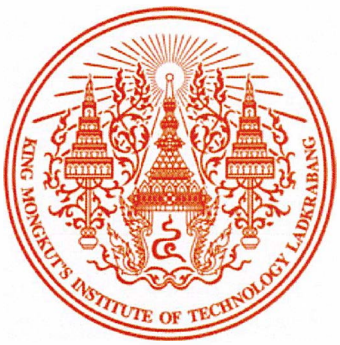

Report of Cooperative Education

Study Safety Integrity Level Classification and Verification with Constant Failure Rate

Naphat Yampry

A Report Submitted in Partial Fulfillment of the Requirements

for the Degree of Bachelor of Engineering (Petrochemical Engineering),

Department of Chemical Engineering, Faculty of Engineering,

King Mongkut's Institute of Technology Ladkrabang

Academic Year 2017

รายงานสหกิจศึกษาฉบับสมบูรณ์

การศึกษาการประเมินและตรวจสอบระดับความเข้มงวดของระบบความปลอดภัย โดยมีอัตราการเสียหายคงที่

ณภัทร แย้มพราย

รายงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต

หลักสูตรวิศวกรรมปิโตรเคมี ภาควิชาวิศวกรรมเคมี คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2560

Co-operative Title:	Study Safety Integrity Level Classification and Verification with Constant Failure Rate
By:	Mr. Naphat Yampry
Field of Study:	Bachelor Degree in Chemical Engineering in Petrochemical Program
Advisor:	Mrs. Siripan Murathathunyaluk
Mentor (Position):	Mr. Pongsakorn Monturat (Section Chief)
Company:	TTCL Public Company Limited

Abstract

Safety Integrity Level (SIL) is a measure of safety system performance for random failure rate which defined as a range in terms of Probability of Failure on Demand. The SIL is measured from Safety Instrumented Function which is a safety function in the Safety Instrumented System for prevent or mitigate hazardous events. There are two different methods to define SIL. Firstly, Risk graph is qualitative method base on four parameters are Consequence, Occupancy, Possibility of avoiding the consequences and Demand rate. Secondly, Layer of Protection Analysis is a semi-quantitative method using numerical categories to estimate the parameters needed to calculate. In this work, the SIL exSILentia version 3.3.0.908 is used to determine SIL level which consist of two steps are SIL Classification for indicating the required SIL level of the safety system and SIL Verification which to perform the safety function needs to be designed. The SIL Verification need to consider about requirements and constrains for define SIL level of the system. The results from SIL Verification are expected to be in line with the expected value of SIL Classification in all cases.

Keywords: Safety Integrity Level, Probability of Failure on Demand, Safety Instrumented System

ACKNOWLEDGEMENTS

I would like to thank TTCL Public Company Limited for giving me the opportunity to do the co-operative education project. I am also appreciative to Mr. Pongsakorn Monturat, Section chief, and all members in process department for sharing knowledge, expertise and support to succeed research.

Furthermore, I am also grateful to my advisor, Mrs. Siripan Murathathunyaluk for teaching me, advising me, and giving me opportunities to practice. Her guidance helped me in all time of research and writing this report.

I would like to thank my family: my parents and my sister for supporting me spiritually throughout writing this thesis and my life in general. I hope this research will be useful for anyone who is interested in it.

Naphat Yampry

TABLE OF CONTENTS

Page

TABLE OF CONTENTS

Page

LIST OF FIGURES

Figure Page

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

CHAPTER I.

INTRODUCTION

1.1 Background

TTCL Public Company Limited is the first integrated Engineering, Procurement and Construction (Integrated EPC) of turnkey projects for industrial and process plants, mainly in energy, petrochemical, chemical and power industries. The company prepares convenient analysis reports for determine the Safety integrity level (SIL), which is used for providing elements according to specification.

Safety integrity level is used to define the performance of safety in the system. The levels of SIL are very important because the digits relate to the strict of safety element(s) that used to protect the system. The safety elements system is called Safety instrumented system (SIS) is designed to prevent or reduce hazardous events. For each Safety instrumented system can contain one or more Safety instrumented function (SIF), which is a safety protective function by detect a hazard and bring the system to a safe state.

The typical methods for determine SIL classification are Risk graph and Layer of Protection Analysis (LOPA) method. The exSILentia software version 3.3.0.908 are convenient, precise and extensive software, which used to determine both SIL classification and SIL verification by the IEC 61508/61511 method. The results of analysist shown as levels of SIL and Risk reduction factor (RRF) which can used to compare between required value and achieved value of SIL.

1.2 Objectives

1.2.1 To implement the SIL Classification with Risk graph and Layer of Protection Analysis method by using exSILentia version 3.3.0.908

1.2.2 To verify desired SIF as per SIL target or SIL Verification via exSILentia version 3.3.0.908

1.3 Scopes of Work

1.3.1 Study safety system which consists of SIS, SIF and SIL.

1.3.2 Study Failure rate prediction to calculate the Probability of Failure on Demand.

1.3.3 Study SIL Determination Methods which consists of Risk graph and Layer of Protection Analysis method.

1.3.4 Use exSILentia version 3.3.0.908 to analysis SIL Classification and Verification

1.4 Expected Output

The results of SIL Verification and SIL achievement from analysis by exSILentia version 3.3.0.908 are meet the SIL Classification or SIL requirement from both of Risk graph and Layer of protection analysis method.

CHAPTER II.

LITERATURE REVIEW

2.1 Safety Instrumented System

Safety Instrumented System (SIS) is designed to prevent or mitigate hazardous events by enchanting a process to a safe state when predetermined conditions are violated. The SIS does this by decreasing the frequency of unwanted accidents. The well know terms for SISs are safety interlock systems, emergency shutdown systems (ESD), and safety shutdown systems (SSD). For one SIS can has one or more Safety Instrumented Functions (SIF). The component of SIS to perform its function, are consists of Sensor(s), Logic solver(s), and Final element(s) (see Figure 2.1).

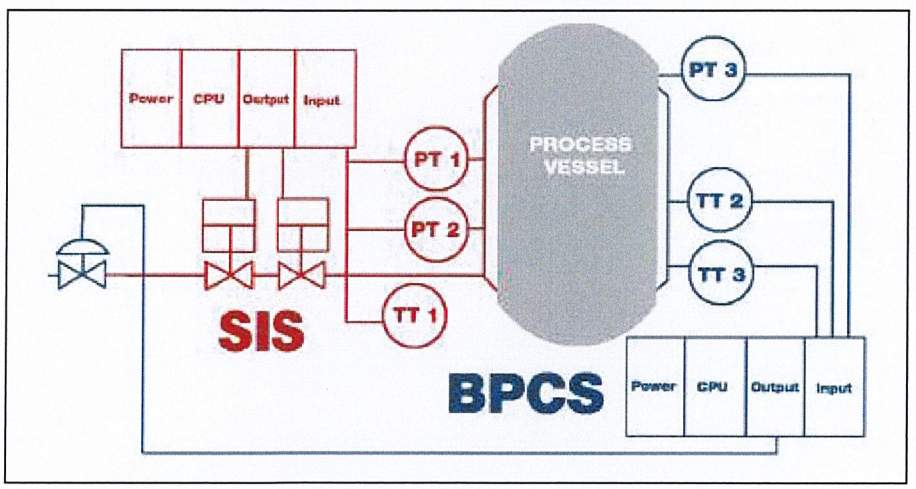

Figure 2.1. The process connection of SIS and BPCS

The process connection of Basic Process Control System (BPCS) which handles process control and monitoring and SIS are clearly separate. The Sensor is used to collect information to define if a hazardous event occurs. The purpose of sensor is to measure process parameters, for examples are temperature, pressure, flow, and level, used to regulate if the process is in a safe state. The Logic solver is used to determine the action is to be taken by based on the information collected. The typically duty of controller is read

signals from the sensors then perform the actions to prevent a hazard by sending output to final element(s). The Final element implements the action determined by the logic system.

2.2 Safety Instrumented Function

A Safety Instrumented Function (SIF) is a safety function with a specified Safety Integrity Level (SIL) which is executed by a SIS in order to achieve or maintain a safe state. This function is a single set of actions that protects against a single specific hazard. The purpose of SIF are to taking a process to a safe state when specified conditions are violated, permit a process to move forward in a safe manner when specified conditions allow and Taking action to mitigate the consequences. The ability to detect, decide and act is designated by the SIL of the function. A SIF's Sensor, Logic solver, and Final elements act in concert to detect a hazard and bring the process to a safe state.

Every SIF within a SIS will have a SIL level. These SIL level may be the same or different depending on the process. It is a common misconception that an entire system must have the same SIL level for each safety function (see Figure 2.2).

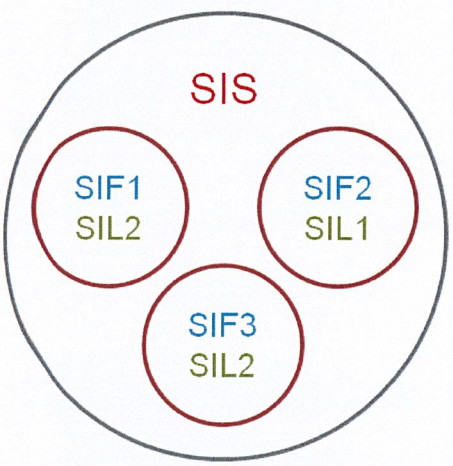

Figure 2.2. The SIS, SIF and SIL relation

2.3 Safety Integrity Level

A Safety Integrity Level (SIL) is a measure of safety system performance which defined as a range in terms of Probability of Failure on Demand (PFD). For easier way to consider the system performance, the agreement was chosen based on the numbers. There are four discrete integrity levels associated with SIL: SIL 1, SIL 2, SIL 3, and SIL 4 (see Table 2.1). The higher the SIL level, the higher the associated safety level, and the lower probability that a system will fail to perform properly. If the SIL level increases, typically the installation, maintenance costs and complexity of the system also increase. The process which in range of SIL 4 is specific process because the safety systems are so complex and expensive that they are not economically beneficial to implement. Additionally, if a process includes so much risk that a SIL 4 system is required to bring it to a safe state, then there is a fundamental problem in the process design that needs to be addressed by a process change or other non-instrumented method.

Table 2.1. The relation of SIL, PFD_{Avg} and RRF

Safety Integrity Level (SIL)	Average Probability of Failure on Demand (PFD_{Avg})	Risk Reduction Factor (RRF)
1	$\geq$10-2 to <10-1	>10 to $\leq$100
2	$\geq$10-3 to <10-2	>100 to $\leq$1000
3	$\geq$10-4 to <10-3	>1000 to $\leq$10,000
4	$\geq$10-5 to <10-4	>10,000 to $\leq$100,000

The risk assessment would determine the current level of risk presented by the facility. This would be compared against a tolerable risk level. The gap between the actual risk level and the tolerable risk is the required level of risk reduction, also called the Risk Reduction Factor (RRF). The RRF is the relation of the actual risk presented by the facility and the risk that must be achieved as a target based on the acceptance criteria (see Figure 2.3).

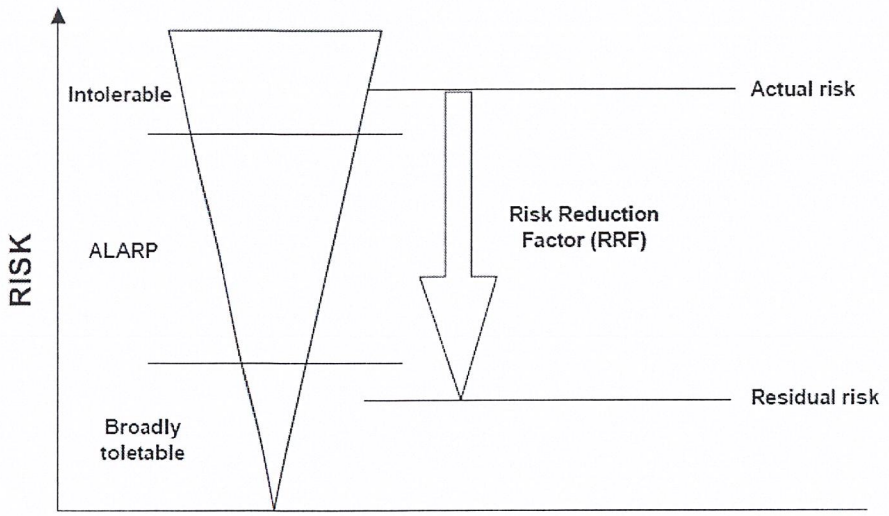

Figure 2.3. Risk reduction factor concept

$$RRF = \frac{1}{PFD_{Avg}} \tag{2.1}$$

2.3.1 SIL Classification

SIL Classification is the activity of indicating the required SIL level for each SIF in SIS. The SIL Classification is generally done after the risk assessment (Hazard Identification and Risk Assessment (HAZOP) or Hazard Identification Studies (HAZID)) has been performed and the SIFs required have been defined. The SIL classification is used to determine the required Reliability of the safety function and is related to the probability of the safety related system suitably performing the required safety function. There are several methods suggested in IEC 61508 and IEC 61511 for SIL classification. The two widely used methods are Layers of Protection Analysis and Risk Graph.

2.3.2 SIL Verification

Once the requirement of the SIL level has been determined, the SIS which will perform the safety function needs to be designed accordingly. The SIL Verification need to consider about requirements and constrains for define SIL level of the system. The SIL level

achievement 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 level is not achieved, the equipment cannot be accurately design because only the action is specified, not the integrity.

2.4 Reliability and Availability

The term random variable is well understood in the field of statistics. It is the independent variable that being studied. Samples of the random variable are taken, and statics are computed about that variable in order to learn how to predict its future behavior. In Reliability engineering, the primary random variable is T: time to failure. Reliability engineers gather data about when and how thing fail. This information is used to gain insight into future performance of system designs.

2.4.1 Reliability

The Reliability (R) can be defined as the probability of that an item will perform a defined function without failure under specified conditions for a period of time. The Reliability is use with non-repairable items which cannot stop the process for a while to repair the equipment. The numerical values of Reliability is indicated as a probability from 0 to 1 and have no units. Mathematically, Reliability is the probability that a system will be successful in the time interval from time interval zero to t. Reliability equals the probability that failure time (T), is greater than operating time interval (t).

$$R(t) = P(T>t) \tag{2.2}$$

2.4.2 Unreliability

The Unreliability (F) can be defined as the probability of a system that the system experiences the first failure or has failed one or more times during the time interval zero to time t. The Unreliability is use with non-repairable items which cannot stop the process for a while to repair the equipment. The numerical values of Unreliability is indicated as a probability from 0 to 1 and have no units. Unreliability equals the probability that operating time interval (t), is greater than failure time (T).

$$F(t) = P(T \leq t) \tag{2.3}$$

The following relationship between Reliability and Unreliability in the time interval zero to t or remain operating over this period has the probability equal to 1.

$$R(t) + F(t) = 1 \tag{2.4}$$

2.4.3 Availability

The Availability is defined as the probability that system will perform a defined function successful at time t. No time interval is involved. The Availability is use with repairable items which can stop the process for a while to repair the equipment. It does not matter whether it has failed in the past and has been repaired or has been operating continuously from time (t) equal to 0 without failure. Availability is a measure of uptime in a system.

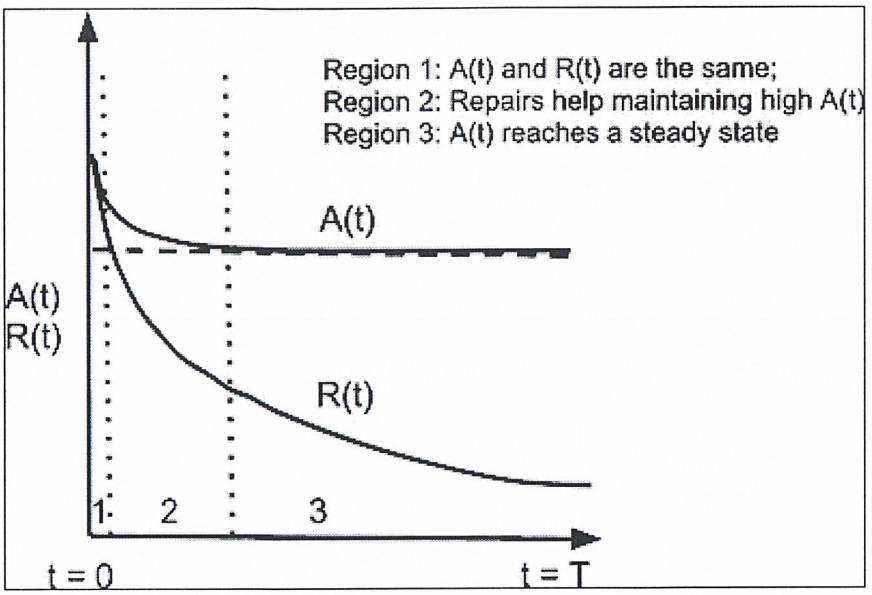

Figure 2.4. Comparison of Reliability and Availability

Availability and Reliability are largely different. Reliability is a function of operating time interval and failure rates. The Reliability measures from start at one and goes to zero as the time interval gets longer. Availability is a function of failure rates, repair rate and operating time. But Availability results will reach a steady-state value as a function of operating time interval. A plot of Availability versus Reliability for a single repairable module is shown in Figure 2.4.

2.4.4 Unavailability

The Unavailability (Q) is the probability that system will perform the failed state at time t. The Unavailability is use with repairable items which can stop the process for a while to repair the equipment.

The following relationship between Availability and Unavailability at the time t remain operating over this period has the probability equal to 1.

$$A(t) + Q(t) = 1 \qquad (2.5)$$

2.5 Failure Prediction

2.5.1 MTTF, MTTR, MTBF and their relations

Mean Time to Failure (MTTF) is the average time to describe the first of failure has been occur for non-repairable system. MTTF is a statistical value which is intended to be the mean over a long period of time and with a large number of units.

Mean Time to Repair (MTTR) is the average time of the total amount of time spent to repair or make the device can undergo to perform its function again. The MTTR is use for repairable system only. It is the expected span of time from a failure (or shut down) to the repair or maintenance completion. This term is typically only used with repairable systems.

Mean Time between Failures (MTBF) is a basic measure of reliability for repairable system. The MTBF is describe the period of time passed before a system fails, until the system fail and then the system has been repair and ready to start processing under a constant failure rate. Another way of MTBF is the expected value of time between two mean times are MTTF and MTBF, for repairable systems. The relation of MTTF, MTTR and MTBF is shown in Figure 2.5.

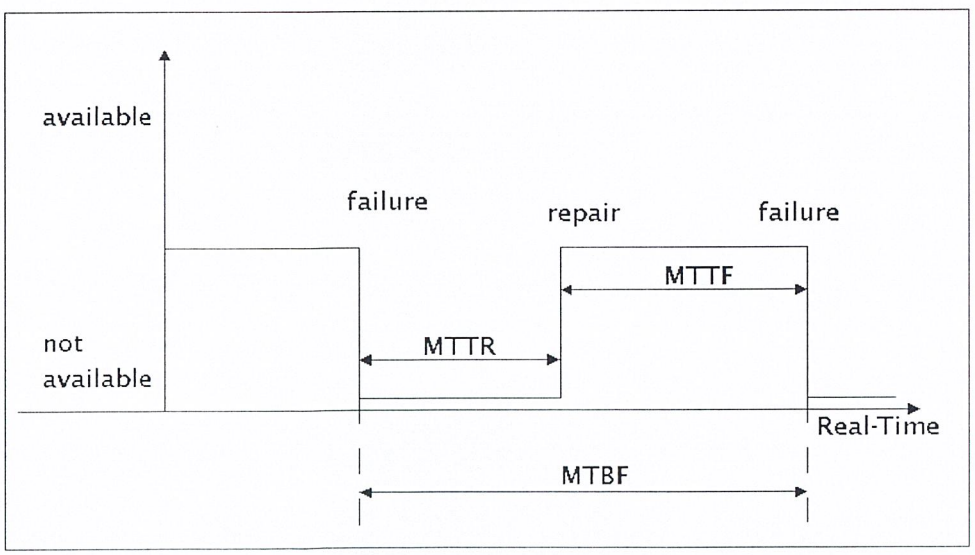

Figure 2.5. The relation of MTTF, MTTR and MTBF

2.5.2 Repairable and Non-repairable systems

Non-repairable systems are the system that cannot stop the process for maintenance or repair. The examples Non-repairable systems are bulb, diode and unmanned spacecraft. Their reliability of Non-repairable systems are the survival probability over the systems expected life or over a period of life time, when only one failure can occur. During the systems life, the sudden probability of the first and only failure is called the failure rate, $\lambda(t)$. The life values can describe by MTTF to define non-repairable items.

Repairable systems are the system that can stop the process for maintenance or repair. The Reliability of Repairable systems are the probability that failure will not occur in the time period of interest. The Reliability can be expressed as the failure rate, $\lambda(t)$. In the case of Repairable systems, the Reliability can be described by MTBF which described above, but only under a constant failure rate. There is also the concern for Availability, A(t), of Repairable systems since repair takes time. Availability, A(t), is the probability that systems are in an operable state at any time.

$$A(t) = \frac{MTTF}{MTTF + MTTR} \tag{2.6}$$

2.5.3 Failure rate

Failure rate is used to express the reliability of simple systems which related to the other reliability functions. The Failure rate is measured in inverse of time, such as failures per million hours. It is also frequently used to express the reliability of particular functions, for example the dangerous failure rate of a safety system. The Failure rate is used to calculate Probability of failure on demand to specify SIL level.

$$\lambda = \frac{\text{Failures per unit time}}{\text{Quantity exposed}} \tag{2.7}$$

The Failure rate consists of two categories are detected Failure rates and undetected Failure rates. Both detected Failure and undetected Failure rates are consisting of two types are safe and dangerous mode.

$$\lambda^{D} = \lambda^{DD} + \lambda^{DU} \quad (2.8)$$

$$\lambda^{S} = \lambda^{SD} + \lambda^{SU} \quad (2.9)$$

$$\lambda = \lambda^{DD} + \lambda^{DU} + \lambda^{SD} + \lambda^{SU} \quad (2.10)$$

When λ^{DD} = dangerous detected failure rates (1/time)

λ^{DU} = dangerous undetected failure rates (1/time)

λ^{SD} = safe detected failure rates (1/time)

λ^{SU} = safe undetected failure rates (1/time)

2.5.4 Failure Pattern

The Failure Pattern has many models that can explain behavior of failure, but the Bathtub Curve is fundamental and well-known model. In common in their failure rate profiles as represented in the bath-tub curve. The Bathtub Curve may be broadly classified in three distinct time zones, each corresponds a distinctive failure mode (see Figure 2.6). The behavior of failures are consists of three patterns, which change with time. The Failure rate may be decreasing, increasing or constant.

The first pattern is Decreasing failure rate can be caused by an item, which becomes less likely to fail as the survival time increases. This is represented by electronic equipment during their early life or at the first period. This is represented at the first half of the Bathtub Curve for electronic equipment where Failure rate is decreasing during the early life period. Then the Failure rate is gradually decrease until past to the second pattern.

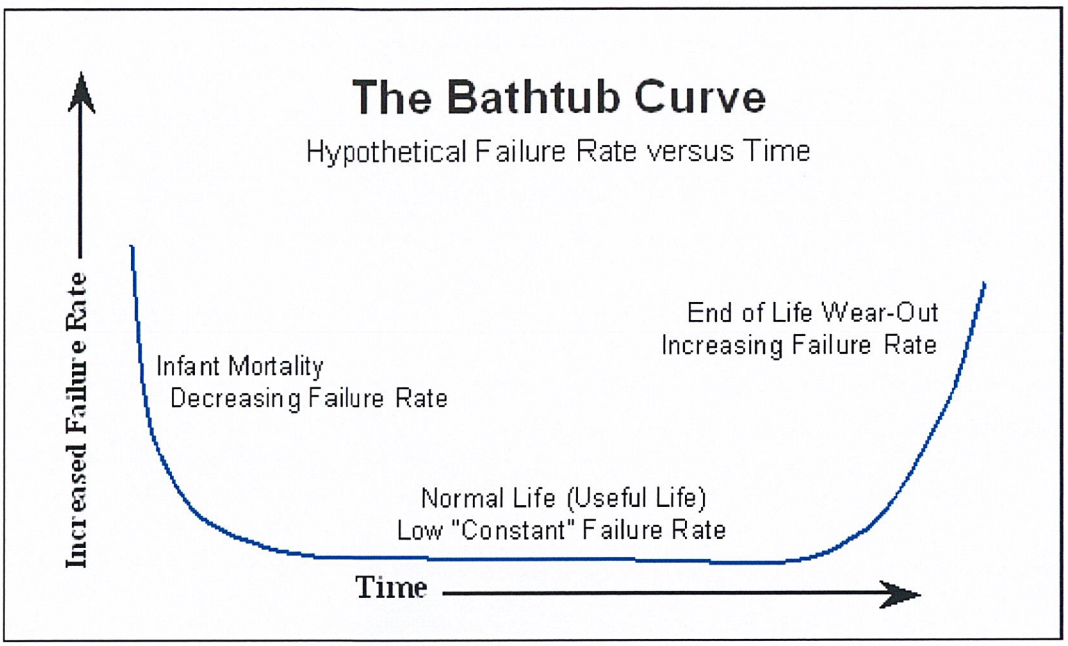

Figure 2.6. Bathtub Curve

The second pattern is Constant failure rate which has constant failure rate. In this pattern is the useful life in the industrial. The useful life is the period of time that the equipment can processing the process even the equipment stop to maintenance or repair. In this model can assume that the time for maintenance or repair is negligible because the time of process is enormous than stopped time. For any calculation include Reliability, Availability, MTTF, MTTR, MTBF, Failure rate and Probability of failure on demand are use the constant data Failure rate to calculate because it is the easiest way and this period take a long time, so it can assume that covers all of the time that equipment is used.

The last pattern is Increasing failure rate can be caused by out of service or cannot repair equipment. The Failure rate is increasing continuously. This is represented at the last of the Bathtub Curve for electronic equipment where Failure rate is increasing during the late life period.

2.5.5 Probability of Failure on Demand

Probability of Failure on Demand (PFD) is the probability that system fail dangerously and cannot perform the safe state when required. The PFD is the unavailability of a safety function. The Average Probability of failure on demand (PFD_{Avg}) is real probability of the system which correct term to use by the Failure rate is constant, so the probability of the system having failed will depending on how long the test takes.

$$PFD_{Avg} = \frac{\lambda^{DU} \times T_{PT}}{2} \quad (2.11)$$

When T_{PT} = proof test time (hour)

λ^{DU} = dangerous undetected failure rates (1/time)

2.6 Requirements and constrains

For Safety Instrumented Systems (SIS) requires a compound called Safety Integrity Level (SIL). Safety integrity is defined by IEC 61508 as the probability of a safety system acceptable performing the required safety functions under the assign conditions within a specified period of time. The two requirements that SIS needed to indicate the SIL Level are Quantitative requirements and Architectural constrains.

2.6.1 Quantitative requirements

The quantitative requirement for low demand mode of operation SISs is expressed as the PFD_{Avg} which is the unavailability of a safety function. The PFD_{Avg} requirement applies for the whole SIS. The PFD_{Avg} for the SIS can be approximated by summarizing the PFD_{Avg} for the sensors, logic solvers and final elements as indicated in Equation 2.2.

$$PFD_{Avg} = PFD_{Sensor} + PFD_{Controller} + PFD_{Final\ element} \quad (2.12)$$

2.6.1.1 Common-Cause Failures

Common-Cause Failures is the failure of more than one system due to the same cause. This failure negates the benefits of a fault-tolerant system. Fault-tolerant systems provide two or more modules to prevent system failure when module failure occurs.

Beta Model is a one of the simplest model from several models that uses β-factor to divide the failure rate of each component into common cause (two or more fails) and normal (one fail). The beta factor is used to divide the failure rate into the "common-cause" portion, λ^C and the normal portion, λ^N. The following equations are used:

$$\lambda^C = \beta \times \lambda \tag{2.13}$$

$$\lambda^N = (1-\beta) \times \lambda \tag{2.14}$$

When β = fraction of undetected failures that have a common cause

λ = failure rates (1/time)

2.6.1.2 Diagnostic tests

Diagnostic tests are normally referred to as online tests or automated tests and are performed either continuously or very frequently. Diagnostic tests detect dangerous failures and can change them to "safe" failures by bringing the process to a safe state or alarm operations/maintenance personnel to take some action. The efficiency of Diagnostic test can be described with Diagnostic coverage factor.

Diagnostic coverage factor (C) is measure the probability that failure will be detected resulting from the use of automatic diagnostic tests.

$$C = \frac{\lambda^{DD}}{\lambda^{DD} + \lambda^{DU}} \tag{2.15}$$

2.6.1.3 Proof Test

Proof tests are usually performed at pre-defined test intervals per the Safety Requirement Specification (SRS). Ideally real operating process conditions should be present or simulated for the proof tests and can be divided into parts versus complete end to end testing depending upon safety conditions.

Proof testing has significant influence on the final PFD_{Avg} value and the effectiveness of proof testing is not negligible. The effectiveness of a proof test is measured by its C_{PT}. The proof test coverage factor (C_{PT}) gives the fraction of dangerous undetected failures which can be detected by proof testing.

$$C_{PT} = \frac{\lambda^{DU}_{\text{identified by PT}}}{\lambda^{DU}_{\text{total}}} \tag{2.16}$$

2.6.1.4 System configurations

To determine the Average Probability of Failure on Demand for each of the subsystems, the equation should be adhered to for each subsystem. There are many types of System configuration, for the common type is M-out-of-N (MooN). M is the number of independent wired connection of system, while N is the number of element. System is composed of statistically independent and identically distributed components with exponential lifetimes. The reliability of such a system is obtained under the assumption that the failure of a component changes the failure rate of the surviving components.

1oo1

$$PFD_{1oo1} = (\lambda^{DU} + \lambda^{DD})t_{CE} \quad (2.17)$$

$$t_{CE} = \frac{\lambda^{DU}}{\lambda^{D}}(\frac{T_{PT}}{2} + MRT) + \frac{\lambda^{DD}}{\lambda^{D}}(MTTR) \quad (2.18)$$

1oo2

$$PFD_{1oo2} = 2(\lambda^{DU} + \lambda^{DD})^2 t_{CE} t_{GE} \quad (2.19)$$

$$t_{GE} = \frac{\lambda^{DU}}{\lambda^{D}}(\frac{T_{PT}}{3} + MRT) + \frac{\lambda^{DD}}{\lambda^{D}}(MTTR) \quad (2.20)$$

2oo2

$$PFD_{2oo2} = 2(\lambda^{DU} + \lambda^{DD})t_{CE} \quad (2.21)$$

2oo3

$$PFD_{2oo3} = 6(\lambda^{DU} + \lambda^{DD})^2 t_{CE} t_{GE} \quad (2.22)$$

1oo3

$$PFD_{2oo3} = 6(\lambda^{DU} + \lambda^{DD})^3 t_{CE} t_{GE} t_{G2E} \quad (2.23)$$

$$t_{G2E} = \frac{\lambda^{DU}}{\lambda^{D}}(\frac{T_{PT}}{4} + MRT) + \frac{\lambda^{DD}}{\lambda^{D}}(MTTR) \quad (2.24)$$

When λ^{DU} = dangerous undetected failure rates (1/time)

λ^{DD} = dangerous detected failure rates (1/time)

λ^{D} = dangerous failure rates (1/time)

T_{PT} = proof test time (hour)

t_{CE} = channel equivalent mean down time (hour)

t_{GE} = voted group equivalent mean down time (hour)

t_{G2E} = voted group equivalent 3rd element mean down time (hour)

MRT = mean repair time (hour)

MTTR = mean time to repair (hour)

2.6.2 Architectural constrains

A second requirement that must be fulfilled for a SIS to obtain a given SIL is the Architectural constrains. Architectural constraints on hardware safety integrity are given in terms of three parameters; Hardware fault tolerance (HFT) ability of a functional unit to continue to perform a required function in the presence of faults or errors. Therefore, hardware fault tolerance is the ability of the hardware (complete hardware and software of the transmitter) to continue to perform a required function in the presence of faults or errors. A hardware fault tolerance of 0 means that if there is one fault, the transmitter will not be able to perform its function (for example, measure level).

Safe failure fraction (SFF) is the fraction of failures which can be considered safe because they are either detected or are classified as safe failures. Equation 2.7 is used to calculate the SFF

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}} \tag{2.25}$$

Hardware fault tolerance (HFT) is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. For the general is MooN voting, the fault tolerance is simply N – M.

The table from the standard showing the minimum hardware fault tolerance of sensors and final elements is shown in Table 2.2.

Table 2.2. Field Device Fault Tolerance Table from IEC 61511

SIL	Minimum Hardware Fault Tolerance
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

The table from the standard showing the minimum hardware fault tolerance of controllers is shown in Table 2.3 .

Table 2.3. Architectural constraints for type B subsystems Fault Tolerance table from IEC 61511

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
< 60%	-	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4

2.7 Methods in determining SIL

As mentioned in the previous section various SIL determination methods and tools exist. Both qualitative and quantitative approaches may be applied. In qualitative methods the parameters used as decision basis are subjective and estimated by expert judgment. Quantitative methods describe the risk by calculations, and a numerical target value is compared with the result, which methods to apply rely primarily on whether the necessary risk reduction is specified in a quantitative method or qualitative method. The scope and extent of the analysis would also be an influencing factor.

2.7.1 Risk graph

Risk graphs are qualitative and category based, which considers the consequence and frequency of the hazardous event, but also occupancy and the probability of personnel avoiding the hazard. In Table 2.4 the classification of the risk parameters suggested in IEC 61511 is shown. The consequence parameter (C) describes the likely outcome of the hazardous event, and four categories of consequences are

suggested. C_A is less severe than C_D, ranging from light injury to many fatalities. In this case consequences are measured in the extent of injury to people, but also environmental or financial target measures can be utilized.

The occupancy parameter (F) indicates the fraction of time the hazardous area is occupied by personnel. F_B indicates higher risk than F_A, as the area is more frequently exposed. Usually, F_A is selected if the hazardous area is occupied less than approximately 10% of the time IEC 61511 (2003).

The possibility of personnel avoiding the hazard is incorporated in the parameter (P). This parameter reflects what methods the personnel have to identify and escape the hazard. In addition skill and supervision in process operation, and the rate of development of the hazardous event are taken into account. Two categories, P_A and P_B, are suggested and P_B indicates the highest risk. A checklist of statements that must be true in order to select P_A, can be utilized in the evaluation. Such statements are suggested in IEC 61511.

The final parameter is the demand rate parameter (W), which is the frequency per year of the unwanted consequence without the concerning SIF but with other safeguards operating. Also for this parameter higher parameter indices indicate higher risk, as they take less credit for risk reduction by other safeguards. W_1 indicates that only a few occurrences are likely, and a demand rate less than 0.03 per year could fit such description. W_2 and W_3 indicate that few occurrences or frequent occurrences are likely, and suitable demand rates per year could be 0.03 - 0.3 and more than 3, respectively. The choice of this parameter will affect the result, and care should be taken when selecting category.

Table 2.4. Classification of risk parameters adopted from IEC 61511

Risk parameter	Category	Classification
Consequence (C)	C_A	Light injury to persons
	C_B	Serious injury to one or more persons. Death of one person
	C_C	Death of several persons
	C_D	Catastrophic effect, very many people killed
Frequency of presence in the hazardous zone (F) (occupancy)	F_A	Rare to more frequent exposure in the hazardous zone
	F_B	Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the consequences of the hazardous event (P)	P_A	Possible under certain conditions
	P_B	Almost impossible
Frequency of the unwanted consequence (W)	W_1	A very slight probability that the unwanted occurrences occur and only a few occurrences are likely
	W_2	A slight probability that the unwanted occurrences occur and few occurrences are likely
	W_3	A relatively high probability that the unwanted occurrences occur and frequent occurrences are likely

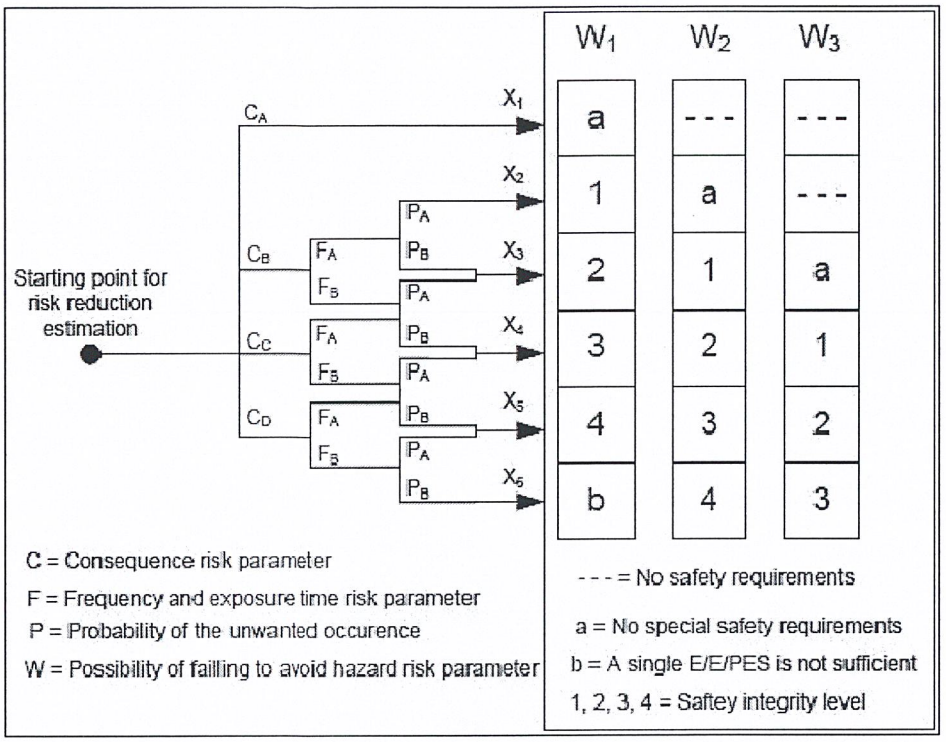

Figure 2.7. Typical risk graph

Figure 2.7 shows a typical risk graph diagram. The path from left to right is decided by the selected risk parameters. The selected consequence, occupancy and possibility of avoidance categories result in an output row X. Each output row corresponds to three values of W. The selection of the demand rate W is the last step in determining the SIL. Higher W-parameter is lead to a higher SIL. The tolerable level of risk is embedded in the boxes in the three columns at the right-hand side, and the choice of these must support the company risk criteria.

The calibrated risk graph method is a semi-qualitative method, similar to the qualitative risk graph. The same risk parameters are used as for the conventional risk graph approach, and Figure 2.7 is also applicable. Calibration means that numerical values are assigned to the risk graph, and these are assigned to the risk parameters. This allows a more precise determination of the SIL, and making the decisions more objective. The

calibration depends on individual and societal risk, and these issues in addition to company criteria and authority regulations, should be considered before assigning the parameter values. Calibration does not need to be carried out every time a SIL need to be determined. The organization only needs to do it once for similar hazards. Documentation of the calibration process with references is necessary, and should be done with care. When the calibration process is finished, and the parameters decided. The risk graph is used to determine the SIL.

Finally the calibration processes has been finished and parameters have been decided. The risk graph is used to determine the SIL classification by the demand rate, occupancy and possibility of avoiding the consequence of the hazardous event, represents the frequency of the unwanted consequence. In combination with the unwanted consequence the frequency constitutes the risk without the Safety instrumented function (SIF) in place. The input in each box in the risk graph must be in accordance with the tolerable risk in IEC 61511.

2.7.2 Layer of Protection Analysis

Layer of Protection Analysis (LOPA) is a semi-quantitative method using numerical categories to estimate the parameters needed to calculate the necessary risk reduction which corresponds to the acceptance criteria. LOPA usually receives output from a HAZOP or HAZID.

In Figure 2.8 is used as an illustration of the protection layers in LOPA. The system or process design has protection layers including basic process control system (BPCS), critical alarms and human intervention, SIFs, physical protection and emergency response.

BPCS is the control system used during normal operation and sometimes denoted as the process control system (BPCS). Input signals from the process and / or from the

operator are generated into output signals which make the process operate in a desired manner. If the control system discovers that the process is out of control (e.g. high pressure) it may initiate actions to stabilize the temperature (e.g. choking the flow).

Alarms monitoring certain parameters (e.g. pressure and temperature) are considered another protection layer. When the alarm is tripped, the operator may intervene to stop the hazardous development. Note that the alarm system has to be wired to another loop than the BPCS in order to be independent.

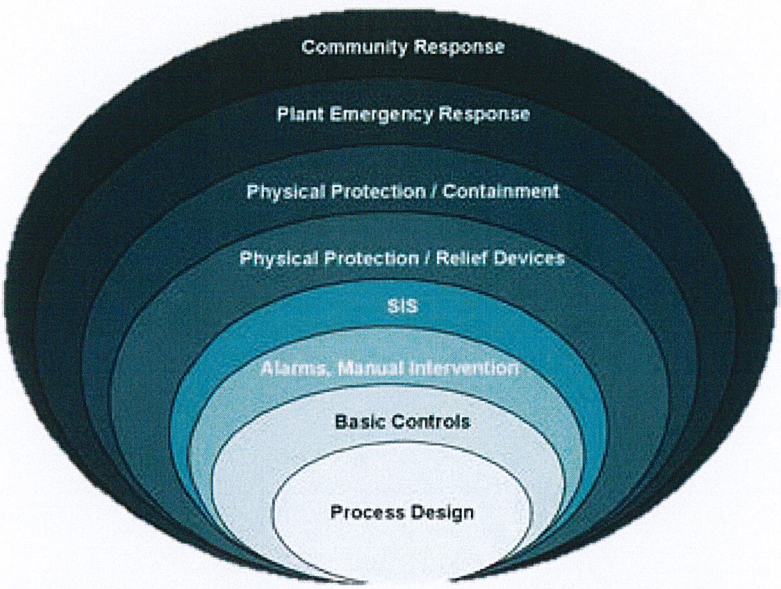

Figure 2.8. The LOPA layers

SIS as a system comprising sensor(s), logic solver(s), and final element(s), and can be looked upon as an independent protection shell for machinery or equipment. A SIS implements the wanted safety function SIF. In LOPA, SIFs are considered as protection layers. The LOPA method a clear methodology and approach is needed to make the team focus on the analysis and not on how to do the analysis. The terms are adapted to the definitions presented earlier thus somewhat different from the ones in IEC 61511. The LOPA

report worksheet presented in IEC 61511 is shown in Table 2.5. Further the columns will be explained briefly step by step.

Table 2.5: Important columns in the LOPA report adapted from IEC 61511

1	2	3	4	5				6	7	8
				Layers of Protection (Probability of Failure)						
Impact Event Description	Initiating Cause	Initiation Likelihood	Target Risk	General Process Design	Basis Process Control system	Alarms & Operator Action	Additional Mitigation, Restricted Access	Intermediate Event Likelihood	SIF integrity level	Mitigated event likelihood

Impact event description: The potential impact event is described in the first column in the table. This is the consequences determined in the HAZOP study.

Initiating cause and initiation likelihood:_All direct initiating causes of the impact event are listed in column 3. In column 4 the likelihood values of the initiating causes occurring, in events per year, are entered. A table showing typical values is shown in IEC 61511, e.g. a failure with a low probability of occurring within the lifetime of the plant (dual instrument or valve failure) is categorized with a frequency between 10^{-4} and 10^{-2} per year. In Table 2.6 initiating likelihood frequencies are presented. In addition expert judgment and plant specific data / company data may be helpful in determining the frequencies.

Table 2.6. Typical frequency values assigned to initiating causes adapted from CCPS

Initiating event	Frequency range from literature (per year)
Pressure vessel residual failure	10^{-5} to 10^{-7}
Piping residual failure-100m-full breach	10^{-5} to 10^{-6}
Piping leak (10%section)-100m	10^{-3} to 10^{-4}
Turbine diesel engine over speed with casing breech	10^{-3} to 10^{-4}
Third party intervention (external impact by backhoe, vehicle etc.)	10^{-2} to 10^{-4}
Lightning strike	10^{-3} to 10^{-4}
Safety valve opens spuriously	10^{-2} to 10^{-4}
Cooling water failure	1 to 10^{-2}
Pump seal failure	10^{-1} to 10^{-2}
BPCS instrument loop failure	1 to 10^{-2}
Regulator failure	1 to 10^{-1}
Small external fire (aggregate causes)	10^{-1} to 10^{-2}
Large external fire (aggregate causes)	10^{-2} to 10^{-3}
LOTO (lock-out tag-out) procedure failure	10^{-3} to 10^{-4} per opportunity
Operator failure (to execute routine procedure, assuming well trained, unstressed, not fatigued)	10^{-1} to 10^{-3} per opportunity

Target risk/Tolerable risk: The Target risk/Tolerable risk is the maximum accepted value when the event occurs. The Target risk consist of 3 categories are Safety, Environment and Economic, which safety is defined in fatalities and injuries while the other categories units are usually defined in monetary impact ($).

Independent Protection layers: If protection layers satisfy the IPL criteria, they are given credit. The PFD value is then added in the worksheet. Estimates of PFDs can be found in tables in CCPS and OREDA. But company or plant specific data can also be used. Table 2.7 shows some PFDs for different IPLs. If a protection layer cannot be given credit as an IPL the PFD value entered in the worksheet is 1. Process design to reduce the likelihood of an impact event from occurring, when an initiating cause occurs, are listed first in column 5. Jacketed pipe or vessels serve as examples. BPCS is the next to be listed in column 5. If the BPCS prevents the impact event from occurring, when the initiating cause occurs, credit based on its PFD is claimed. Next item in column 5 takes credit for alarms that alert the operator and utilize operator intervention.

Additional mitigation layers with associated PFDs are the last listed in column 5. Mitigation layers are normally mechanical, structural, or procedural and may reduce the severity. However, not prevent the impact event from occurring. Examples of additional mitigation could be pressure relief devices, dikes, restricted access and evacuation procedures.

Table 2.7. PFDs for IPLs adapted from CCPS and BP

IPL	PFD
BPCS, if not associated with the initiating event being considered	10^{-1}
Operator alarm with sufficient time available to respond	10^{-1}
Relief valve	10^{-2}
Rupture disc	10^{-2}
Flame / detonation arrestors	10^{-2}
Dike / bund	10^{-2}
Underground drainage system	10^{-2}
Open vent (no valve)	10^{-2}
Fireproofing	10^{-2}
Blast-wall / bunker	10^{-3}
Identical redundant equipment	10^{-1} (max credit)
Diverse redundant equipment	10^{-1} to 10^{-2}

Intermediate event likelihood: The intermediate event is the occurrence of the end-consequence with the existing planned protection layers in place, but without the SIF under consideration. The intermediate event likelihood is the frequency per year of the occurrence of event. The intermediate event likelihood is entered in column 6. It is calculated by multiplying the initiating event likelihood (column 4) by the PFDs of the protection layers and mitigating layers (column 5). The calculated number should be in events per year, and compared with the corporate criteria. If the intermediate event likelihood is greater than the corporate criteria, additional mitigation is needed. Inherently safer design should be considered before new SIFs are introduced.

Safety integrity level (SIL): If a new SIF is needed, the SIL is calculated by dividing the corporate criteria for this target risk by the intermediate event likelihood. The result is entered in column 7.

Mitigated event likelihood: The mitigated event is the occurrence of the end-consequence with all protection layers in place, including the proposed SIF. The mitigated event likelihood is the frequency per year of the occurrence of event. The mitigated event likelihood is calculated by multiplying columns 6 and 7 and entering the result in column 10. This is step is continued until the team has calculated a mitigated event likelihood for each impact event.

CHAPTER III.

RESEARCH METHODOLOGY

The purposes of this project are to implement the Safety integrity level (SIL) Classification and to verify SIL Verification via exSILentia version 3.3.0.908. The exSILentia is the software from EXIDA company which certificated the IEC 61508/61511 standard. The cases study use Piping and instrumentation diagrams (P&IDs) to consider for execute SIL Classification and Verification, which consists of three P&IDs concern in Dehydrator vacuum unit, Seal liquid loop of separator vacuum pump and Methanol removal column (see Figure 3.1-3.3). The lists of hazards from each P&ID are the results from Hazard Identification (HAZID) or Hazard and operability study (HAZOP). The hazard lists are used to identify SIL Classification, then design the Safety instrumented system (SIS) that can meet the system requirement. The SIL Verification is used to verify the design of each Safety instrumented function (SIF) of SISs.

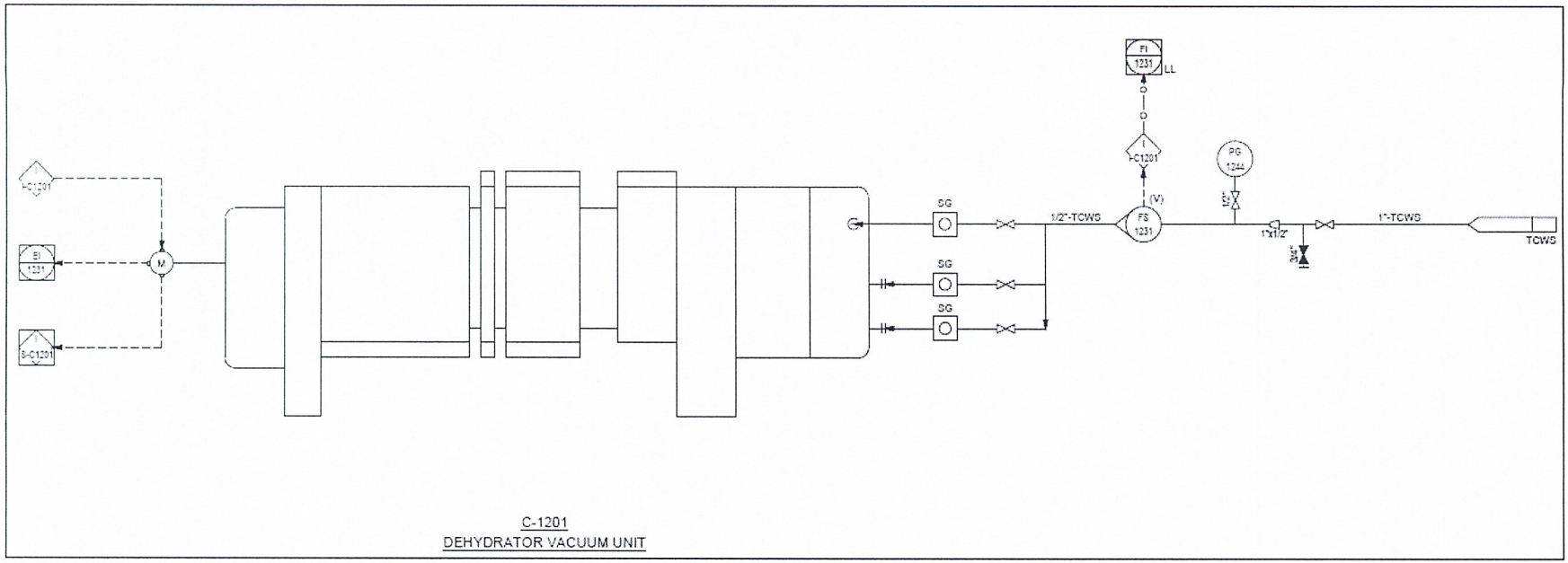

Figure 3.1. Piping and instrumentation diagram of Dehydrator vacuum unit

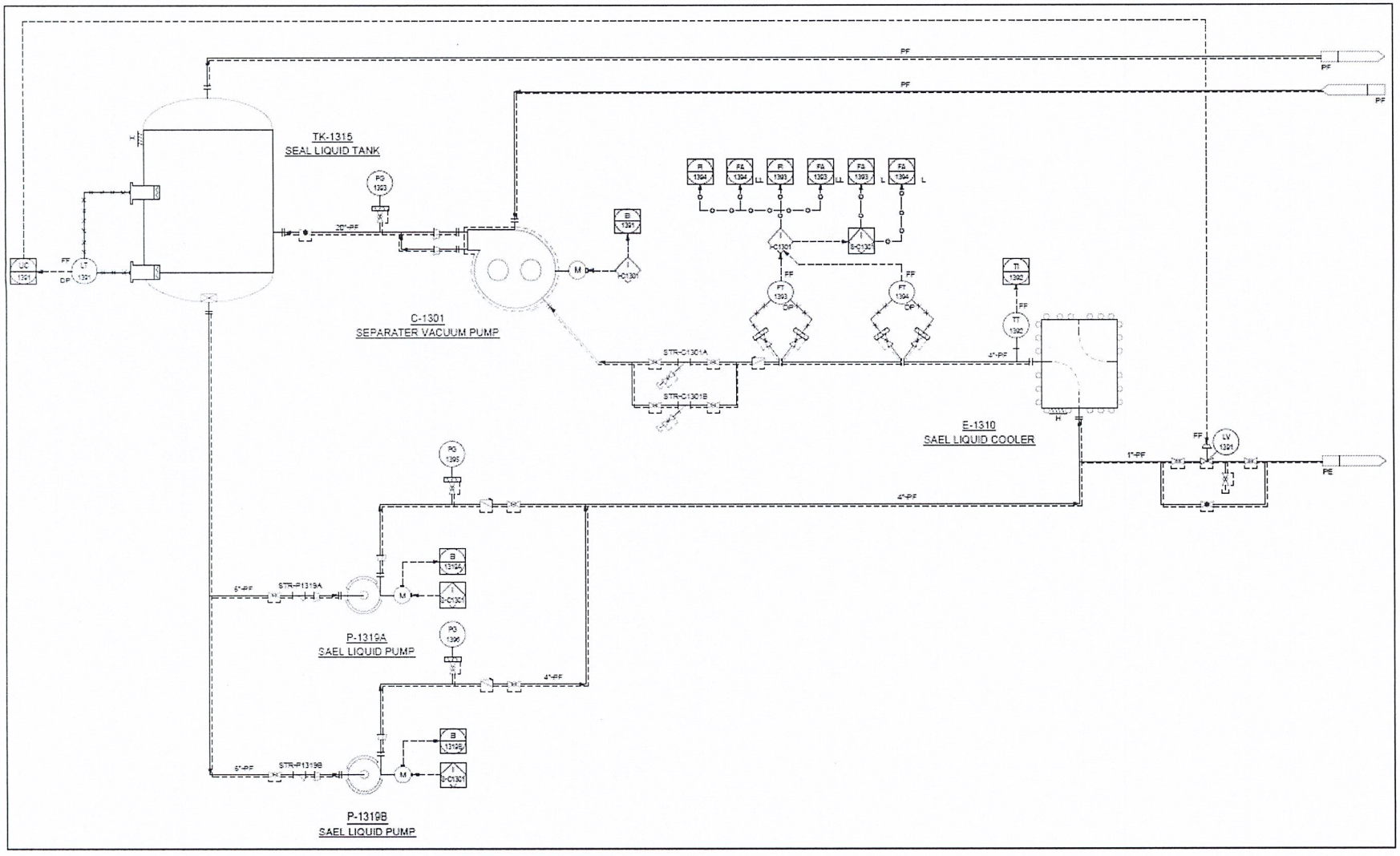

Figure 3.2. Piping and instrumentation diagram of Seal liquid loop of separator vacuum pump

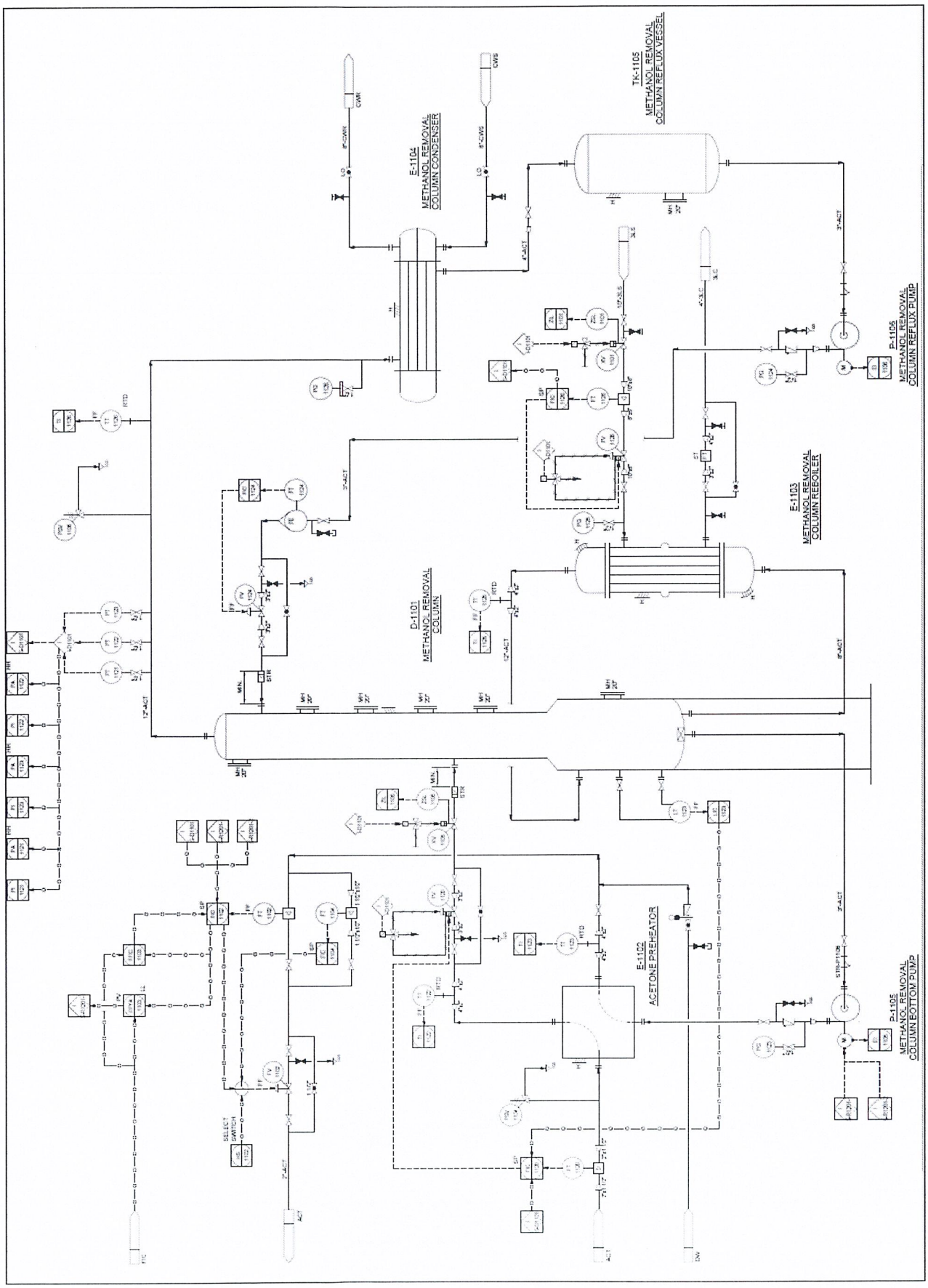

Figure 3.3. Piping and instrumentation diagram of Methanol removal column

The methods for determine SIL classification consists of Risk graph and Layer of protection analysis (LOPA) method, on the contrary SIL Verification can determine by LOPA method only. Risk graph method is qualitative method therefore the target risks are used parameters for consider SIL levels, while LOPA method is semi-quantitative method hence SIL levels are compared from SIL table (see Table 2.1) with Probability of failure on demand (PFD) or Risk reduction factor (RRF).

3.1 SIL Classification

The exSILentia is used to determine SIL classification both Risk graph and LOPA method. The purpose of SIL classification are to determine the SIL levels for each SIF and indicate the needed of SIL levels requirement for SIS.

3.1.1 Risk graph method

The Risk graph method is used to determine SIL classification by consider SIL levels from the risk factors from parameters calibration follow IEC 61511 and then compare the hazards with the risk factors for determine SIL requirement of the system.

The risk factors can classify into three categories are the personal safety (C) is quantified by the number of fatalities, the asset damage (A) is define cost of damage when the hazards occur and the environmental impact (E) concern about effect of hazard through the environment.

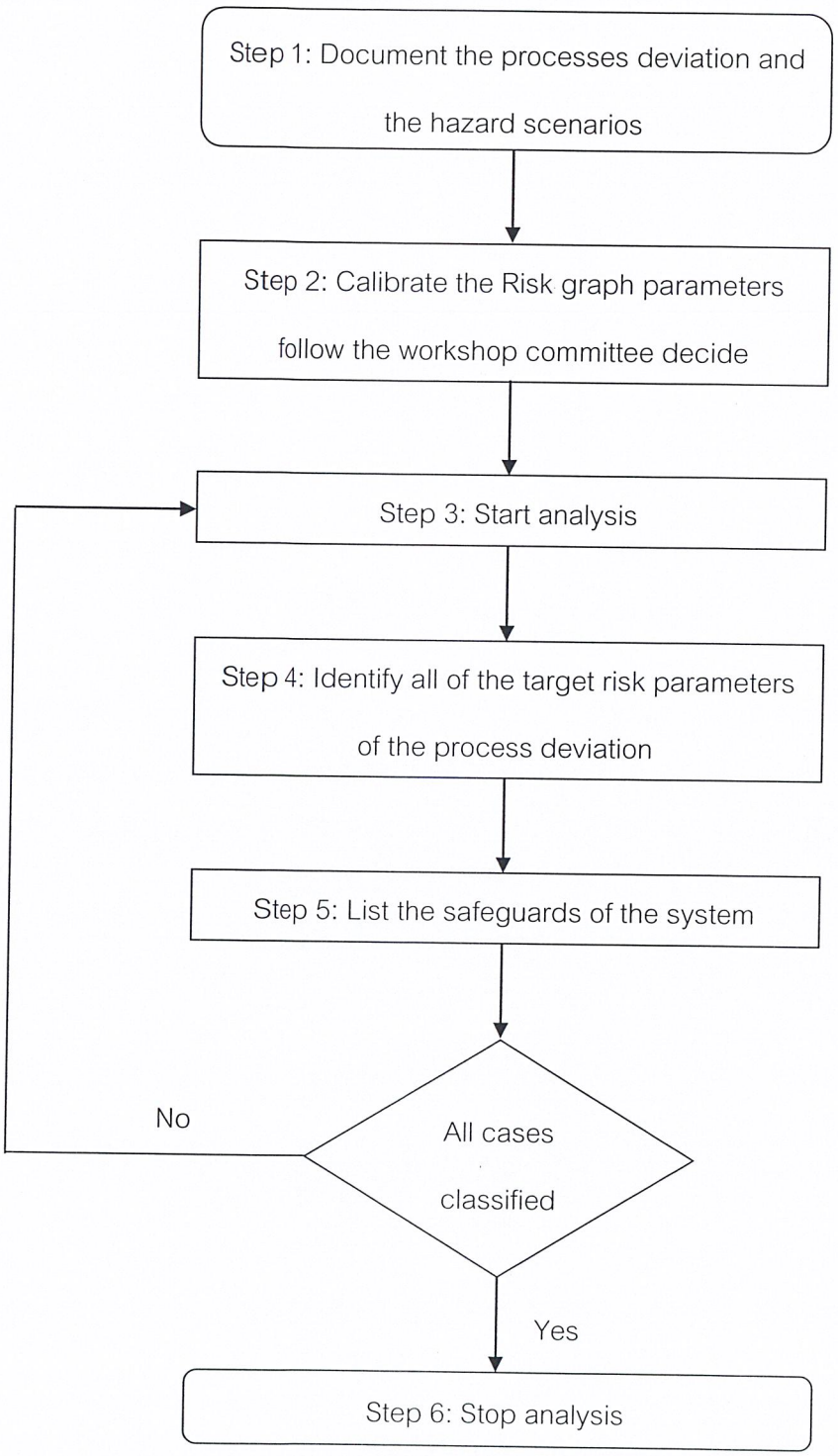

Figure 3.4. A simplified logic diagram for SIL Classification via Risk graph method

The exSILentia can calibrate the risk graph to consider in the SIL Classification by setting the risk graph option in the Tolerable risk calibration dialog. This method is category based, which based on IEC 61511 (see Figure 3.5).

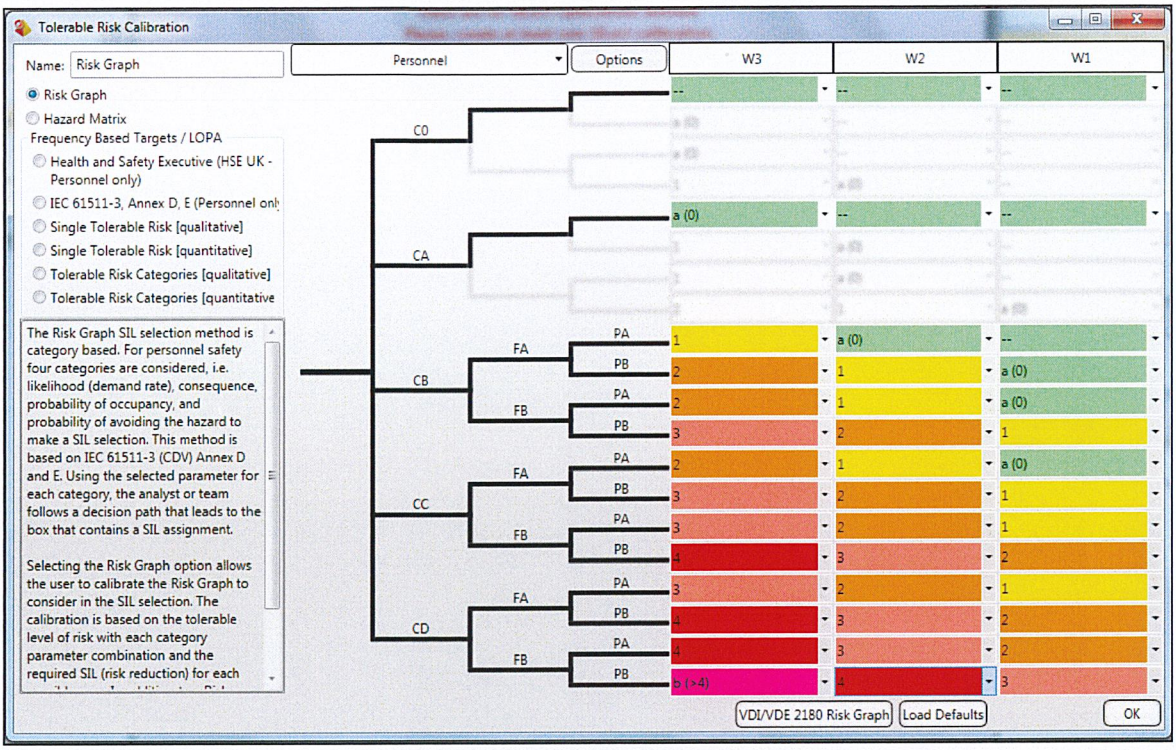

Figure 3.5. The risk graph calibration

The SIL levels required can be determine by consider and select the parameters in the SIL selection as shown in Figure 3.6. The SIL selection using the risk graph is able to specify Safe guards for protect or reduce hazard events, which indicate as Independent protection layers to account for non-SIF protection.

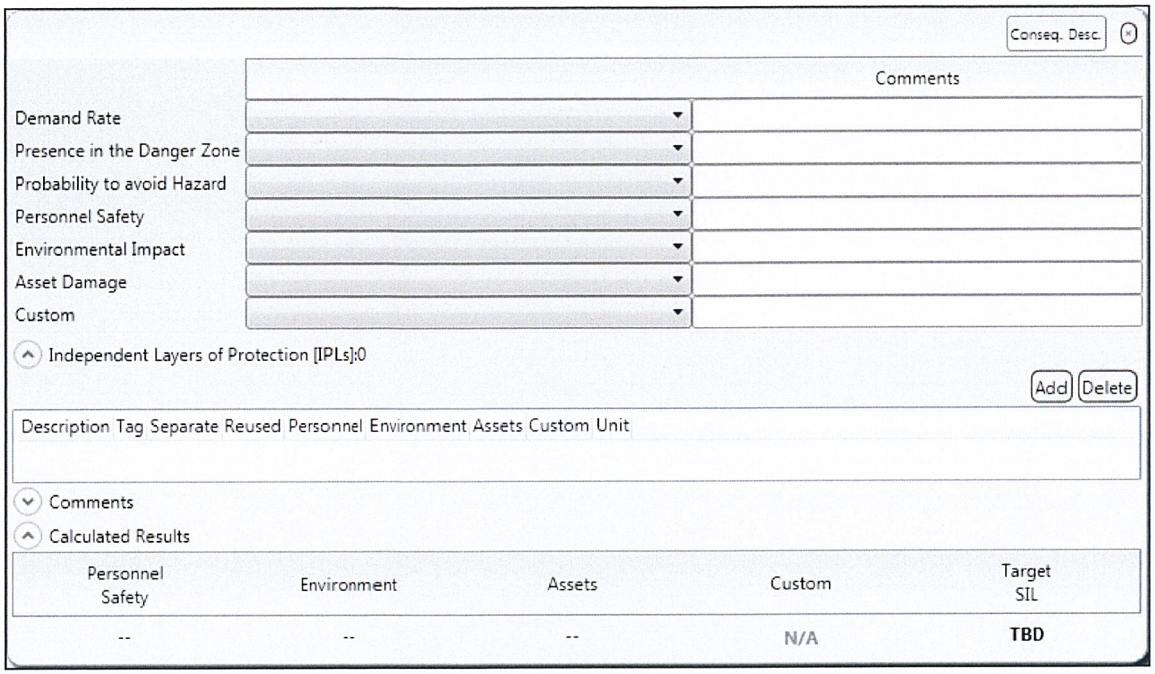

Figure 3.6. The SIL selection using risk graph

3.1.2 Layer of Protection Analysis method

The SIL classification using LOPA method is consider SIL levels from the tolerable risk parameters calibration based on IEC 61511-3 annex D and E. The parameters consist of Personnel safety, Environmental impact and Asset damage. A tolerable frequency is defined the frequency of occurring of hazardous events that can implies as six difference consequence categories are Minor, Modulate, Serious, Major, Extreme and Catastrophic.

The tolerable risk for Personnel safety is defined in fatalities and injuries per year(s). The other risk receptor units are typically defined in monetary impact ($ per year). The severity level that is associated with a risk receptor can be set (see Figure 3.8).

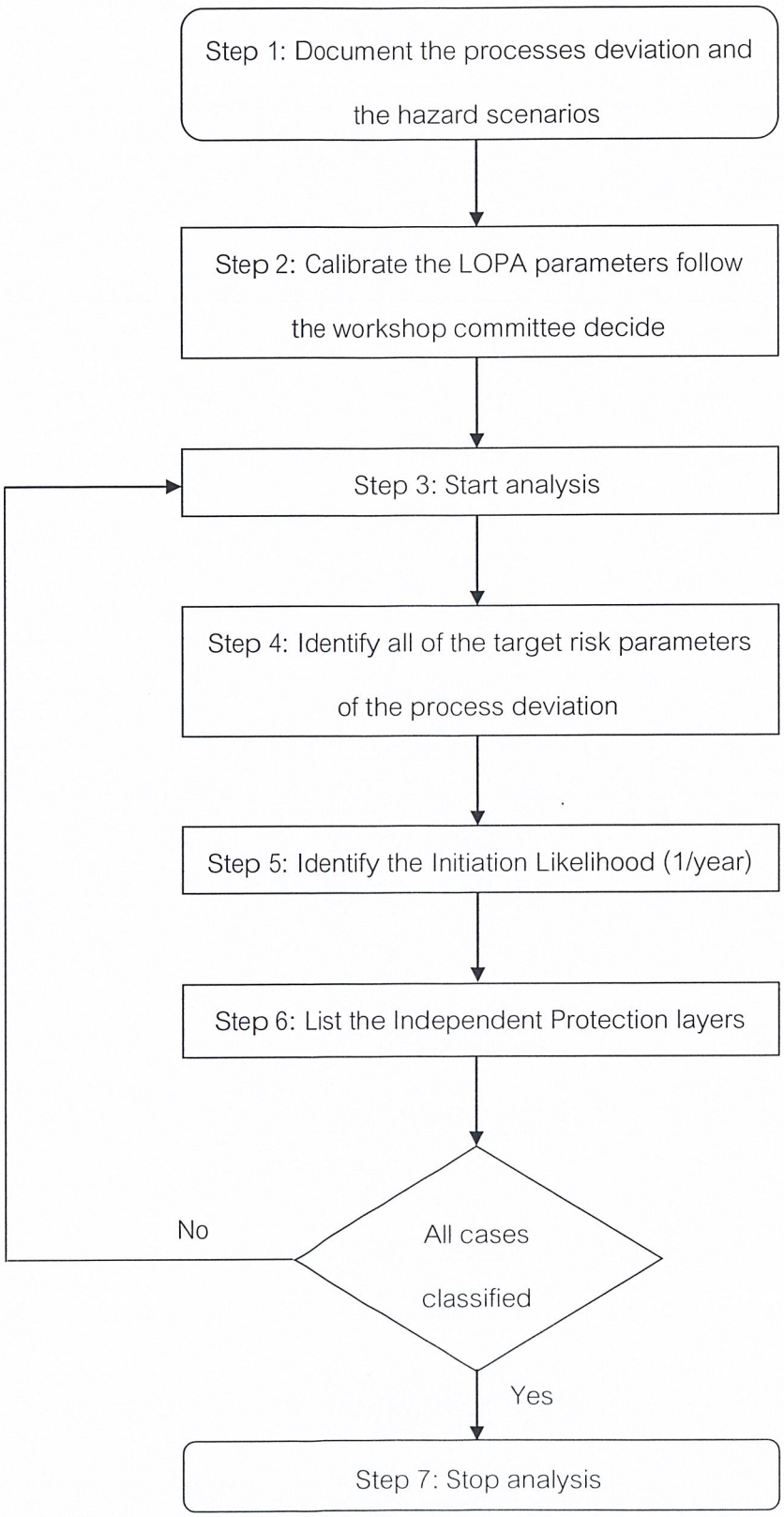

Figure 3.7. A simplified logic diagram for SIL classification via LOPA method

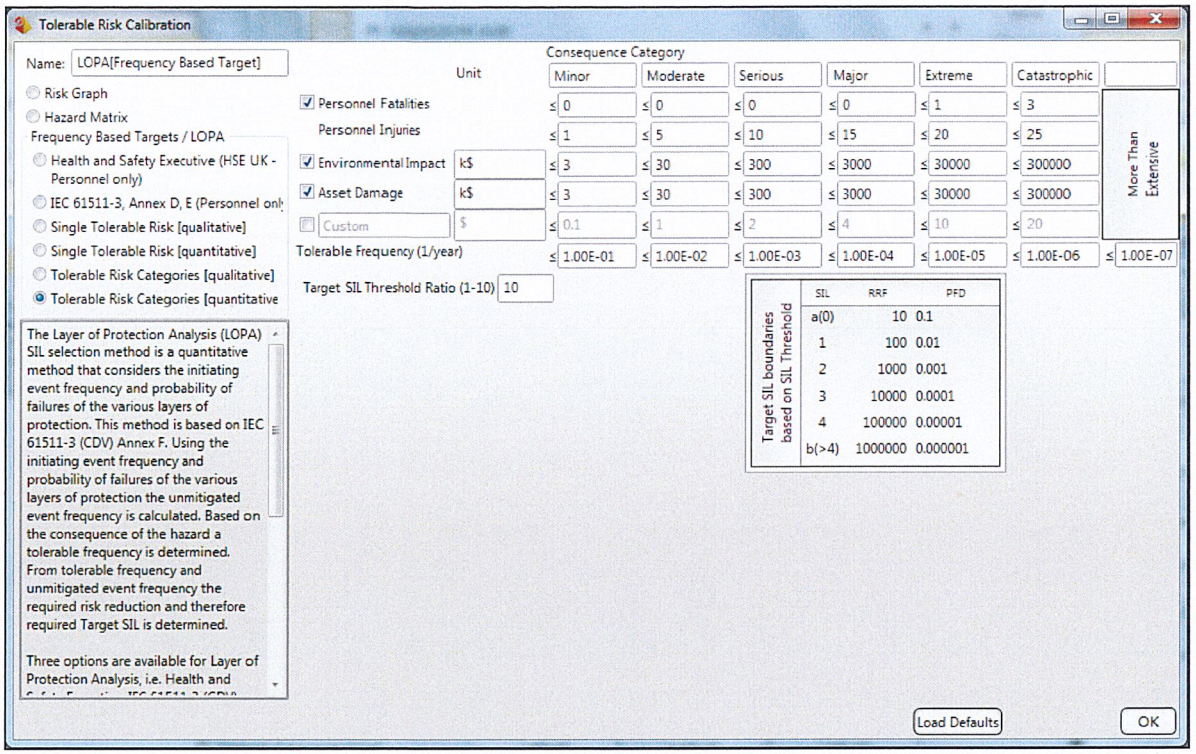

Figure 3.8. The LOPA calibration

The SIL levels required can be determine by indicate the parameters in the Severity level selections as shown in Figure 3.9. The initiation event frequency (1/year) is needed to indicate for LOPA method. The SIL selection using the LOPA is able to specify Independent protection layers (IPLs) to account for non-SIF protection.

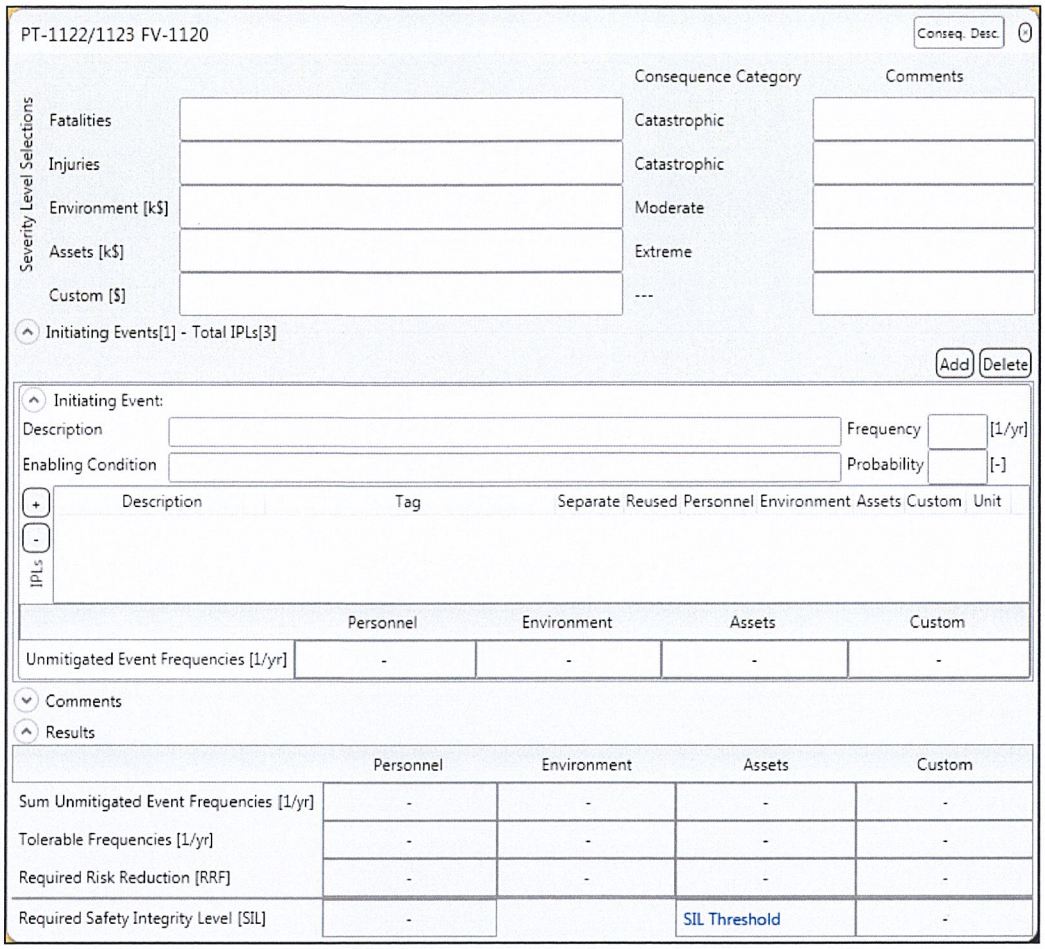

Figure 3.9. The SIL selection using LOPA

3.2 SIL Verification

The exSILentia is used to determine SIL verification with LOPA method. The purpose of SIL verification is to verify SIL from desired each SIF from SIS. Analyzing a SIS; the functional safety standards IEC 61508/61511 distinguish three distinct parts. These three parts are the Sensor Part, the Logic Solver Part, and the Final Element Part.

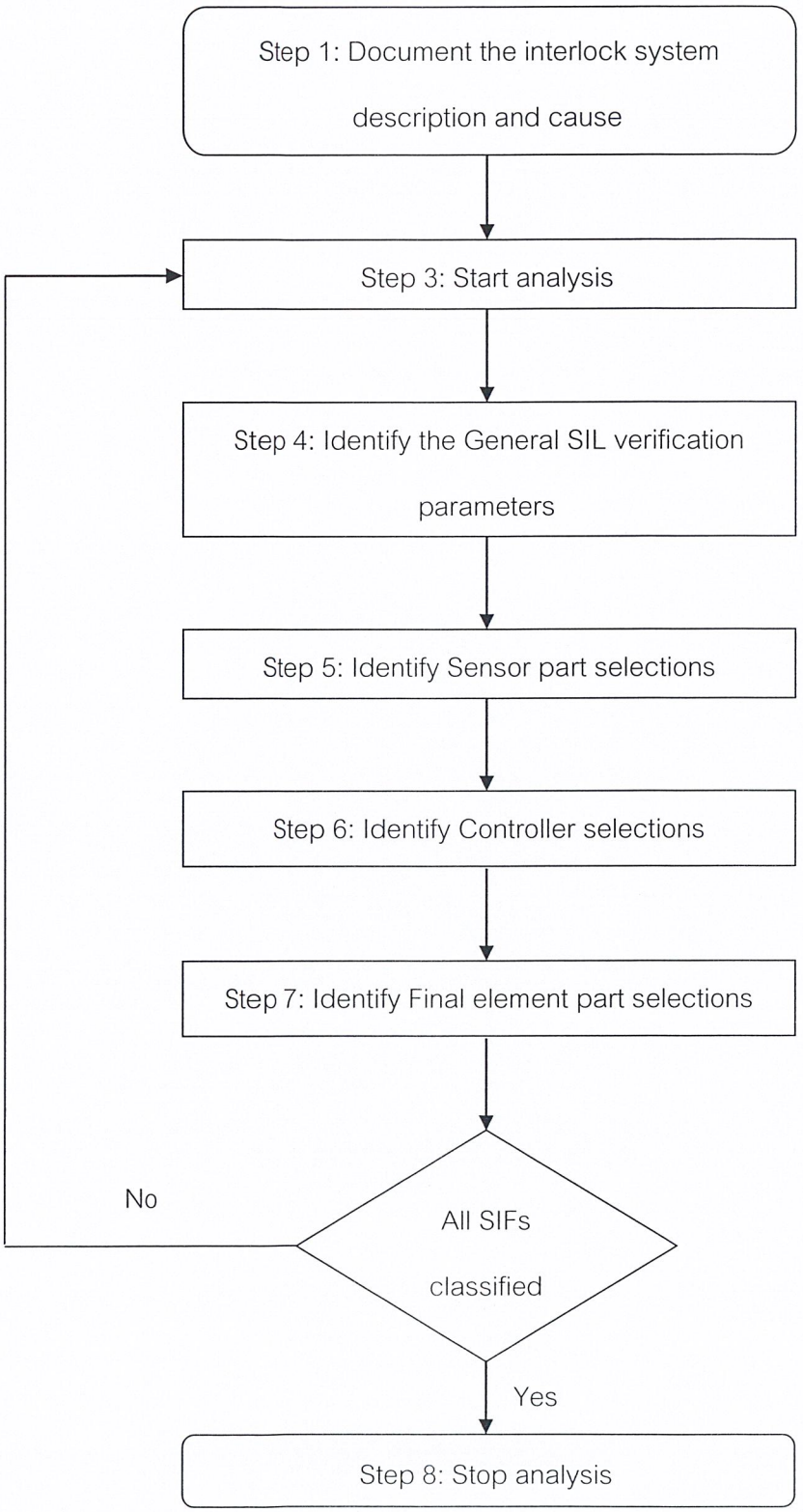

Figure 3.10. A simplified logic diagram for SIL verification via LOPA method

3.2.1 General SIL verification parameters

The general SIL verification parameters are used to indicate the condition for design SIF which consists of consists of Architectural constraints, Mission time, Startup time and Maintenance capability.

The Architectural constraints use IEC 61511 tables, the achieved SIL of the SIF will be limited to the SIL supported by SIL table (see Table 2.1 and 2.2) of IEC 61511 based on Hardware Fault Tolerance. The Mission time indicates the time period that the SIF is expected to be operational. The Startup time indicates the number of hours that takes to re-start the process after a shutdown. The Maintenance capability is considered the effectiveness of the repair processes in place at a specific site.

3.2.2 Sensor part selections

The sensor selection options are available for indicate the reliability data and Sensor information parameters. The reliability data of the specific sensor group that needed to informative are Group voting, Beta factor, Mean time to repair (MTTR), Proof test interval and Proof test coverage. The information of Sensor leg consists of Measurement type, Process connection, Sensor, Input interface module and Configuration options.

The group voting is indicating the sub-system configuration. The beta factor is the common cause factor of failures. The Mean time to repair (MTTR) indicates the expected time to repair the equipment. The Proof Test Coverage indicates the effectiveness of a proof test.

Measurement type indicates the type of sensor measure consists of temperature, flow, pressure and level. Process connection indicates connecting of sensor wire. Sensor selects the one suitable for the SIF. Input interface module is the module of sensor. Configuration options are the extra options for sensor configuration.

3.2.3 Controller selections

The controller selection options are available for indicate the parameters value. The reliability data of the controller group that needed to informative are Mean time to repair (MTTR), Proof test interval and Proof test coverage. The logic solver selects the one suitable for the SIF.

3.2.4 Final element part selections

The finial element selection options are available for indicate the reliability data and Final Element information parameters. The reliability data of the specific sensor group that needed to informative are Group voting, Beta factor, Mean time to repair (MTTR), Proof test interval and Proof test coverage. The information in the Final Element Leg consists of Interface module, Actuator-valve and Final Element.

Interface module is the module of finial element. Actuator-valve selects between separate and combination. Final Element selects the sensor suitable for the SIF.

CHAPTER IV.

RESULTS AND DISCUSSION

As the dehydrator vacuum loop shown in Figure 3.1, a hazard is damage to the vacuum unit which has cause from loss of tempered cooling water flow. The seal liquid loop shown in Figure 3.2, seal liquid is used to prevent leakage of separator vacuum pump for seal at stationary part of vacuum pump the leakage of pump can occur explosion because the process fluid in rotating part of pump is contain Hydrocarbon which inflammable, the three possible causes are loss of flow of liquid ring sealant, strainer or valve closed and failure of liquid indicator control. The Methanol removal column loop shown in Figure 3.3 is used to separate Methanol from Acetone in removal column, the hazards can be occur when the vapor pressure of removal column is high then pipe or equipment rupture, loss of containment of flammable acetone vapor and liquid, serious explosion from 5 possible causes are failure of level transmitter which effect to flow control valve of feed to the removal column fully open, loss of condenser cooling water, loss of reflux to the removal column overflow of steam at the inlet of reboiler and block in acetone discharge.

Table 4.1. Required processes deviation and the hazard scenarios

P&ID Name	Cause	Impact Description
Dehydrator vacuum unit	Loss of tempered cooling water	Damage to the vacuum unit C-1201
Seal liquid loop of separator vacuum pump	Loss of flow of liquid, Loss of supply pump	C-1301 Pump Damage
	Loss of flow of liquid, Blockages e.g. strainer or valve closed	C-1301 Pump Damage
	Loss of fluid level in tank	C-1301 Pump Damage
Methanol removal column	Loss of control of distillation column	Pipe or equipment rupture, serious explosion and/or fire
	Loss of condenser cooling water	Pipe or equipment rupture, serious explosion and/or fire
	Loss of flow of liquid	Pipe or equipment rupture, serious explosion and/or fire
	Block in acetone discharge, Loss of Pump	Pipe or equipment rupture, serious explosion and/or fire

4.1 SIL Classification

4.1.1 Risk graph method

As shown in Figure 4.1, the example of results from SIL classification by risk graph method from exSILentia. Before the results which are SIL levels requirement has been defined, the risk parameters should be full fill in the program. For the Personnel safety, Environment impact and Asset damage are in the same category which is consequence of the hazardous event; afterwards the software will decide for the highest consequence to consider the SIL levels requirement with other risk parameters.

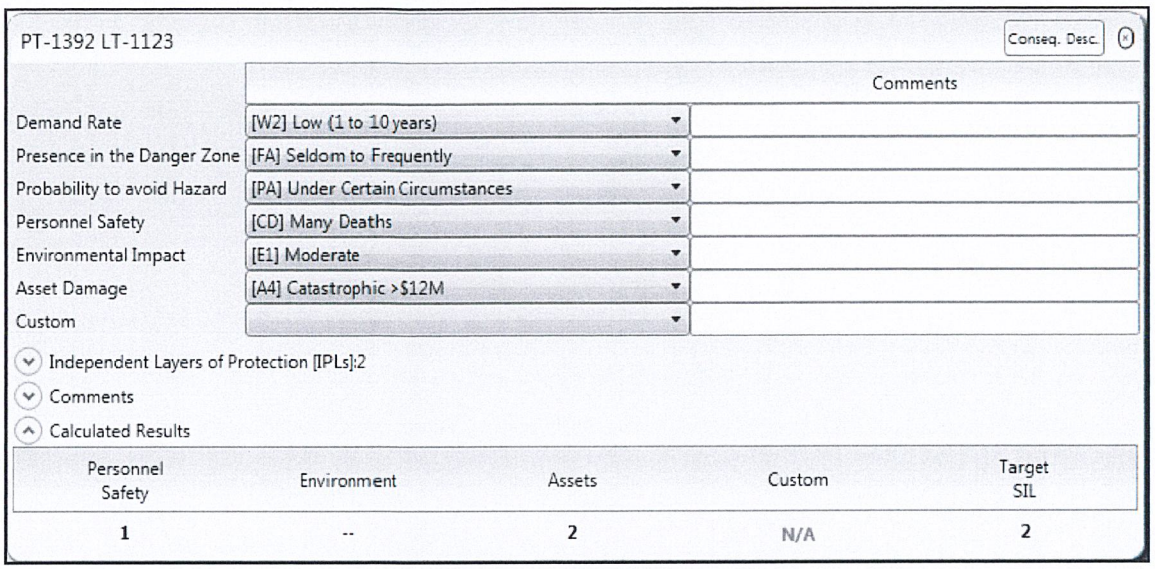

Figure 4.1. The results of Risk Graph method for SIL classification

The safe guard has directly influence to the SIL levels requirement because one safe guard that take credit (Probability of failure on demand (PFD) lower than 1) can reduce one of SIL levels requirement.

The results of SIL classification by use risk graph method from analysis three P&IDs which consists of 8 loops that has possibility to occur hazard events are shown in Table 4.2. The value of Risk reduction factor (RRF) is not available because risk graph method is qualitative analysis so cannot calculate the PFD which used to calculate RRF. The highest value of SIL levels requirement is 2 from the Methanol removal column loop so the safety functions or safety equipment are required for provide the safe state. While the Dehydrator vacuum unit loop and two of three from the Seal liquid loops of separator vacuum pump do not need any safety function or safety equipment for keep the loops from hazard.

Table 4.2. The results of SIL classification with Risk graph analysis

P&ID Name	SIF Description	Required	
		SIL	RRF
Dehydrator vacuum unit	Prevent loss of tempered cooling water flow in C-1201	-	N/A
Seal liquid loop of separator vacuum pump	Prevent loss of sealant flow to supply C-1301	-	N/A
	Prevent blockages e.g. strainer or valve of C-1301	-	N/A
	Prevent loss of fluid level in TK-1315	0	N/A
Methanol removal column	Prevent loss of level control of D-1101	2	N/A
	Prevent loss of condenser cooling water of D-1101	1	N/A
	Prevent loss of control	1	N/A
	Prevent block in Acetone discharge of D-1101	1	N/A

4.1.2 Layer of Protection Analysis method

The example of results from SIL classification by LOPA method from exSILentia is shown in Figure 4.2. The target risks should be indicating which consist of Fatalities, Injuries, Environment and Assets. For Fatalities and Injuries are the same category as safety category but from target risks calibration is demonstrated the consequence level of safety category as the same, so when selecting the target risks of safety, the software will select the highest one. Finally, the software will select the highest consequence for consider the SIL levels requirement with the frequency of the initiating causes occurring or Initiation likelihood and the PFD of protection layers.

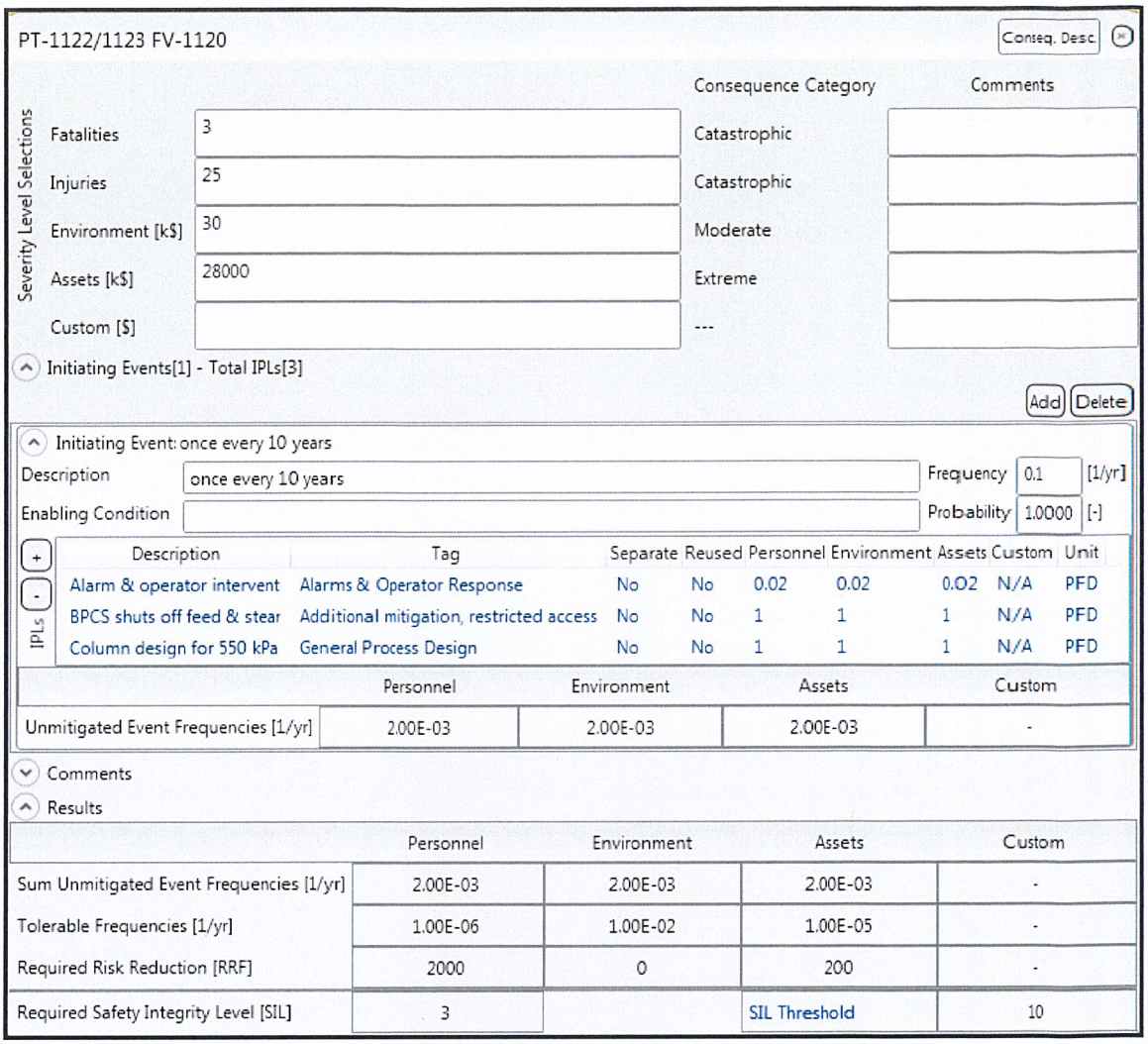

Figure 4.2. The results of LOPA method for SIL classification

In Table 4.3 are shown the results of SIL classification by use LOPA method from analysis 3 P&ID which consists of 8 loops that has possibility to occur hazard events. The results show the SIL levels requirement and RRF. For LOPA method the software calculates the value of RRF and then compare the RRF value to SIL table (see Table 2.1). The highest and lowest SIL levels requirement are the same loops via consider with risk graph method.

Table 4.3. The results of SIL classification with LOPA analysis

P&ID Name	SIF Description	Required	
		SIL	RRF
Dehydrator vacuum unit	Prevent loss of tempered cooling water flow in C-1201	1	37
Seal liquid loop of separator vacuum pump	Prevent loss of sealant flow to supply C-1301	0	7
	Prevent blockages e.g. strainer or valve of C-1301	1	40
	Prevent loss of fluid level in TK-1315	2	200
Methanol removal column	Prevent loss of level control of D-1101	3	2000
	Prevent loss of condenser cooling water of D-1101	0	3
	Prevent loss of control	2	200
	Prevent block in Acetone discharge of D-1101	2	400

LOPA method can understandable obviously more than risk graph method because this method uses numerical to identify the possibility to occur hazard events. The RRF value can be used to compare the violence level of hazard which equal to SIL levels requirement.

The results of SIL classification (SIL levels requirement and RRF) use LOPA method will be used as minimum requirement in SIL verification.

4.2 SIL Verification

The international standards IEC 61508 and 61511 have the difference method to consider Architectural constraints for IEC 61508 the achieved SIL of the SIF will be limited to the SIL supported by based on Equipment type, Safe Failure Fraction (SFF) and Hardware Fault Tolerance (HFT) but IEC 61511 the achieved SIL of the SIF will be limited to the SIL supported by based on Hardware Fault Tolerance and Prior Use considerations, which has more strictness more than IEC 61508.

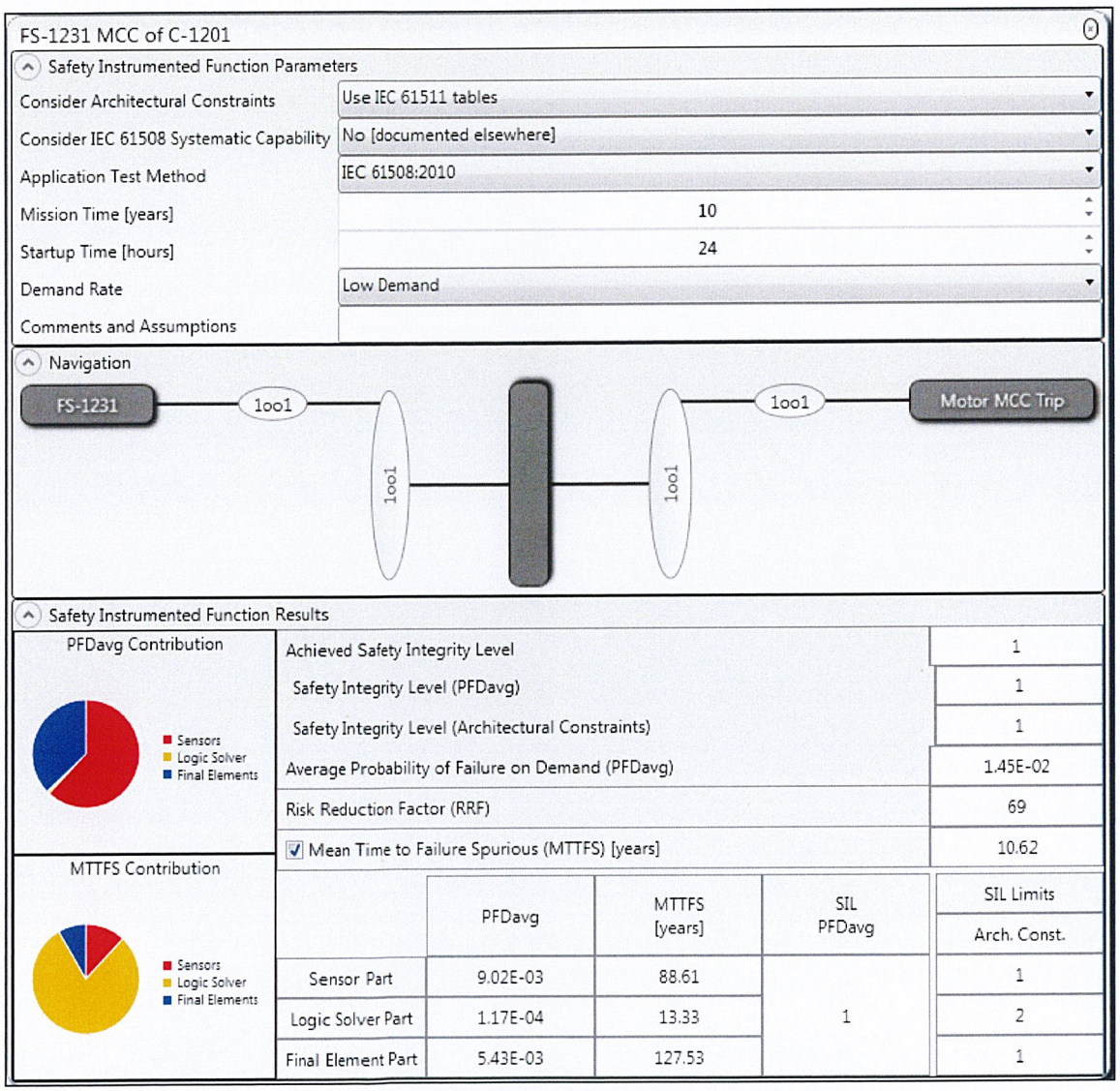

Figure 4.3. The results of LOPA method

The example of results from desired Safety instrumented function (SIF) by the software is shown in Figure 4.3. The results are calculated from the PFD configuration of Safety instrumented system (SIS) which consists of sensor(s), controller(s) and final element(s). The software consider two requirements are Quantitative requirements and Architectural constrains for define RRF, PFD and SIL levels achievement.

The SIL Verification results which is SIL levels requirement consider both PFD_{Avg} and Architectural constrains of the system. The SIL levels of PDF_{Avg} can be taken from compare the PDF_{Avg} of the system with the SIL table (see Table 2.1). The SIL levels of Architectural constrains depend on HFT which resulting from system configurations and SFF (see Table 2.2 and 2.3). If the constrain is not match for example SIL levels of PDF_{Avg} is 2 and SIL levels of Architectural constrains is 3 the software will be select the worst case which is lowest one.

The lists of SIL verification results are shown in Table 4.4. From the comparison of the results between SIL classification by using risk graph method and LOPA method (see Table 4.2 and 4.3) found that SISs, which containing appropriate SIFs of each unit, can be protect or reduce the possibility to occur hazard events because all of the values of SIL levels achievement from desired SIS are equal of higher than the SIL levels requirement from SIL classification both risk graph and LOPA method.

Table 4.4. The results of SIL verification with LOPA analysis

P&ID Name	SIF Description	Achieved	
		SIL	RRF
Dehydrator vacuum unit	Prevent loss of tempered cooling water flow in C-1201	1	63
Seal liquid loop of separator vacuum pump	Prevent loss of sealant flow to supply C-1301	-	-
	Prevent blockages e.g. strainer or valve of C-1301	1	63
	Prevent loss of fluid level in TK-1315	2	308
Removal column	Prevent loss of level control of D-1101	3	2238
	Prevent loss of condenser cooling water of D-1101	-	-
	Prevent loss of control	2	310
	Prevent block in Acetone discharge of D-1101	2	320

If considering just only LOPA method, the value of RRF can be express or compare the safety of system between requirement and achievement. The values of RRF from SIL verification in Table 4.4 compare with the value of RRF from SIL classification in Table 4.3 found that the values of RRF from achievements are higher than requirements, hence can be indicate that SISs of all safety systems can be protect or reduce the possibility to occur hazard events.

CHAPTER V.

CONCLUSION

For Risk graph method, the Safety Integrity Level (SIL) levels required is considered by using four parameters are Consequence (Safety, Environment and Asset), Occupancy, and Possibility of avoidance and Demand rate. The SIL levels required can be decreased one by adding one safeguard. For Layers of Protection Analysis (LOPA) method, the SIL levels required is calculated by using the value of highest consequence target risk divided by Event Likelihood and compare the answer with SIL table. It can be decreased by using higher standard of safety equipment which has lower failure value.

The SIL levels achieved is considered by the Safety Instrumented Function of Safety Instrumented System (Sensor, Controller, Final element), which depend on Probability of Failure on Demand requirement and Architectural constraints. The SIL levels achieved can meet all SIL levels required from SIL classification of LOPA method.

SUGGESTIONS

From the results of SIL Verification in exSILentia software, the safety equipment that used for SIL determination are all Generic equipment which have not good properties compared with the others brand name equipment that have some special properties in each device. So, the brand name equipment is recommended for the plant design situation and also the cost of the brand name equipment can be determined. The owner can set an agreement with the providers for make the cost-effective safety equipment.

REFERENCES

ANSI/ISA 84.00.01-2004 (IEC 61511 Mod). Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels. The International Society of Automation, North Carolina, USA, 2004.

CCPS. Layer of Protection Analysis. Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, 2001.

IEC 61508. Functional Safety of Electrical / Electronic / Programmable Electronic Safety related systems, Parts 1-7, 2nd Edition. International Electro technical Commission, Geneva, Switzerland, 2010.

IEC 61511. Functional Safety - Safety Instrumented systems for the Process Industry Sector - Part 1: Framework, definitions, system, hardware and software requirements. International Electro technical Commission. Geneva, Switzerland, 2003.

OREDA (Offshore Reliability Data). 4th Edition: SINTEF Industrial Management; 2002.

William M.Goble. Control Systems Safety Evaluation and Reliability. 2nd Edition: Instrument Society of America; 1998.

APPENDIX

APPENDIX A

SIL VERIFICATION GENERAL ASSUMPTIONS

The specific data of failure rate are quantified using the following reliability data handbooks: OREDA 92, OREDA 97, OREDA 2002, OREDA 2009, SERH 2009.

- Consider Architecture constrains per IEC 61511 tables.
- Not consider IEC 61508 Systematic capability.
- Application test method is use IEC 61508:2010.
- Overall Mission times for SIF are taken as 10 years.
- Start-up time of the SIF is taken as 24 hours.
- Maintenance capability of initiators, logic solver and final elements are all taken as 90%.
- For redundant architecture, β -factor is set at 0.05.
- MTTR of initiators, logic solver and final elements are taken 8, 24 and 24 hours respectively.
- Test interval for initiators, logic solver and final elements are all taken as 48 months.
- Proof Test Coverage (PTC) for initiators, logic solver and final elements are all taken as 90%.
- Use Generic transmitters with SFF between 60% to 90% are used in the calculation, and are regarded as Type B instruments.

APPENDIX B

FAILURE RATE RAW DATA OF GENERIC TRANSMITTERS

EQUIPMENT ITEM: Generic Flow Transmitter - Coriolis Meter				DATA VERSION: 2006.2.02
GENERAL INFORMATION				SERH
MANUFACTURER	Generic Equipment			
MODEL	~~~			
MEASUREMENT TYPE	Flow - Mass: Coriolis			
ANALOG / DIGITAL	Analog	HARDWARE FAULT TOLERANCE	0	
ARCHITECTURE TYPE	B	SIL CAPABILITY	N/A	
ASSESSMENT	N/A	BY	N/A	
DATA SOURCE	exida Comprehensive Analysis			
USEFUL LIFE	10 years			
REMARKS	None			

FAILURE RATE DATA	PER 10^9 HOURS [FITS]
FAIL LOW	500
FAIL HIGH	100
FAIL DETECTED	800
FAIL DANGEROUS DETECTED	
FAIL DANGEROUS UNDETECTED	900
FAIL SAFE DETECTED	
FAIL SAFE UNDETECTED	
FAIL ANNUNCIATION DETECTED	
FAIL ANNUNCIATION UNDETECTED	
FAIL NO EFFECT	200
SFF [%]	64.0

Figure B.1. Generic Flow Transmitter - Coriolis Meter raw data

Equipment Item: Generic DP/ Pressure Transmitter				Data Version: 2006.2.02
General Information				
Manufacturer	Generic Equipment			
Model	~~~			
Measurement Type	Pressure			
Analog / Digital	Analog	Hardware Fault Tolerance		0
Architecture Type	B	SIL Capability		N/A
Assessment	N/A	By	N/A	
Data Source	exida Comprehensive Analysis			
Useful Life	10 years			
Remarks	Generic Smart DP / Pressure Transmitter.			

Failure Rate Data	Per 10^9 Hours [FITs]	
Fail Low	400	
Fail High	150	
Fail Detected	150	
Fail Dangerous Detected		
Fail Dangerous Undetected	600	
Fail Safe Detected		
Fail Safe Undetected		
Fail Annunciation Detected		
Fail Annunciation Undetected		
Fail No Effect	200	
SFF [%]	60.0	

Figure B.2. Generic DP (Pressure Transmitter) raw data

Equipment Item: Generic SIL2 Certified PLC				Data Version: 2006.2.02
General Information				
Manufacturer	Generic Equipment			
Model	~~~			
Logic Solver Type	PLC	Beta Factor [%]		0
Configuration	1oo1D	Hardware Fault Tolerance		0
Architecture Type	B	SIL Capability		2
Assessment	IEC 61508 Certification	By	N/A	
Data Source	exida Comprehensive Analysis			
Useful Life	10 years			
Remarks	None			

Failure Rate Data		Per 10^9 Hours [FITs]						
	Model #	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	λ^{AD}	λ^{AU}	λ^{NE}
Main Processor	N/A	6930	70	2850	150			
Power Supply	N/A	2250		250				
Analog In Module	N/A	950	50	900	100			
Analog In Channel		48	3	48	3			
Digital In Module	N/A	570	30	380	20			
Digital In Channel		124	7	67	4			
Analog Out Module	N/A	356	19	119	6			
Analog Out Channel				95	5			
Digital Out Low Module	N/A	792	8	190	10			
Digital Out Low Channel		139	1	57	3			
Digital Out High Module	N/A	792	8	190	10			
Digital Out High Channel		277	3	114	6			

Figure B.3. Generic SIL2 Logic solver raw data

Equipment Item				Data Version
Generic SIL3 Certified PLC				2006.2.02
General Information				
Manufacturer	Generic Equipment			
Model	~~~			
Logic Solver Type	PLC	Beta Factor [%]		2
Configuration	1oo2D	Hardware Fault Tolerance		1
Architecture Type	B	SIL Capability		3
Assessment	IEC 61508 Certification	By	N/A	
Data Source	exida Comprehensive Analysis			
Useful Life	10 years			
Remarks	None			

Failure Rate Data		Per 10^9 Hours [FITs]						
	Model #	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	λ^{AD}	λ^{AU}	λ^{NE}
Main Processor	N/A	7425	75	2375	125			
Power Supply	N/A	2250		250				
Analog In Module	N/A	990	10	900	100			
Analog In Channel		48	3	48	3			
Digital In Module	N/A	570	30	380	20			
Digital In Channel		124	7	67	4			
Analog Out Module	N/A	1425	75	475	25			
Analog Out Channel				95	5			
Digital Out Low Module	N/A	760	40	190	10			
Digital Out Low Channel		139	1	57	3			
Digital Out High Module	N/A	760	40	190	10			
Digital Out High Channel		277	3	114	6			

Figure B.4. Generic SIL3 Logic solver raw data

Equipment Item: Generic Relay				Data Version: 2006.2.02
General Information				
Manufacturer	Generic Equipment			
Model	~~~			
Annunciation Type	Relay			
Analog / Digital	Digital Low	Hardware Fault Tolerance	0	
Architecture Type	A	SIL Capability	N/A	
Assessment	N/A	By	N/A	
Data Source	exida Comprehensive Analysis			
Useful Life	10 years			
Remarks	None			

Failure Rate Data	Per 10^9 Hours [FITs]	
Fail Dangerous Detected		
Fail Dangerous Undetected	600	
Fail Safe Detected		
Fail Safe Undetected	900	
Fail Annunciation Detected		
Fail Annunciation Undetected		
Fail No Effect		
SFF [%]	60.0	

Figure B.5. Generic Relay raw data

Equipment Item				Data Version
Generic Air Operated Ball Valve, Hard Seat				2012.3.02
General Information				
Manufacturer	Generic Equipment			
Model	~~~			
Actuator Type	Spring-Return, Air-To-Open			
Valve Type	Ball Valve	Hardware Fault Tolerance	0	
Architecture Type	A	SIL Capability	N/A	
Assessment	N/A	By	N/A	
Data Source	exida Comprehensive Analysis			
Useful Life	10 years			
Remarks	None			

Failure Rate Data — Per 10^9 Hours [FITs]

Clean Service	Close on Trip						Open on Trip		
	Full Stroke			Tight Shutoff					
	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn
Fail Dangerous Detected		680	---		680	---		900	---
Fail Dangerous Undetected	1480	800	---	3180	2500	---	1750	850	---
Fail Safe Detected		500	---		500	---		500	---
Fail Safe Undetected	500		---	500		---	500		---
Fail Annunciation Detected			---			---			---
Fail Annunciation Undetected			---			---			---
Fail No Effect			---			---			---
SFF [%]	25.3	59.6	---	13.6	32.1	---	22.2	62.2	---

Severe Service	Close on Trip						Open on Trip		
	Full Stroke			Tight Shutoff					
	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn
Fail Dangerous Detected		925	---		925	---		1080	---
Fail Dangerous Undetected	2050	1130	---	4750	3830	---	1960	880	---
Fail Safe Detected		500	---		500	---		500	---
Fail Safe Undetected	500		---	500		---	500		---
Fail Annunciation Detected			---			---			---
Fail Annunciation Undetected			---			---			---
Fail No Effect			---			---			---
SFF [%]	19.6	55.8	---	9.5	27.1	---	20.3	64.2	---

Figure B.6. Generic Air operated ball valve, hard seat raw data

Equipment Item				Data Version
Generic Control Valve				2012.3.02
General Information				
Manufacturer	Generic Equipment			
Model	~~~			
Actuator Type	Spring-Return			
Valve Type	Globe Valve	Hardware Fault Tolerance	0	
Architecture Type	A	SIL Capability	N/A	
Assessment	N/A	By	N/A	
Data Source	exida Comprehensive Analysis			
Useful Life	10 years			
Remarks	None			

Failure Rate Data — Per 10^9 Hours [FITs]

Clean Service	Close on Trip						Open on Trip		
	Full Stroke			Tight Shutoff					
	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn
Fail Dangerous Detected			---	---	---	---	---	---	---
Fail Dangerous Undetected	1150	1150	---	---	---	---	---	---	---
Fail Safe Detected			---	---	---	---	---	---	---
Fail Safe Undetected	500	500	---	---	---	---	---	---	---
Fail Annunciation Detected			---	---	---	---	---	---	---
Fail Annunciation Undetected			---	---	---	---	---	---	---
Fail No Effect			---	---	---	---	---	---	---
SFF [%]	30.3	30.3	---	---	---	---	---	---	---

Severe Service	Close on Trip						Open on Trip		
	Full Stroke			Tight Shutoff					
	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn	Normal	PVST Stat	PVST Dyn
Fail Dangerous Detected	---	---	---	---	---	---	---	---	---
Fail Dangerous Undetected	---	---	---	---	---	---	---	---	---
Fail Safe Detected	---	---	---	---	---	---	---	---	---
Fail Safe Undetected	---	---	---	---	---	---	---	---	---
Fail Annunciation Detected	---	---	---	---	---	---	---	---	---
Fail Annunciation Undetected	---	---	---	---	---	---	---	---	---
Fail No Effect	---	---	---	---	---	---	---	---	---
SFF [%]	---	---	---	---	---	---	---	---	---

Figure B.7. Generic Control valve raw data

APPENDIX C

FAILURE RATE RAW DATA OF EACH CASE

Table C.1. The failure rate raw data of dehydrator vacuum loop

Impact Event Description	Initiating Cause	Initiating Frequency	Target Risk			Layers of Protection			
			Safety	Environment	Economic	General Process Design	Basic Process Control System	Alarms & Operator Response	Additional mitigation, restricted access
		/Year			$				
Damage to the vacuum unit C-1201	Loss of tempered cooling water flow (P-1911A/B)	one pump run and one stand-by (P-1911A/B),MTTR is one month	None	Minor	6,000,000	-	-	Low Flow Alarm (FAL-1231) , Low Pressure Alarm (PI-1931) & DW pump low pressure and flow alarm	-
		3.7×10^{-3}	1×10^{-1}	1×10^{-1}	1×10^{-5}	-	-	1	-

Table C.2. The failure rate raw data of seal liquid loop

Impact Event Description	Initiating Cause	Initiating Frequency	Target Risk			Layers of Protection			
			Safety	Environment	Economic	General Process Design	Basic Process Control System	Alarms & Operator Response	Additional mitigation, restricted access
		/Year			$				
C-1301 Pump Damage	Loss of flow of liquid ring sealant FT-1393(1) Loss of supply pump	One pump running one stand-by (P-1319A/B)	None	Minor	6,000,000	Duty/stand-by pumps with auto start (does not help for blockage or loss of level),Dual strainers on system	-	Alarms (flow, level) and operator intervention, low flow alarm (FT-1393), low level alarm (LT-1391) of TK-1315, Pump trip alarm status.	-
		3.7×10^{-3}	1×10^{-1}	1×10^{-1}	1×10^{-5}	1	-	2×10^{-2}	-
C-1301 Pump Damage	Loss of flow of liquid ring sealant FT-1393(2) Blockages e.g. strainer or valve closed, Two strainer are available, one run and one stand by.	once in every fifty years	None	Minor	6,000,000	Duty/stand-by pumps with auto start (does not help for blockage or loss of level),Dual strainers on system	-	Alarms (flow, level) and operator intervention, low flow alarm (FT-1393), low level alarm (LT-1391) of TK-1315, Pump trip alarm status.	-
		2×10^{-2}	1×10^{-1}	1×10^{-1}	1×10^{-5}	1	-	2×10^{-2}	-
C-1301 Pump Damage	Loss of fluid level in TK-1315, failure of control loop LIC-1391, cause to full open LV-1391.	Once in every 10 years	None	Minor	6,000,000	Duty/stand-by pumps with auto start (does not help for blockage or loss of level),Dual strainers on system	-	Alarms (flow, level) and operator intervention, low flow alarm (FT-1393), low level alarm (LT-1391) of TK-1315, Pump trip alarm status.	-
		1×10^{-1}	1×10^{-1}	1×10^{-1}	1×10^{-5}	1	-	2×10^{-2}	-

Table C.3. The failure rate raw data of Methanol removal column loop

Impact Event Description	Initiating Cause	Initiating Frequency	Target Risk			Layers of Protection			
			Safety	Environment	Economic	General Process Design	Basic Process Control System	Alarms & Operator Response	Additional mitigation, restricted access
		/Year			$				
Pipe or equipment rupture, loss of containment of flammable acetone vapor and liquid, serious explosion and/or fire	Loss of control of distillation column (multiple causes), Loss of LIC-1123 level control loop, FV-1120 fully open, vessel in high level in column	once every 10 years	Multiple fatalities	Moderate	28,000,000	Column design for 550 kPa g	-	Alarm & operator intervention, High Pressure Alarm (PAHH-1122 & 1123 from safety system), High Level Alarm (LT-1123)	BPCS shuts off feed & steam control valves – provides protection in some failure modes
		1×10^{-1}	1×10^{-6}	1×10^{-2}	1×10^{-6}	1	-	2×10^{-2}	1
Pipe or equipment rupture, loss of containment of flammable acetone vapor and liquid, serious explosion and/or fire	Loss of condenser cooling water	Two pump running and one stand-by, Assuming MTTR 1 month of pump	Multiple fatalities	Moderate	28,000,000	Column design for 550 kPa g	-	Alarm & operator intervention, High Pressure Alarm (PAHH-1122 & 1123 from safety system), Total plant shutdown	Plant shutdown by losing of cooling water, (2 out of 3)
		1.7×10^{-3}	1×10^{-6}	1×10^{-2}	1×10^{-6}	1	-	2×10^{-2}	1×10^{-1}
Pipe or equipment rupture, loss of containment of flammable acetone vapor and liquid, serious explosion and/or fire	Loss of reflux by pumping of P-1106, Flow control loop failure FIC-1124 closing.	once every 5 years	Multiple fatalities	Moderate	28,000,000	Column design for 550 kPa g	-	Alarm & operator intervention, Pump Status (P-1106), Low Flow Alarm (FT-1124)	BPCS shuts off feed & steam control valves – provides protection in some failure modes
		2×10^{-1}	1×10^{-6}	1×10^{-2}	1×10^{-5}	1	-	2×10^{-2}	1

Table C.3. The failure rate raw data of Methanol removal column loop (cont.)

Impact Event Description	Initiating Cause	Initiating Frequency	Target Risk			Layers of Protection			
			Safety	Environment	Economic	General Process Design	Basic Process Control System	Alarms & Operator Response	Additional mitigation, restricted access
		/Year			$				
Pipe or equipment rupture, loss of containment of flammable acetone vapor and liquid, serious explosion and/or fire	(4) Loss of FIC-1126 control loop cause in FV-1126 fully open.	once every 10 years	Multiple fatalities	Moderate	28,000,000	Column design for 550 kPa g	Level Control (FV-1120) would trend to close.	Alarm & operator intervention, High Temperature (TI-1125 & 1124), High Pressure (PI-1115) , High Level Alarm (LT-1123)	BPCS shuts off feed & steam control valves – provides protection in some failure modes
		1×10^{-1}	1×10^{-6}	1×10^{-2}	1×10^{-5}	1	1×10^{-1}	2×10^{-2}	1
Pipe or equipment rupture, loss of containment of flammable acetone vapor and liquid, serious explosion and/or fire	(5) Block in acetone discharge, Loss of Pump (P-1105), Block in the STR -P1105, Loss of control loop FIC-1102 to close.	once every 5 years	Multiple fatalities	Moderate	28,000,000	Column design for 550 kPa g	Level Control (FV-1120) would trend to close.	Alarm & operator intervention, High Pressure (PI-1115) , High Level Alarm (LT-1123)	BPCS shuts off feed & steam control valves – provides protection in some failure modes
		2×10^{-1}	1×10^{-6}	1×10^{-2}	1×10^{-5}	1	1×10^{-1}	2×10^{-2}	1

APPENDIX D

EXAMPLE OF CALCULATION

1. Sensor part

Type : Generic Flow Transmitter - Coriolis Meter raw data

System configuration : 1oo1

$$TI = 8760 \text{ hours}$$

$$\lambda_{DU} = 900 \times 10^{-9} \text{ 1/hours}$$

$$PFD_{Sensor} = \frac{\lambda_{DU} \times TI}{2}$$

$$= \frac{900 \times 10^{-9} \times 8760}{2}$$

$$= 3.942 \times 10^{-3}$$

2. Controller part

Type : Generic SIL2 Logic solver

System configuration : 1oo1

$$TI = 8760 \text{ hours}$$

$$\lambda_{DU} = (150 + 100 + 3 + 10 + 3) \times 10^{-9} \text{ 1/hours}$$

$$= 266 \times 10^{-9} \text{ 1/hours}$$

$$PFD_{Controller} = \frac{\lambda_{DU} \times TI}{2}$$

$$= \frac{266 \times 10^{-9} \times 8760}{2}$$

$$= 1.165 \times 10^{-3}$$

3. Final element part

Type : Generic Relay

System configuration : 1oo1

$$TI = 8760 \quad \text{hours}$$

$$\lambda_{DU} = 600 \times 10^{-9} \quad 1/\text{hours}$$

$$PFD_{Final\ element} = \frac{\lambda_{DU} \times TI}{2}$$

$$= \frac{600 \times 10^{-9} \times 8760}{2}$$

$$= 2.628 \times 10^{-3}$$

4. PFD_{Avg} of system

$$PFD_{Avg} = PFD_{Sensor} + PFD_{Controller} + PFD_{Final\ element}$$

$$= (3.942 + 1.165 + 2.628) \times 10^{-3}$$

$$= 7.735 \times 10^{-3}$$

Table D.1. The PFD_{Avg} form calculation and ExSILentia

P&ID Name	SIF Description	PFD_{Avg}	
		Calculation	ExSILentia
Dehydrator vacuum unit	Prevent loss of tempered cooling water flow in C-1201	7.735×10^{-3}	1.59×10^{-2}
Seal liquid loop of separator vacuum pump	Prevent loss of sealant flow to supply C-1301	-	-
	Prevent blockages e.g. strainer or valve of C-1301	7.735×10^{-3}	1.59×10^{-2}
	Prevent loss of fluid level in TK-1315	1.546×10^{-3}	3.24×10^{-3}
Methanol removal column	Prevent loss of level control of D-1101	5.510×10^{-4}	4.47×10^{-4}
	Prevent loss of condenser cooling water of D-1101	-	-
	Prevent loss of control	1.480×10^{-3}	3.23×10^{-3}
	Prevent block in Acetone discharge of D-1101	1.723×10^{-3}	3.13×10^{-3}

BIOGRAPHY

Name: Naphat Yampry

Date of Birth: 18 February 1996

Address: 199/60 Nakorn-in Road, Bangkruy, Nonthaburi, 11130

E-mail: Yampry.N@hotmail.com

Telephone: 097-236-0220

Academic Background

- 2010 – 2013: High School Rajavinit Mathayom School, Bangkok
- 2014 – Present: Bachelor of Petrochemical Engineering Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang

Working Experiences

- June 2017 – July 2017: National Chung Cheng University Internship Program 2016
- August 2017 – November 2017: TTCL Public Company Limited Co-operative Education 2017