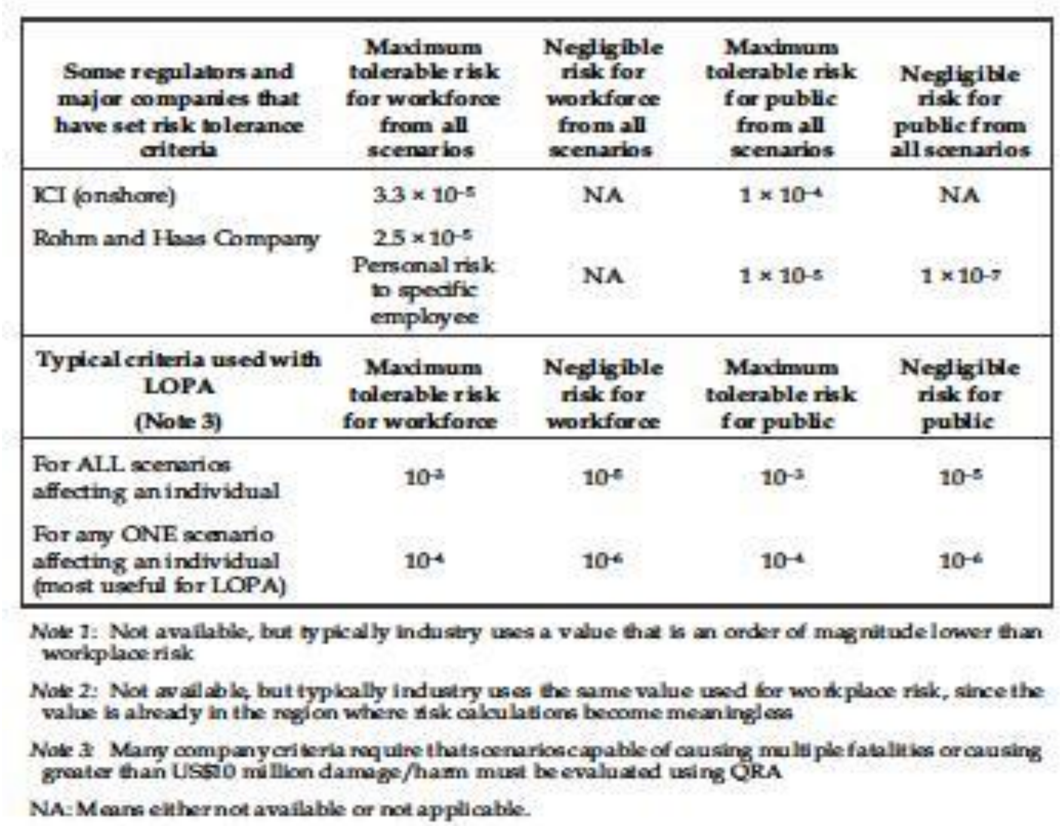


Generalized USA Industry Data	Risk for workforce from all scenarios	Risk for public from all scenarios
High risk (e.g., mining, heavy construction)	10^{-3}	10^{-3} to 10^{-5}
Low risk (e.g., engineering, services)	10^{-6}	10^{-6} to 10^{-5}
General Industry (chemical, manufacturing, rail, trucking)	10^{-4}	10^{-4} to 10^{-5}

Statistical Data from USA	Risk for workforce from all scenarios; derived by dividing applicable fatalities by the affected population	Risk for public from all scenarios; derived by dividing applicable fatalities by the affected population
Driving accidents	10^{-4}	10^{-4}
Airline accidents	5×10^{-7}	4×10^{-6}
Work-related accidents in US industry	1.9×10^{-5}	NA
All accidents in US (work and nonwork); sometimes called "background" risk	3.5×10^{-4}	3.5×10^{-4}

Some regulators and major companies that have set risk tolerance criteria	Maximum tolerable risk for workforce from all scenarios	Negligible risk for workforce from all scenarios	Maximum tolerable risk for public from all scenarios	Negligible risk for public from all scenarios
Health & Safety Executive, UK (existing industry)	10^{-3}	10^{-6}	10^{-4}	10^{-6}
VROM, The Netherlands (existing industry)	NA	NA	10^{-5}	NA
VROM, The Netherlands (new industry)	NA	NA	10^{-6}	NA
Hong Kong Government (new industry)	NA	NA	10^{-5}	NA
Santa Barbara County, CA, USA (new industry)	NA	NA	10^{-5}	10^{-7}
Shell (onshore and offshore; approx.)	10^{-3}	10^{-6}	Note 1	Note 2
BP (onshore and offshore)	10^{-3}	10^{-6}	Note 1	Note 2

Figure 4.2.1: Typical Data Related to Risk Tolerance Criteria



Some regulators and major companies that have set risk tolerance criteria	Maximum tolerable risk for workforce from all scenarios	Negligible risk for workforce from all scenarios	Maximum tolerable risk for public from all scenarios	Negligible risk for public from all scenarios
KCI (onshore)	3.3×10^{-5}	NA	1×10^{-4}	NA
Rohm and Haas Company	2.5×10^{-5} Personal risk to specific employee	NA	1×10^{-5}	1×10^{-7}
Typical criteria used with LOPA (Note 3)	**Maximum tolerable risk for workforce**	**Negligible risk for workforce**	**Maximum tolerable risk for public**	**Negligible risk for public**
For ALL scenarios affecting an individual	10^{-3}	10^{-6}	10^{-3}	10^{-5}
For any ONE scenario affecting an individual (most useful for LOPA)	10^{-4}	10^{-6}	10^{-4}	10^{-6}

Note 1: Not available, but typically industry uses a value that is an order of magnitude lower than workplace risk

Note 2: Not available, but typically industry uses the same value used for workplace risk, since the value is already in the region where risk calculations become meaningless

Note 3: Many company criteria require that scenarios capable of causing multiple fatalities or causing greater than US$10 million damage/harm must be evaluated using QRA

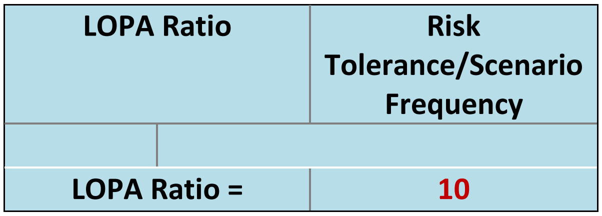
NA: Means either not available or not applicable.

Figure 4.2.2: Typical Data Related to Risk Tolerance Criteria

All values above have units of probability of death per year for an individual. Below shows the steps involve to calculate LOPA ratio, thus determining the SIL:

4.0.1 BPCS Instrument Loop Failure

From Figure 4.6, risk tolerance frequency for general industry (chemical, manufacturing, rail, trucking): 10^{-4} to 10^{-5} (probability of death per year). Take maximum allowable risk, 10^{-5} for safety purposes.



LOPA Ratio	Risk Tolerance/Scenario Frequency
LOPA Ratio =	10

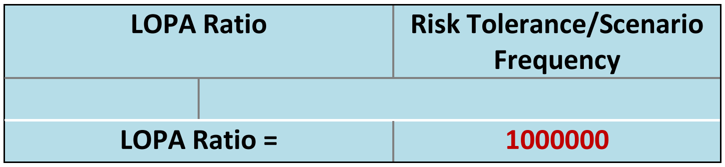
Table 4.2.1

Scenario frequency: $f_{\text{BPCS Instrument Loop Failure}}$ x $f_{\text{Inherently Safe Design}}$ x $f_{\text{Operator Response}}$ x f_{Dike}

Since LR ≥ 1, no need to add other independent protection layers (IPL). So, IPLs are applicable and risk is tolerable.

4.0.2 Pressure Vessel Residual Failure

Maximum allowable risk frequency: 10^{-5}



LOPA Ratio	Risk Tolerance/Scenario Frequency
LOPA Ratio =	1000000

Table 4.2.2

Scenario frequency: $f_{\text{Pressure Vessel Residual Failure}}$ x $f_{\text{Inherently Safe Design}}$ x f $_{\text{Critical Alarms \& Human Intervention}}$ x f $_{\text{Relief Valve}}$

Since LR ≥ 1, no need to add other independent protection layers (IPL). So, IPLs are applicable and risk is tolerable.

4.0.3 Pump Seal Failure

Maximum allowable risk frequency: 10^{-5}

LOPA Ratio	**Risk Tolerance/ Scenario Frequency**
LOPA Ratio =	**0.1**

Table 4.2.3

Scenario frequency: $f_{Pump\ Seal\ Failure}$ x $f_{Inherently\ Safe\ Design}$ x $f_{Operator}$

From above result, LOPA ratio is $0.1 \leq 1.0$. So, the risk is not reliable and need to add other IPLs to ensure that the LOPA ratio reaches 1.0 or above 1.0. To determine the level of safety integrity level, the gap is calculated. Thus, to ensure the LOPA ratio reaches 1.0, an SIL with frequency 10^{-1} is required.

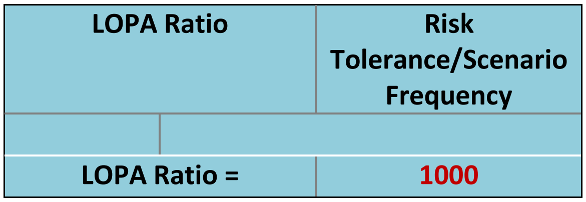
So, SIL to be added=	**Risk tolerance / Scenario Frequency x 0.1**
New LOPA Ratio=	**1.0** (risk is acceptable)

Table 4.2.4

SIL Level= 1* 10-1, SIL 1 is to be used.

4.0.3 Small External Fire

Maximum allowable risk frequency: 10^{-5}



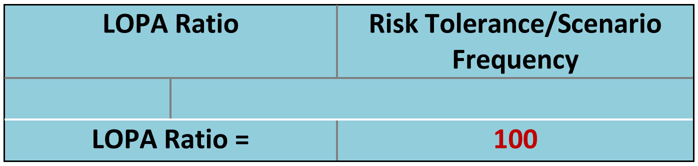
LOPA Ratio	Risk Tolerance/Scenario Frequency
LOPA Ratio =	1000

Table 4.2.5

Scenario frequency: $f_{\text{Small External Fire}}$ x $f_{\text{Inherently Safe Design}}$ x $f_{\text{Operator Response}}$ x $f_{\text{Relief Valve}}$ x $f_{\text{ Dike}}$

Since LR ≥ 1, no need to add other independent protection layers (IPL). So, IPLs are applicable and risk is tolerable.

4.0.3 Loss of Power



LOPA Ratio	Risk Tolerance/Scenario Frequency
LOPA Ratio =	100

Table 4.2.6

Scenario frequency: $f_{\text{Loss of Power}}$ x $f_{\text{Inherently Safe Design}}$ x f_{BPCS} x $f_{\text{Alarm \& Operator Response}}$ x $f_{\text{Relief Valve}}$

Since LR ≥ 1, no need to add other independent protection layers (IPL). So, IPLs are applicable and risk is tolerable.

CHAPTER FIVE
CONCLUSION AND RECOMMENDATIONS

It can be concluded that the whole project involves analysis tool in determining the SIL for hazardous installation. The methodology provided by LOPA help in achieving the risk decision making. In conclusion, LOPA help in classifying Safety Instrumented Function (SIF) to determine the appropriate SIL. Estimating consequence and severity is the initial step to proceed with LOPA. From this estimating consequence and severity, the scenario which is the unplanned event or the sequence of events that result in an undesirable consequence can be developed. Then, initiating event frequency can be identified. When all of those steps are completed, related Independent Protection Layers (IPLs) should be identified. During this stage, the PFD data should be determined. After all information is gathered, the scenario frequency can be determined. Risk decision can be made by comparing the calculated scenario frequency with the tolerable risk frequency. Risk has to be compared with allowable risk to ensure that the system in the plant is in inherently safe design. LOPA facilitates the determination of more precise cause-consequence pair, and therefore improves scenario identification. LOPA also helps resolve conflicts in decision making by providing a consistent, simplified framework for estimating the risk of a scenario and provides a common language for discussing risk. In other words, LOPA helps in risk decision making steps. For future work, it is recommended to apply this LOPA in specific unit or system because this project is applied for general cases. Because in this project involve semi-quantitative method, it is recommended to further this study to quantitative method which involve more mathematical tools to evaluate the scenario for potential fire, explosion and toxic release.

REFERENCES

1) 2001, *Layer of Protection Analysis*, New York; Center for Chemical Process Safety of the American Institute of Chemical Engineers (AIChE).
2) Marszal E.M., Fuller B.A., and Shah J.N.1999, *Process Safety Progress,***(8:4)**, 189-194.
3) Bhimavarapu K., Stavrianidis P. 2000, *Process Safety Progress* **(19:1)**, 19-24
4) Wei C., Rogers W.J., Mannan M.S, 2008, "Layer of protection analysis for reactive chemical risk assessment,"*Journal of Hazardous Materials*, 19-24.
5) Marszal Ed, Scharpf E., 2002, "Safety Integrity Level Selection, Systematic Methods Including Layer of Protection Analysis".
6) Center for Chemical Process Safety (CCPS), "Guidelines for Process Equipment Reliability Data with data tables," American Institute of Chemical Engineers, New York (1989).