BACHELOR THESIS – ME141502

DETERMINATION OF SAFETY INTEGRITY LEVEL BY USING LAYER OF PROTECTION ANALYSIS METHOD ON FLOATING REGASIFICATION UNIT

FITRANI KAMILA
4212 101 033

Supervisor :
Ir. Dwi Priyanta, M.SE
Juniarko Prananda, S.T., M.T.

MARINE ENGINEERING DEPARTMENT
FACULTY OF MARINE TECHNOLOGY
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2016

BACHELOR THESIS – ME141502

DETERMINATION OF SAFETY INTEGRITY LEVEL BY USING LAYER OF PROTECTION ANALYSIS METHOD ON FLOATING REGASIFICATION UNIT

FITRANI KAMILA
4212 101 033

Supervisor :
Ir. Dwi Priyanta, M.SE
Juniarko Prananda, S.T., M.T.

MARINE ENGINEERING DEPARTMENT
FACULTY OF MARINE TECHNOLOGY
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2016

SKRIPSI – ME141502

PENENTUAN SAFETY INTEGRITY LEVEL DENGAN MENGGUNAKAN METODE LAYER OF PROTECTION ANALYSIS PADA FLOATING REGASIFICATION UNIT

FITRANI KAMILA
4212 101 033

Dosen Pembimbing :
Ir. Dwi Priyanta, M.SE
Juniarko Prananda S.T., M.T.

JURUSAN TEKNIK SISTEM PERKAPALAN
FAKULTAS TEKNOLOGI KELAUTAN
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2016

APPROVAL SHEET

DETERMINATION OF SAFETY INTEGRITY LEVEL BY USING LAYER OF PROTECTION ANALYSIS METHOD ON FLOATING REGASIFICATION UNIT

BACHELOR THESIS

Submitted to Comply One of The Requirements
to Obtain a Bachelor Engineering Degree
on
Laboratory of Marine Reliability Availability Maintainability and Safety (RAMS)
Bachelor Degree Program of Marine Engineering Department
Faculty of Marine Technology
Institut Teknologi Sepuluh Nopember

Prepared by :
FITRANI KAMILA
4212 101 033

Approved by
Supervisor of Bachelor Thesis :

1. Ir. Dwi Priyanta, M.SE. ( )
2. Juniarko Prananda, S.T., M.T. ( )

Surabaya,
Juli 2016

This Page Intentionally Left Blank

APPROVAL SHEET

DETERMINATION OF SAFETY INTEGRITY LEVEL BY USING LAYER OF PROTECTION ANALYSIS METHOD ON FLOATING REGASIFICATION UNIT

BACHELOR THESIS

Submitted to Comply One of The Requirements
to Obtain a Bachelor Engineering Degree
on
Laboratory of Marine Reliability Availability Maintainability and Safety (RAMS)
Bachelor Degree Program of Marine Engineering Department
Faculty of Marine Technology
Institut Teknologi Sepuluh Nopember

Prepared by :
FITRANI KAMILA
4212 101 033

Approved by
Head of Marine Engineering Department

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
FAKULTAS TEKNOLOGI KELAUTAN
JURUSAN TEKNIK SISTEM PERKAPALAN

Dr. Eng. M. Badrus Zaman, ST. MT.
NIP. 1977 0802 2008 01 1007

This Page Intentionally Left Blank

APPROVAL SHEET

DETERMINATION OF SAFETY INTEGRITY LEVEL BY USING LAYER OF PROTECTION ANALYSIS METHOD ON FLOATING REGASIFICATION UNIT

BACHELOR THESIS

Submitted to Comply One of The Requirements
to Obtain a Bachelor Engineering Degree
on
Laboratory of Marine Reliability Availability Maintainability and Safety (RAMS)
Bachelor Degree Program of Marine Engineering Department
Faculty of Marine Technology
Institut Teknologi Sepuluh Nopember

Prepared by :
FITRANI KAMILA
4212 101 033

Approved by
Representative of Hochschule Wismar in Indonesia

Dr. -Ing. Wolfgang Busse

This Page Intentionally Left Blank

DECLARATION OF HONOUR

I hereby who signed below declare that :

This bachelor thesis has written and developed independently without any plagiarism act. All contents and ideas drawn directly from internal and external sources are indicated such as cited sources, literatures, and other professional sources.

Name	:	Fitrani Kamila
ID Number	:	4212 101 033
Bachelor Thesis Title	:	Determination of Safety Integrity Level by Using Layer of Protection Analysis Method on Floating Regasification Unit
Department	:	Marine Engineering

If there is plagiarism act in the future, I will fully responsible and receive the penalty given by ITS according to the regulation applied.

Surabaya, July 2016

Fitrani Kamila

This Page Intentionally Left Blank

DETERMINATION OF SAFETY INTEGRITY LEVEL BY USING LAYER OF PROTECTION ANALYSIS METHOD ON FLOATING REGASIFICATION UNIT

Name : **Fitrani Kamila**
ID Number : **4212 101 033**
Department : **Marine Engineering**
Supervisor : **1. Ir. Dwi Priyanta, M.SE**
2. Juniarko Prananda, S.T., M.T.

ABSTRACT

This bachelor thesis will present the assessed system of safety integrity level (SIL) on the storage tank of FRU. SIL is a measure of safety system performance or probability of failure on demand (PFD) for a SIF or SIS. The first step to determine SIL (Safety Integrity Level) by doing HAZOP (Hazard and Operation). HAZOP will analyze the failure and the cause of failure of the system. LOPA is Layer of Protection Analysis which aimed at determining the frequency of undesirable events, which certainly could have been prevented by a layer of protective installed. It is a consequence based method and the first start using the data from HAZOP report. Several steps must be done to determine the SIL number. The first step is to verify the SIS (Safety Instrumented System) by developing safety requirement for example ESD (Emergency Shutdown) and failure rates, and also perform SIS conceptual design by finding SFF (Safety Failure Factors) and the PFD (Probability of Failure on Demand) average of the logic solver and final element. And SIL number can be determined by the calculation. And the result of this bachelor thesis is the system, especially on storage tank, has met the requirement based on the standard.

Keywords : Risk, Hazard, Protection, SIL, PFD, Failure rate.

This Page Intentionally Left Blank

PENENTUAN *SAFETY INTEGRITY LEVEL* DENGAN MENGGUNAKAN METODE *LAYER OF PROTECTION ANALYSIS* PADA *FLOATING REGASIFICATION UNIT*

Nama : Fitrani Kamila
NRP : 4212 101 033
Jurusan : Marine Engineering
Dosen Pembimbing : 1. Ir. Dwi Priyanta, M.SE
2. Juniarko Prananda, S.T., M.T.

ABSTRAK

SIL adalah ukuran kinerja sistem keselamatan atau probabilitas kegagalan pada permintaan untuk SIF *(Safety Instrumented Function)* atau SIS *(Safety Instrumented System)*. Nilai SIL yang akan dihitung adalah pada tangki penyimpanan FRU. Langkah pertama untuk menentukan SIL (Safety Integrity Level) dengan melakukan HAZOP (*Hazard and Operation*). HAZOP akan menganalisis kegagalan dan penyebab kegagalan sistem. LOPA adalah Lapisan Analisa Perlindungan yang bertujuan untuk menentukan frekuensi kejadian yang tidak diinginkan, yang tentunya bisa dicegah oleh lapisan pelindung terpasang. Ini adalah metode berdasarkan konsekuensi dan menggunakan data dari laporan HAZOP. Terdapat beberapa langkah yang harus dilakukan untuk menentukan jumlah SIL. Langkah pertama adalah untuk memverifikasi SIS dengan mengembangkan persyaratan keselamatan misalnya ESD (*Emergency Shutdown)*) dan tingkat kegagalan, dan juga melakukan SIS desain konseptual dengan mencari SFF (*Safety Fraction Failure*) dan PFD (*Probability of Failure Demand)* rata-rata. Dan jumlah SIL dapat ditentukan dengan perhitungan. Dan hasil dari tesis sarjana ini sistem, terutama pada tangki penyimpanan, telah memenuhi persyaratan berdasarkan standar.

Keywords : Risiko, *Hazard*, Perlindungan, SIL, PFD, Tingkat kegagalan.

This Page Intentionally Left Blank

PREFACE

Firstly I would like to thank Allah almighty for giving us the audacity, sanctioning us with acquaintance and confidence to fulfill this task. Then we owe our deepest and profound gratitude to our project advisor, Allah SWT, who shepherded us through the bulk of work with his sage guidance and shrewd cooperation

This bachelor thesis as a final assignment to reach the bachelor engineering degree of Marine Engineering on Ocean Faculty Institute of Sepuluh Nopember Surabaya. This bachelor thesis has been writing from January to July 2016.

This bachelor thesis was done by much support from family, friends, supervisors, and many sides that I cannot list one by one.

This bachelor thesis still not perfect because the lack of knowledge and any other factors so that I hope some suggestions that will help me to make a better research.

Surabaya, July 2016

Fitrani Kamila

This Page Intentionally Left Blank

TABLE OF CONTENTS

This Page Intentionally Left Blank

LIST OF FIGURES

This Page Intentionally Left Blank

LIST OF TABLES

This Page Intentionally Left Blank

LIST OF ABREVIATIONS

FRU	: Floating Regasification Unit
LOPA	: Layer of Protection Analysis
SIS	: Safety Instrumented System
SIL	: Safety Integrated Level
ESD	: Emergency Shutdown
SFF	: Safety Failure Factor
PFD	: Probability of Failure Demand
HAZOP	: Hazard and Operability
IEC	: International Electrotechnical Commission
IPL	: Independent Protection Layer

This Page Intentionally Left Blank

CHAPTER 1
INTRODUCTION

1.1. BACKGROUND

The forecast of Indonesia's domestic natural gas demand is bright. The upstream oil and gas authority, SKK MIGAS, estimates that domestic natural gas demand will grow by 5.1 percent per year from 2.9 billion cubic feet per day (BCFD) in 2007 to 5.5 BCFD in 2020, fueled by new power generation and industry demand. Going forward, the country's power needs will remain high, with more than 10,000 megawatts of new capacity required by 2015 to prevent a long-term power crisis. The state-owned electricity company PLN plans to reduce production and operating costs by increasing natural gas use from 21 percent to 40 percent by 2015. Therefore, the Indonesian government is looking at LNG as a promising solution to natural gas infrastructure problems. [1]

Oil and gas industry performing petroleum and natural gas has a system on their product distribution after the drilling process and passed some stage such as separation and distillation, distribution from land after had some production steps will be distributing to tanker (offshore) that will export the product worldwide. On each step, there must be some risks of failure, on big industry continue failure is very common such as; a false trip alarm to the risk of explosion because of overflow or over pressure. Those failures are possible happening in every industry. However, the main job of the engineer is to minimize the risk and to prevent as if the risk happens.

Safety system needed to protect the plan from major failure or minor failure that leads to dangerous failure. Safety Instrumented System (SIS) having an important role in serving layer protection system on each industry process to decrease the possible risk happening. The safety layer protection means emergency shut down or safety interlock to continue the safe state process when the predetermined set point if the safety operation condition violated. One of the recommended solutions is to determine the SIL (Safety Integrity Level) as the number that states the reliability of the asset. SIL a measure of the availability of a protection layer or barrier. Protection layers include critical alarms and human intervention, SIF (Safety Instrumented Functions), physical protection and emergency response. All these mitigate the frequency of the occurrence of the potential unwanted end-consequence or mitigate the impact the end-consequence represents. Based on IEC 61511-1:2003 [2] safety integrity is the performance that can be done by SIS and SIF on every mode.

Based on IEC 61508 [3] the step required to determine the SIL is doing HAZOP. HAZOP is a standard hazard analysis techniques used in the prepare the establishment of security on the new system or modifications to an existence of potential hazards or operation problem. As the asset existed, the following step is to verify the SIS (Safety Instrumented System) by develop the safety requirement and perform SIS conceptual design. And the last step to calculate the SIL number.

On this final project will analyze the performance and the reliability of the protection system of the regasification unit focusing on storage tank F-6001. The safety level must meet the standard of IEC 61508 and IEC 61511.

1.2. STATEMENT OF PROBLEMS

Based on description above, could be conclude some problems:

1. The accretion of failure number of LNG storage tank.
2. Safety system for LNG storage tank that consists of HAZOP (Hazard and Operation), SIS (Safety Instrumented System) and SIL (Safety Integrity Level) should meet the IEC 61508 & IEC 61511.
3. Determine SIL as the measure of the availability of a protection layer.

1.3. PROBLEM LIMITATION

Research limitations are:

1. LNG distribution system does not include.
2. The safety level only on storage tank F-6001.

1.4. RESEARCH OBJECTIVES

The aim of this bachelor thesis include :

1. To observe the failure rate of the LNG storage tank on FRU based on standard IEC 61508 & IEC 61511.
2. To analyze the safety system of the storage tank F-6001 on the FRU.
3. To determine the SIL (Safety Integrity Level) of the storage tank on FRU.

1.5. RESEARCH BENEFITS

Benefits could gain from this bachelor thesis are :

1. Decrease the number of failure of existing LNG storage tank.
2. The standard of safety system required based on IEC 60115 and IEC 61508.

This Page Intentionally Left Blank

CHAPTER 2
STUDY LITERATURE

2.1. REGASIFICATION UNIT

FSRU (Floating Storage Regasification Unit) is special floating vessel that stores gas and regasifies the LNG (Liquefied Natural Gas). Studies on FSRU have been developed by many engineering and oil & Gas Company and some of them have been approved by ABS (American Bureau Standard).

2.1.1. Step on Loading LNG

Some steps must be done to loading the LNG start from LNG processing to LNG distribution. There are some unit must be passed, such as:

a. LNG Storage

This is the first step on loading process system start from Train 1-6 product the gas and change the gas into liquid form, this 6 train also to neutralize the LNG become pure from any other material. The production of LNG from 6 trains will send to storage tank F-6001-5. The distribution line is shown in **Figure 2. *1***.

The main pipe of the 6 train has a diameter of 20" and will connect to another tank. This parallel pipe divided into two part because there are the top and bottom input of the tank, so the main pipe will decline into 16" because the smaller diameter will help the LNG to flow upward against the gravitation.

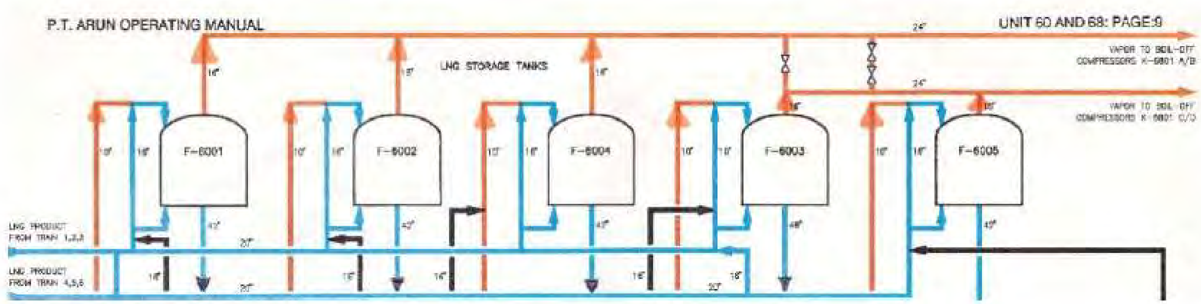


Figure 2. 1 LNG Distribution fromTrain to Storage Tank F-6001

b. LNG Transfer

Loading LNG Transfer to the vessel and the Loading and Circulating pump works because this loading process is the main job of the pipeline system of the Loading and Circulating pump.

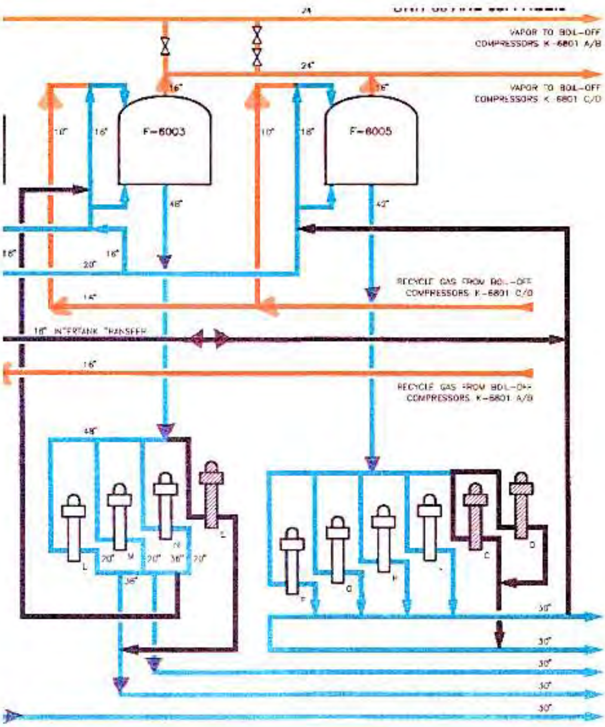


Figure 2. 2 Loading Process Pump (Blue) and Circulating Pump (Grey)

Figure 2. 2 shows the loading process from the tank, pipe with the blue mark as the output. The pipe is the loading pipe to outside the tank by loading pump, the output ofI the tank is a pipe with diameter 48” and divided into 4, for each pipe with a diameter of 20” where the pump located. There are L-M-N pump (white) are the loading pump, the main job of this pump is to send the transfer flow to the vessel, and the grey one is the Circulating pump.

Circulating pump is to circulate the LNG to the whole part so the temperature of LNG is stable. The output of 3 loading pump are 2 pipes with a diameter of 36”. As the diameter decrease will help the flow rate of LNG as the loading process will faster. And then will come together to the pipe with a diameter of 30” that will continue to Berth.

c. Berth and Loading Arm

The last unit is Berth that directly contact with the vessel. There are 2 Berth for loading LNG, Berth 2&3. Each berth consists of 4 Loading Arm where 3 Loading Arm as the LNG distributor and the other Loading Arm as the waster of the vapor of loading from inside the vessel by burning process by marine flare. The main job of this unit to transfer the LNG to the storage inside the vessel, done by Loading Arm on Berth 2 & 3 as shown in Figure 2. 3.

LNG flow to the berth by 2 pipes with a diameter of 24” and goes to Loading Arm that controlled by the on the operator room on each berth. Each pipe will protect from overpressure by Pressure safety valve. The process on berth is the end of loading process on storage tank, start from loading and ended by LNG transferred to the vessel.

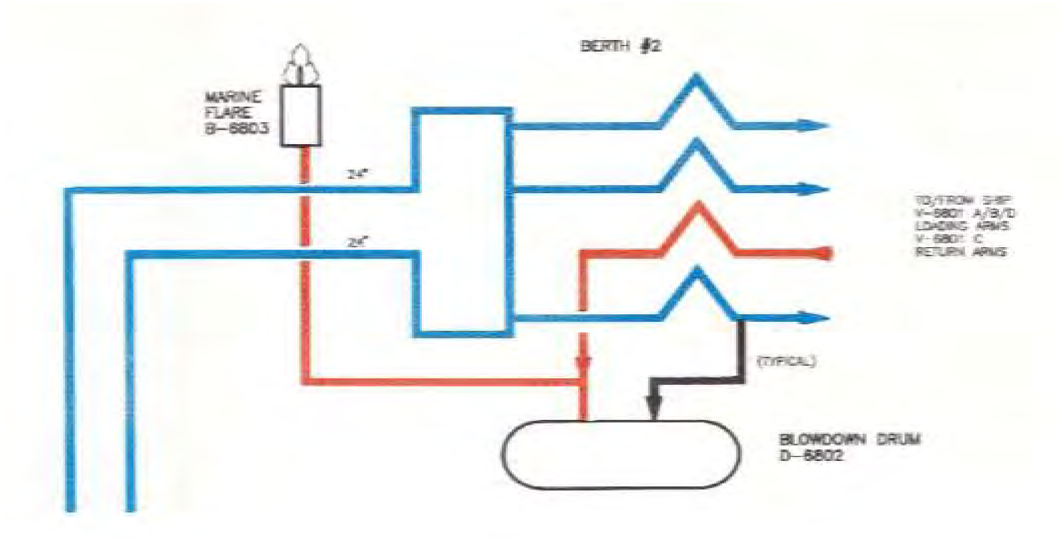


Figure 2. 3 Berth Process

In order to vaporize the LNG, there are a number of possible technologies and some of them are heated vaporizers, ambient vaporizers, and remote heated vaporizers. According to DNV, the heated vaporizer system uses a direct heat procedure with natural gas as fuel. The gas is combusted to get heat, which is used to vaporize the LNG.

Since this system uses natural gas as fuel the result will be CO_2 and pollutants in the air. The ambient vaporizers receive, according to DNV, the heat from naturally occurring sources. This could, for example, be air or sea water. A commonly used method is the open loop water-based system where LNG is heated by seawater that is taken from the surrounding sea. After the sea water is consumed as the heating medium it is removed from the regasification unit and transferred overboard and back to the sea.

This type of approach is possible as long as the surrounding sea is warm enough, which could be a problem when operating in the North Sea. Another concern with this type of vaporizer is that the water, after the heat exchanging process, will be heavily chilled. Therefore, the output water will be very cold in relation to the surrounding water, especially in a warmer climate.

The environmental impact, both long term, and short term, of this cold water emission, needs to be considered for the area where it is supposed to operate. For the example of regasification shown in Figure 2.4.

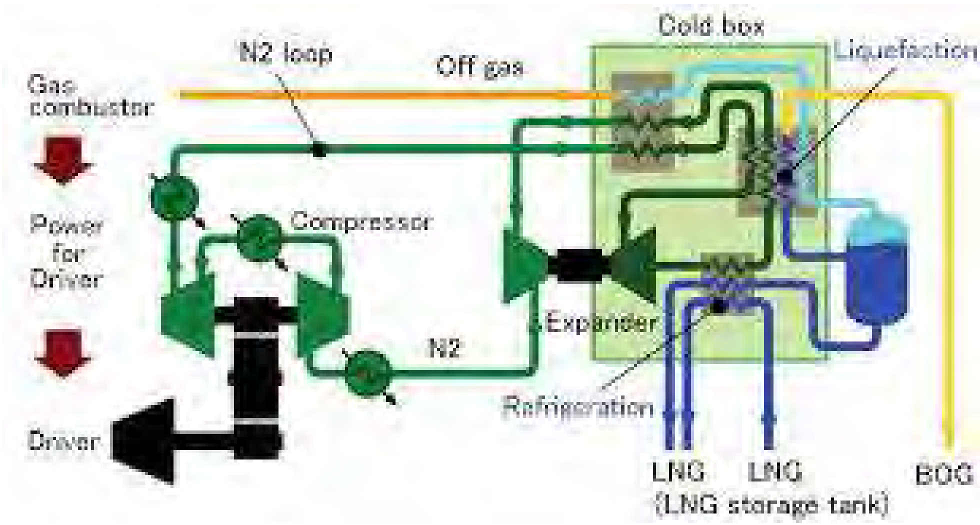


Figure 2. 4 Regasification Plant

Tabel 2. 1 FSRU Particulars

Length Overall	294 meter
Breadth Moulded	46 meter
Depth Moulded	26 meter
Deadweigth FSRU in seawater	81.900 ton
Storage Capacity	170.000 m^3
Regasification Capacity	240 MMSCFD
Offshore Pipeline	± 21 km
Pipeline Specification	24" , API 5L (SAWL) X-65 (PSL 2)

Tabel 2. 1 shows the FRSU particulars data. FSRU location is close to the gas receiving and dividing station Labuan Maringgai or exactly at the coordinates 50 26' 30"S and 1050 56' 30"E [4].

2.2. DATA OF STORAGE TANK F-6001

Figure 2. 5 shows the Process Flow Diagram working system, and Figure 2. 6 shows the Piping and Instrument Diagrams for Storage Tank. The details of PFD of Process Storage Tank & Loading Pump shows in Figure 2. 7. From those several data then divided into some small part called ESD or emergency shutdown to detailing the analysis. ESD used are ESD 1, ESD 2, and ESD 3. The function of each ESD is supporting each ESD, for example, if ESD 1 failed to run the operation the will help by ESD 2. Moreover, if ESD 2 still cannot work to run the operation then ESD 3 will activate. In this final project will analyze the safety integrity level on the storage tank. Based on Figure 2. 8 the system will be divided into 3 nodes; Storage Tank Input, Storage Tank Process, and Storage Tank Output.

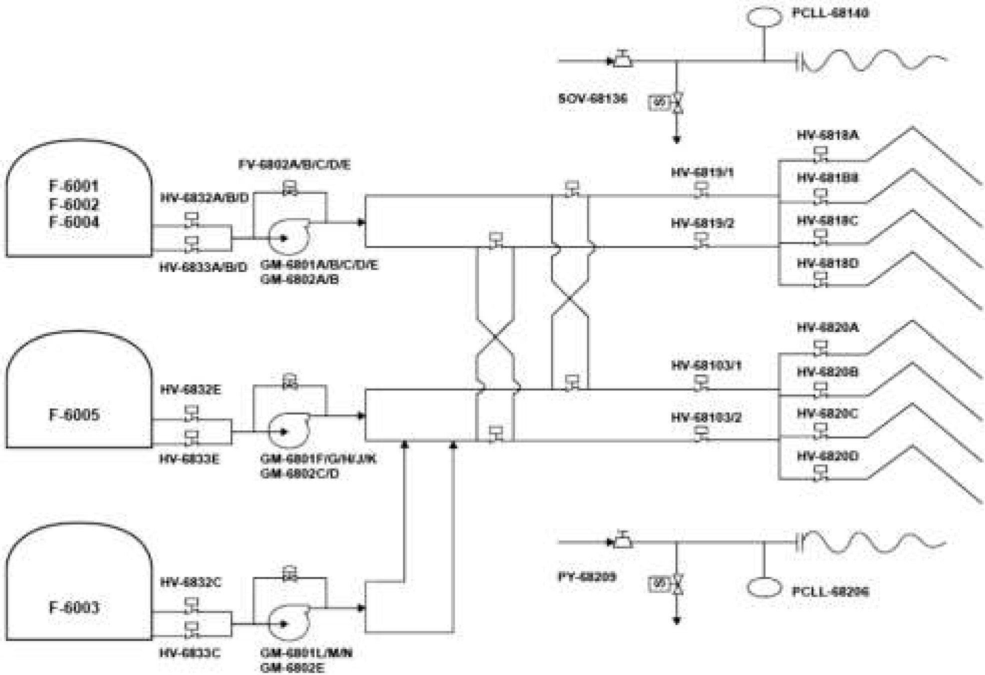


Figure 2. 5 Overall PFD of SIS System

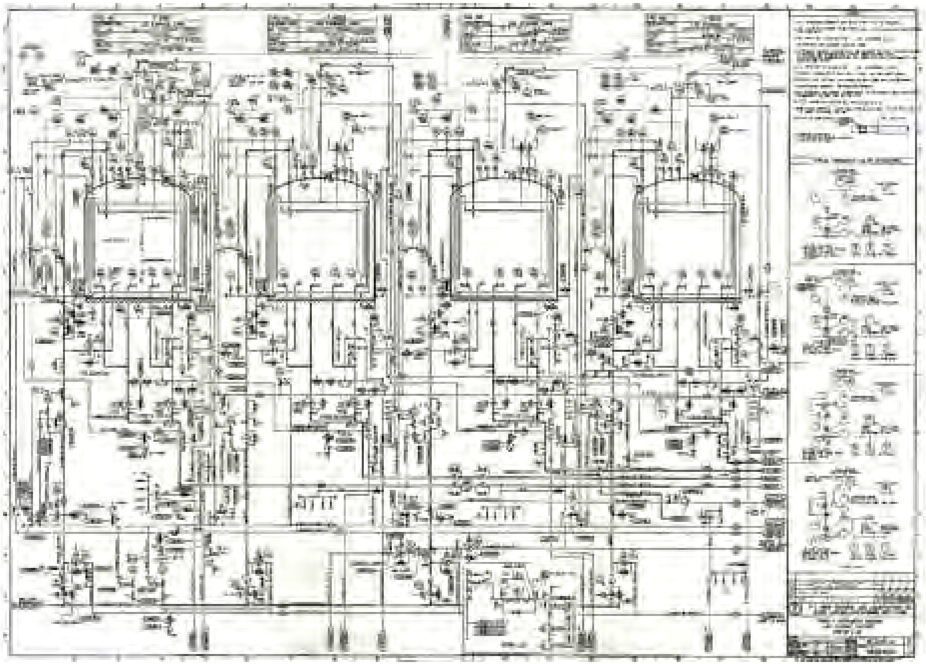


Figure 2. 6 Piping and Instrument Diagrams for Storage Tank

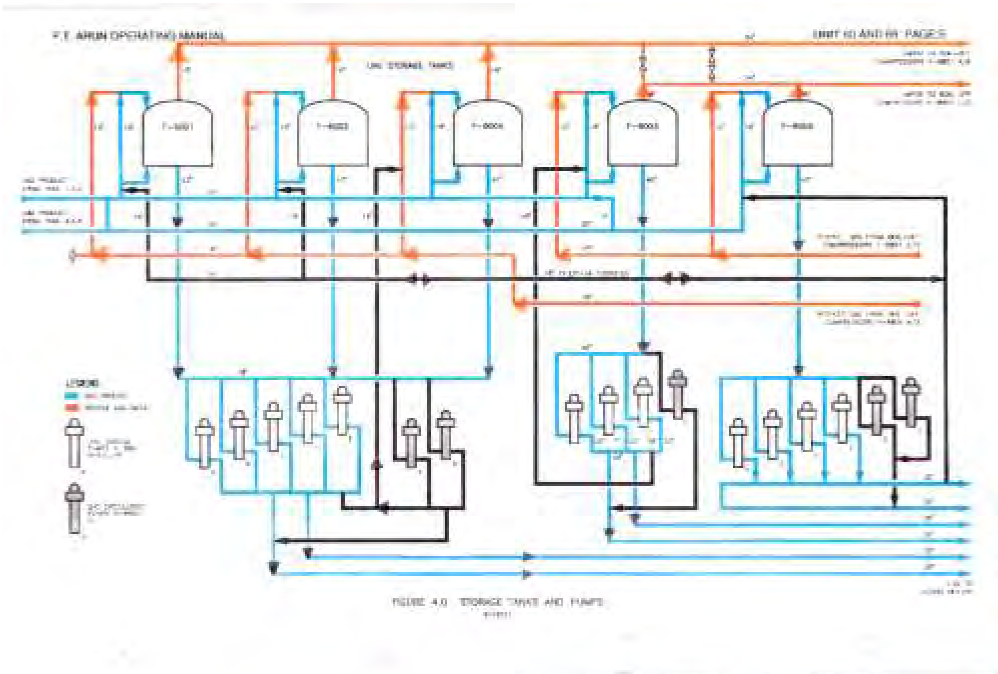


Figure 2. 7 PFD of Process Storage Tank & Loading Pump

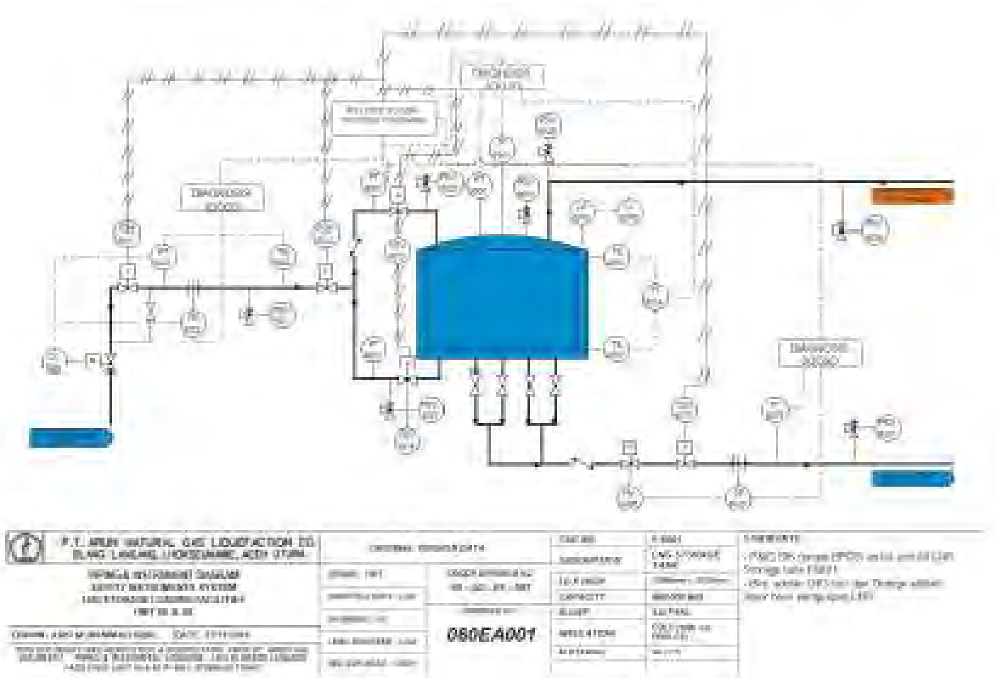


Figure 2. 8 P&ID SIS for Storage Tank

From the system on Figure 2. 5 to Figure 2. 8, some loading valve and the pump will be shut down/stop when a failure occurs, to perform SIL calculation requires the value of the overall failure rate of the process instruments which will be calculated on next stage. Figure 2. 5 shows the whole system of SIS and will divide into several categories based on SIS working on the system. The categories are divide into each class of SIS named ESD (Emergency Shutdown) such as ESD I, ESD II and III. Process Flow Diagram illustrating the ESD system, starting from storage. Berth ended with a tank that is part of the charging liquid LNG tanker headed offshore. On the Figure 2. 5 can be found that the entire system had some final element as security equipment. On each storage tank there is a safety valve that will close when danger occurs, continued on a storage pump that will stop working when the ESD is activated, on the calculation of the verification did not include the pump because these pumps work mechanically and difficult to get the reliability data, besides the final element in small scale.

Storage tank LNG designed to store LNG at low temperature, -162^{O}C. This tank contains two storages, inner storage to store the LNG and the outside storage as the insulation material. On storage tank, the steam must be release or the pressure and temperature inside the tank will increase. To keep the pressure constant by releasing the boil-off gas (BOG) from the tank, this called auto-refrigeration.

The main characteristic of LNG storage tank is able to store LNG at very low temperature, lower than -162 ° C (-260 °F). The typical LNG storage tank is full containment tank, around 55 m (180 ft) height and 75 m (250 ft) diameter (= 250 000 m^3).

In storage tank, if the pressure not releases, the pressure inside the tank will increase and the temperature inside the storage tank also increasing. LNG is cryogen and stored in the liquid phase at very low temperature. The temperature inside the tank should be constant Storage tank has the same function of thermos that insulates the heat inside the bottle. Storage tank to keep the low temperature -160 °C so the storage tank designed to keep the temperature inside stable and the LNG still in liquid form.

Some variable changes on the operation of the storage tank:

Flow	:	Flow change as the flow from the train the volume of LNG change to the production of LNG.
Pressure	:	Normal operation pressure inside storage tank 700-1100mm H_2O
Temperature	:	Normal operation temperature -159°C

Control System process on storage tank has controlled by two systems, normally controlled by PT/PIC-6001A that will send the signal to compressor boil off control. And the other is PT/PIC – 6002A that will release the excess pressure to the atmosphere if the normal control system failed to control.

Alarm on storage tank that shows the high pressure by an instrument with tag number PH-6003A and low pressure by PL-6003A. To high level on tank showed by LAH-6001A and low level showed by LAL-6001A. High temperature showed by TAH-6002E 15/16 and for low temperature by TAL-6002AE-15/16.

Storage Tank F-600 has maximum capacity 127000$mm3$ to receive the flow from train 4/5. The tank will full in 12 days when the filling of LNG from train 4/5 that will operate maximum 115% with pressure 0,08 $k/c2$ and temperature -159 °C to -162 °C.

2.3. INSTRUMENT SYSTEM

Instrument system is the hardware, software, and process. SIS (Safety Instrument System) is the instrumentation system that used to implemented one or more SIF (Safety Instrument Function). SIS consist of some component such as sensors, logic solvers, and final element that work to protect the system into a safe condition.SIF is a function of SIS as protector or controller to do the safety task.

Figure 2. 9 shows the general instrument system.

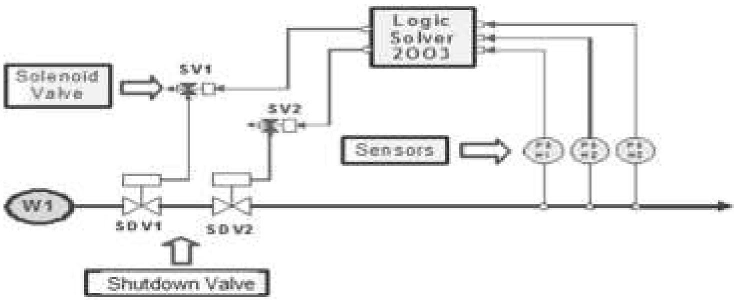


Figure 2. 9 General Instrument System

2.4. HAZOP (HAZARD AND OPERABILITY)

"A hazard evaluation of broad scope that identifies and qualitatively analyzes the significance of hazardous situations associated with a process or activity." (Definition from Layer of Protection Analysis, Simplified Process Risk Assessment, pg. 261). At this stage, HAZOP (Hazard and Operability Study) is used. HAZOP is a standard hazard analysis technique that used in the preparation to establish the security on the new system or modifications to an existence of potential hazards or operation problem.

HAZOP is a qualitative technique based on the GUIDE - WORDS And Implemented by a team during HAZOP Process For Example Instrument Engineering. To start HAZOP needed PFD / P&ID document from the unit that is going to be analyzed, it will be split into some stages according to the unit, there are Storage Tank and Loading Pump. By using HAZOP method can identify the possibility of a dangerous situation will occur, eventually the results will be HAZOP report.

2.4.1. HAZOP Steps

HAZOP will be explaining on the following step:

a. Determination of Node

Node is the point to mark the start and end point of the sub-system. HAZOP study will do on each sub-system.

b. Determination of Deviation

Based on IEC 61882 Hazard and Operability Studies (HAZOP studies) - Application guide, there are some deviation that might happened along the operation of the plan [6], such as:

1. No Flow
2. Low Flow
3. More/High Flow
4. Reverse/Misdirected Flow
5. Low Level
6. High Level
7. Less/Low Pressure
8. High Pressure
9. Less/Low Temperature
10. High Temperature

c. Determination of Parameter

The parameter is the measure or limitation, also used to know as if the determined deviation will happen to each node. The parameter will be determined based on the deviation. Each node will have different parameter from its deviation.

d. Likelihood

The likelihood is the chance of LNG released to the environment because of leakage or PVS (Pressure Safety Valve) activated causing by overpressure.

Table 2. 1 Likelihood Level [6]

Likelihood	Significance
1	Low- hazard not expected at all in the plant life
2	Medium low- hazard not expected more than once in the plant life
3	Medium High – Hazard expected several times in plant life
4	High – hazard expected more than 1/year

Table 2. 1 shows the likelihood level of leakage. The likelihood level classified by the hazard consequence. The lowest likelihood is level 1 which indicate the lower risk of consequence or by mean the hazard not expected to cause fatality. Following by moderate level 2, level 3 and the highest level is likelihood level 4 with hazard consequences could causing fatality or damage more than 1/years.

To correctly assign these levels, it is important to recognise this is a conditional probability of a consequence occurring.

e. Severity Analysis

Severity is the effect that might happen when the LNG released to the air. There are 3 possible effects that might be happened, for example to the human, to the operation and the financial effect. Table 2. 2 shows the severity level and its effect. Table 2. 3 shows the description of injury effect to the operator.

Table 2. 2 Severity Level [6]

Severity	Significance
1	Low- no Injury hazard or hazard leading to loss of <1 weeks production or loss less than $100.000
2	Medium Low- minor injury hazard or hazard leading to loss of 1-4 weeks production or loss between $0,1-1M
3	Medium High- Injury hazard or hazard leading to loss of 1-6 months production or loss between $1-10M
4	High- fatality/ serious injury hazard or hazard leading to loss of > 6 months production or loss greater than $ 10M

Table 2. 3 Severity Description [6]

Category	Description
No injury hazard	- No burn
Minor injury	- Minor burn
Injury hazard	- First-degree burn
Fatality/serious injury	- Death occurs when accident occurred - Third degree burn - Second degree burns on face, hand, or and stomach.

f. Risk Ranking

The risk is when the cause of risk meets the source of risk. Table 2. 4. shows the risk ranking and the definition based on their ranking.

Table 2. 4 Risk Definition [6]

Ranking	Significance
A	Acceptable Risk Level
B	Almost Acceptable level risk. Acceptable if suitably controlled by management. Should check that suitable procedure and/or control systems are in place
C	Undesirable risk level. Must be reduced to level B at the most by engineering or management control
D	Unacceptable risk level. Must be reduced to level B at the most by engineering or management control.

Figure 2. 10 Risk Matrix [7]

Figure 2. 10 shows the matrix used. If the risk level that happened is 1 or 2 it should be reduced to risk level 3. To reduce the risk level can be done by adding more safety equipment and SIL analysis to analyze the availability of the recommended safety tools. And Figure 2. 11 shows the relation between likelihood and severity.

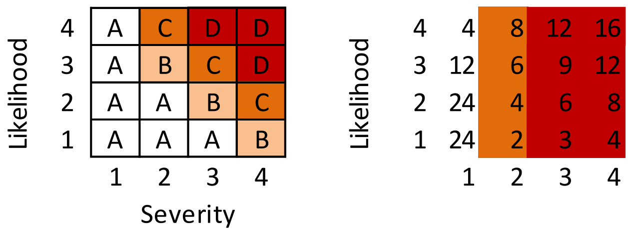


Figure 2. 11 Risk Matrix of Likelihood and Severity [7]

2.5. THE LAYER PROTECTION ANALYSIS (LOPA)

The Layer of Protection Analysis (LOPA) method is a Process Hazard Analysis tool modified LOPA can be considered as a simplified form of a quantitative risk assessment. It can be used after a hazard and operability analysis (HAZOP), and before a quantitative risk analysis (QRA). A difference between LOPA and other tools is that LOPA analyze the different protection layers individually, and the mitigation they lead to. LOPA is especially used to determine the safety integrity level (SIL) of safety instrumented functions in conjunction with IEC 61511 [2], but also as a general risk assessment tool to evaluate if the protection layers in a system are satisfactory. In addition, several other applications of LOPA as capital improvement planning, incident investigation and management of change and the method was implemented internationally.

In gas/oil industry LOPA is more frequently applied to topside equipment than subsea equipment. The LOPA method allows the user to determine the risk associated with the various hazardous events by utilizing their severity and the likelihood of the events being initiate.

The method starts with data developed in the Hazard and Operability analysis (HAZOP) and accounts for each identified hazard by documenting the Initiating Cause and the protection layers that prevent or mitigate the hazard.

Figure 2. 12 illustrate the relationship between HAZOP and LOPA Worksheets. HAZOP worksheet cells equal to cells in LOPA report, and automatic transformation of data [8]. This applies to:

- HAZOP consequence indicates impact event on LOPA worksheet
- HAZOP possible causes indicates initiating causes on LOPA worksheet
- HAZOP consequence likelihood indicates initiating cause frequency on LOPA worksheet (Note: may need adjustment)
- HAZOP consequence severity level indicates Severity level on LOPA worksheet (Note: May need adjustment)

The total value of risk reduction can be determined and need more risk reduction analysis. If additional risk reduction is required and be provide in the form of a Safety Instrumented Function (SIF), the LOPA methodology allows the determination of the appropriate Safety Integrity Level (SIL) for the SIF.

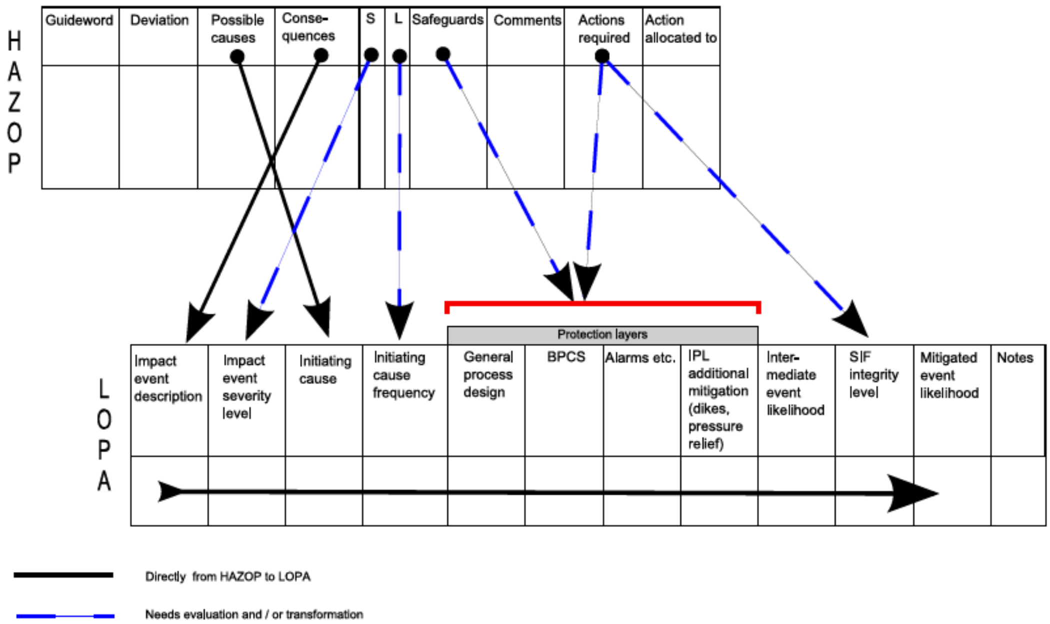


Figure 2. 12 Relationship between HAZOP and LOPA worksheets

Table 2. 5 SIL and Required Safety System performance for Low Demand Mode System [8]

Mode Low Demand Rate			
SIL	Availability	PFD	RRF
4	>99.99 %	10-5 s/d 10-4	100000 s/d 10000
3	99.90 – 99.99 %	10-4 s/d 10-3	10000 s/d 1000
2	99.00 – 99.90 %	10-3 s/d 10-2	1000 s/d 100
1	90.00 – 99.00 %	10-2 s/d 10-1	100 s/d 10

Table 2. 5 shows that the greater PFD number of the system need a high level of safety. In another word the greater failure, the greater level of safety to make sure that the plan is safe to operate. It also shows that the plan needs more safety system to secure the system from failure.

In IPL (Independent Layer Protection) stacked layer stacks are applied to minimize the unwanted circumstances, the layer will backup the other layers so that the system will be more secure to reduce the level of risk as low as possible up to the limit tolerated. In this LOPA IPL method is divided into 7 types with two main categories as listed in Table 2. 6.

Table 2. 6 Distribution of IPL Categories in LOPA

IPL (Independent Protection Layer)						
Prevention				Mitigation		
Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Layer 6	Layer 7
BPCS	Alarm	Operator	SIS	Passive	Passive Outside	Emerge

From Table 2. 6 is divided into two main categories, Prevention and Mitigation, for descriptions are as follows:

a. Prevention

Prevention is the category that used to the 4 initial layer. There are 4 layers to prevent the occurrence of a failure, with 4 categories on layer works as a deterrent and will back up to each other in case of failure in one layer. The category of prevention are:

- **BPCS**; Basic Process Control System including normal manual control, is the first level of protection during normal operation. BPCS is designed to maintain the process in the area of safe operation. Normal operation BPCS control loop can be credited as an IPL if it meets the appropriate criteria.

- **Alarm**; In terms of actual operation alarm is not included in the IPL, but because Alarms should inform the operator if a failure occurs, the alarm may have some importance because the operator will not respond if the layer is not activated.

- **Operator**; Someone who control and supervise the process called the operator, in this case, the operator will take over the action to restore the plant to a safe state in the event of failure. The role of the operator as the IPL is very important for operators to be the one in control when BPCS system failure.

- **SIS**; Safety instrumented system into a final layer in this category. SIS will be active when the BPCS and the operator have failed to take over and bring in a safe condition. SIS works automatically without any interference from the operator, the system will actively be protective in the event of circumstances outside the specified tolerance.

b. Mitigation

Mitigation is carried out when the IPL category on Prevention has failed to take over. Mitigation works when a failure has occurred, with this mitigation will seek to minimize possible casualties or damage to the plant.

The main difference between Prevention and Mitigation is when the Prevention works to prevent the failure by minimizing the possibility of failure, but Mitigation works when it happened and Prevention has failed, Mitigation works to minimizing the number of losses incurred. This category is divided into 3 IPL are:

- **Passive Device**; Passive devices to prevent many losses such as relieve Pressure Valve that will work when excess pressure and SIS are not able to take over, causing leakage by the pressure then PSV will release these pressures so that losses can be reduced.

- **Outside Passive**; On Passive Outside is more directed at preventing losses, for example, is a Bunkers as the protection of workers when there has been a blast, with the IPL is the number of losses will be minimized.

- **Emerge**; The final step in the event of failure of the plant such as blast then performed the last time all the IPL has failed to take over is to make the evacuation status to all workers at the plant to immediately leave the plant to reduce the occurrence of victims.

With the IPL, the next need HAZOP report of the possible likelihood of failure on several systems and grouped in IPL that will take over if the occurrence of a failure. After getting the results of the IPL table LOPA for determining the amount and many types of IPL then it can be done signifies the end of the process this method. And the result of the LOPA is LOPA worksheet based on HAZOP.

2.6. INDEPENDENT PROTECTION LAYER (IPL)

Independent Protection Layer is a tool, system, or action to exceed the consequence on the unwanted scenario. The tools are known as IPL is meet the requirement:

a. Effective to prevent the planned consequences.
b. One similar case to one or more equipment.
c. Checked and assumed to effective prevent the consequences.

Table 2. 7 Typical Probability of PFD value [9]

No	Independent Protection Layer (IPL)	PFD
1	Pressure relief device	10^{-2}
2	Operator Response (educated, no stress)	10^{-2}
3	Operator Response (Under high stress, average training)	$5x10^{-1}$
4	Operator response to alarms and procedures (low stress, recognized event)	10^{-1}

2.7. SAFETY LIFE CYCLE

Safety life cycle is engineering process that contains about required steps needed to accomplish the high safety level functionally, design, plan, operation and Safety Instrumented System maintenance. An automation system that has been plan based on required term and decrease the failure risk on industry process. Safety life cycle starts with the conceptual design of a process and ends if the SIS decommissioned.

The key to this idea is that we must consider that safety must be the plan from the beginning of the conceptual design of the process and should be at every design, operation, and maintenance. Safety life cycle has 3 phase that can be identified as analysis (risk analysis), realization (part of the asset), and operation. Safety life cycle shows that most of the activity on analysis stage is using logic steps.

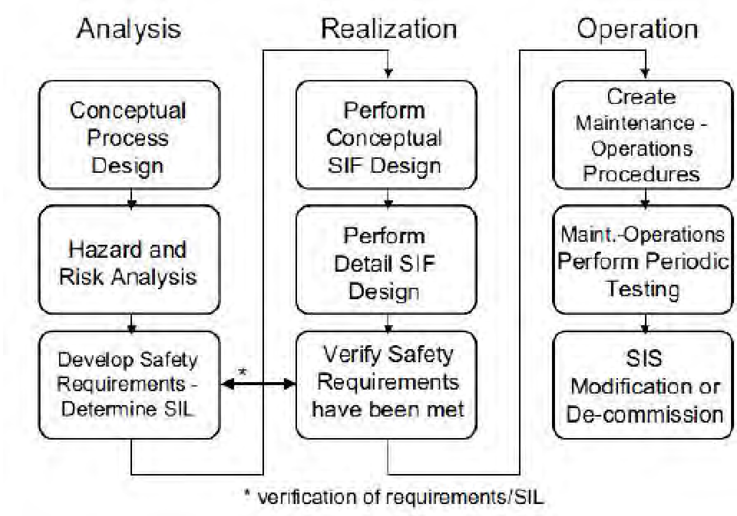


Figure 2. 13 Phase of Safety Life Cycle [3]

As shown in Figure 2. 13 that to accomplish high safety level there are 3 phase that should be done. But on this final project only consist of analysis and realization only.

On the Chapter 3 will explain more about the details. On Figure 2. 14 more detail step will be explained. Basically, this final project will stop on SIS conceptual design.

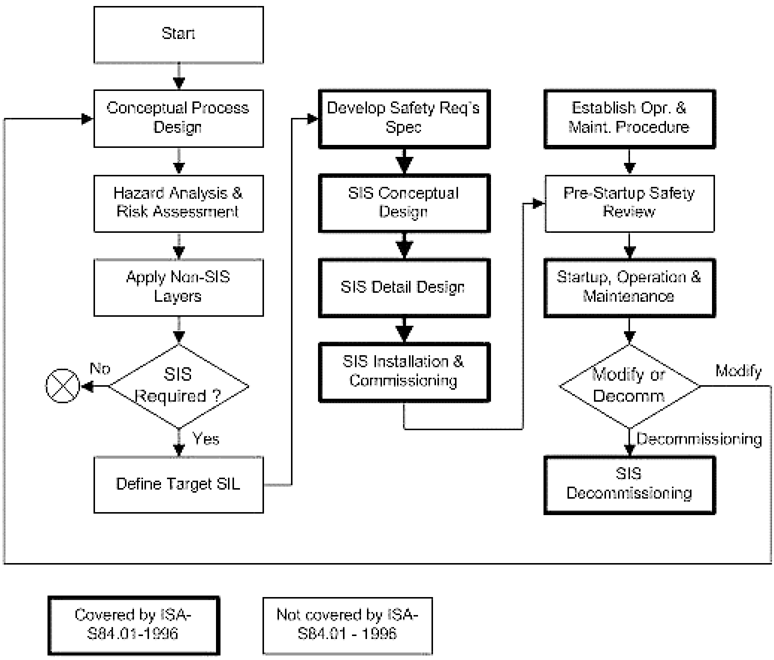


Figure 2. 14 Safety Life Cycle Based on IEC 61508 Standards [3]

Figure 2. 14 above shows the safety life cycle based on IEC 61508 Standards. details of the step will describe the following step:

1. Conceptual process design

   This is the first step on safety life cycle step. On this step, we study more about the detail of the process, controllable asset, and the environments. So that next steps able to be done.

2. Hazard analysis and risk assessment

   The next step is understanding all about risk in the process, this can be done by hazard analysis and risk assessment. Hazard analysis is identifying the risk of the asset, some technique that can we use are Hazop, fault tree, and checklist. Risk assessment is giving grade/rank based on the hazard analysis.

3. Application of non-SIS layers

   We can not get 100% safety on the asset by design, the rest of the risk can be handled by non-SIS equipment for the control system.

4. Is SIS required?

   If the rest of the risk can be handled by non-SIS equipment so the safety level can be accepted, the SIS design stops at this step. If there the risk level is still high, SIS equipment is needed.

5. Define target SIS

   SIS equipment should meet the risk level. In another word, to handle higher risk level we also need better SIS equipment. The level of SIS equipment needs to be called safety integrity level (SIL)

6. Develop safety requirement specification

   The next step is to develop safety requirement specification which contains the functional logic of the system. Every safety function should connect to the SIL requirement and reliability requirement. This specification for every operation, from startup to shutdown.

7. SIS conceptual design

   This step is developing an initial design to check as if the design meet the safety requirement and SIS performance requirement. This steps also about choosing the technology, configuration, interval testing, field devices and logic box.

2.8. SAFETY INSTRUMENTED SYSTEM (SIS)

The operation process of industrial have a great risk due to presence of dangerous material, chemical, gases, and the others. A safety instrumented system (SIS) can dramatically reduce the risk of accident in industrial process.

Safety Instrument System is a system composed of sensors, logic solver, and final element that have function to secure the system in case of a defiant operation not to endanger people, environment, and assets. Figure 2. 15 shows the Safety Instrument System (SIS) in a general overview of safety instrument system.

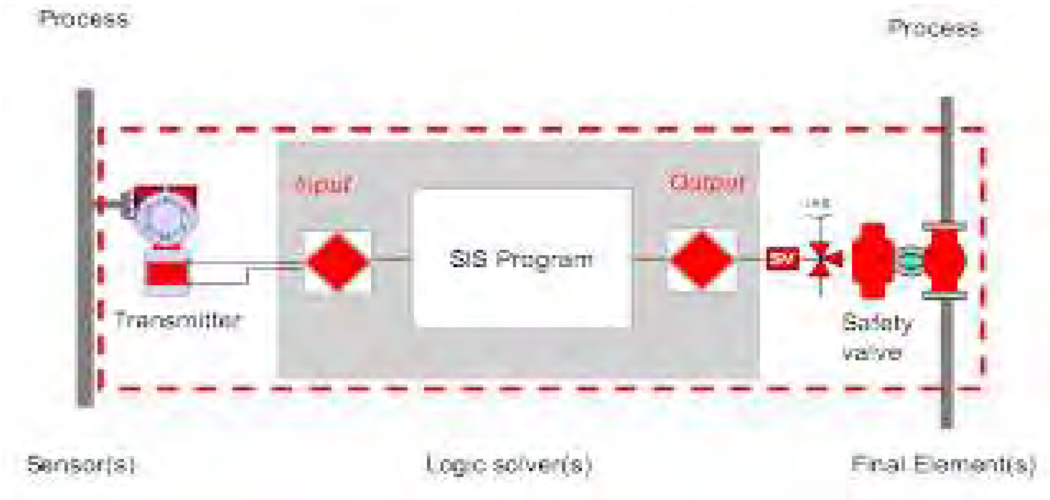


Figure 2. 15 Safety Instrumented System [10]

2.8.1. Sensors

The sensor is a device or combination of devices that used to measure the process condition such as transmitters, transducers, process switches or position switches. Sensor used to convert physical quantities into electrical quantities that can be analyzed by using an electric circuit.

2.8.2. Logic Solver

The logic solver is a processor of the electric signal that sent from a sensor or more to be processed and produce electric signals to be sent to the final element. An example of the logic solver includes the electrical system, electronic system, programmable electronic system, pneumatic system, and hydraulic systems.

2.8.3. Final Element

The final element is part of the SIS which function is to take action to reach a safe condition. The final element is valves, switch gear, motors, solenoid valve, and actuator.

2.8.4. SIS Design

SIS design is made to meets the requirement IEC 61508 on Safety Life Cycle as guidance to SIS design. On this SIS design only has plan and design, do not continue to installation and operation stage, so it is only about analysis and realization. Data needed to complete this stage are some detail data about the LNG, specification of the storage tank, and the specification of loading pump. SIS design shows in Figure 2.16.

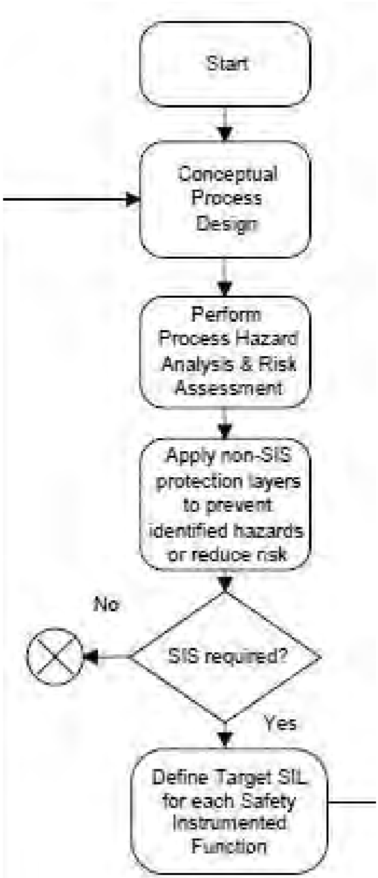


Figure 2. 16 SIS Design Flow Chart [3]

2.8.5. Conceptual Process Design

The process occurs in storage that will proceed to the port through the pump as a medium that delivers the LNG through pipelines. Loading Pump Storage Tank and has the specs of each listed in Table 2.8 to 2.10

Table 2. 8 Specification of LNG

Specification LNG	
Form	Liquid
Density	430 – 478 kg/m^3
Mocular Weight	16,58 – 18,88 kg/mol
Nitrogen	1,24 max % mol
Hidrogen Sulfide (H2S)	5,0 max % mg/nm^3
Temperature	(-158) – (-162)°C

Table 2. 9 Specification of LNG Storage Tank

Specification of LNG Storage Tank	
Tag no	F-6001
Description	LNG Storage Tank
Capacity	800.000BBL (127000 m^3)
MAWP	2.0 PSG (0,4 kg/cm^{2}G)
Insulation	Cold (1000 mm Perlite)
Diameter x High	7000 mm x 35760 mm

Table 2. 10 Specification of LNG Loading Pump

Specification LNG Loading Pump	
Tag no	G-6801
Description	LNG Loading Pump
Flow	12.000GPM (2,724 m^3/h)
Diff Pressure	97,0 PSI (6,82 kg/cm^2)
SG	0,465
Motor	1000 HP (735 KW)
Casing	356 AL_- ALLOY
Insulation	6,5" (165 mm)

Based on data process and the specification above, flow chart on Storage Loading Facilities is done. Conceptual design is completed, data is completed so the next step can ben done based on this conceptual design.

2.8.6. Verification SIS (Safety Instrumented System)

Verification of SIS aims to find out what is the SIL achieved, and the value of SIL represented the security level of the plant. The smaller the value of SIL, the greater the risk that would be obtained in the event of a catastrophic. The greater the value SIL means the ability to reduce the level of risk the better. The appropriate standard of IEC 61058 [3] is a method on the Safety of Life Cycle as a guide to verify the SIS. By analyzing the SIL of the SIS is intended to determine the value of existing systems. Some numbers of failure factors as consider the existing system. Verification of the SIS shows on the Safety of Life Cycle flow chart on Figure 2.14.

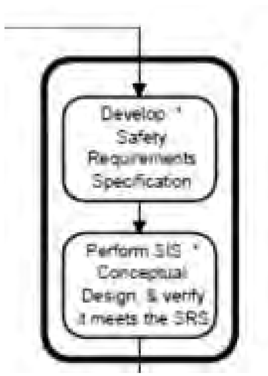


Figure 2. 17 Flow Chart for SIS Verification [3]

The step of Figure 2.17 above, develop safety requirement and perform SIS, will explain more detail on the next step.

2.8.6.1. Develop Safety Requirement

To perform the verification analysis on Safety Instrumented System that must be done by collect some data that contains specifications, instrument number, piping systems, process systems and another data. Most of the data obtained from the P&ID that contains a complete description of a process and the control of a unit. All of the data collected will be analyzed and classified into several categories according to running processes. At SIS analysis requires also the value of each instrument failure rate SIS on the field, this value will be calculated to obtain the value of SIL.

2.8.6.2. Perform SIS (Safety Instrumented System) Conceptual Design

SIS verification has some method; one of them is Simplified Method. In this case, Simplified Method will be used because it is easy to do. Simplified Method is a method used for verification and cannot be separated from the main elements of this method is PFD (Probability Failure on Demand) number. PFD is a failure number that owned by the equipment when it needs to work. For example, failure to activate an alarm when desired, or failure of the control valve to close when it is desirable to close. The numbers are usually expressed in units per year (760 hours). Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

- *The fraction of failures*

  The safety of failures do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad (2.\ 1)$$

Where:
λ^{S} : Failure Safe
λ^{DD}: Failure Danger Detected
λ^{DU}: Failure Danger Undetected

To detailing the cause of failure, the Failure rate on the failure of an equipment divided into 2 parts, fail safe (λ^{S}) and fail danger (λ^{D}). The definition of failure safe or "if failure, then safe" is if the failure happened on the equipment it will not affect to the equipment or the system. Based on IEC 61508 the definition of Fail safe is a failure that does not have the potential for system leads to dangerous conditions, so when the failure does not potentially to be harm but still be calculated for a safety of an equipment. Practically failure safe divided into 2 section, fail safe detected (λ^{SS}) and fail safe undetected (λ^{SU}). The diagnose of fail safe detected and fail safe undetected doing by logic solver.

Based on IEC 61508 *fail danger is* a *failure* that has the potential for a safety system into the dangerous condition. That means even a small failure but potentially to be harm to the equipment or the system. Fail danger also divided into 2 section, *fail danger detected* (λ^{DD}) and *fail danger undetected* (λ^{DU}). Failure danger undetected is very dangerous, because the failure happened is not detected on logic solver but the failure might lead to another failure.

From the failure safe and failure danger only diagnosed by the logic solver. These two data is very important to influence the reliability and SIL number of SIF.

SIL verification by using Simplified Method without calculating the human factor as operation participation on this system. The main term used in that calculation is PFDavg that can get from Failure Mode on each device. The calculation of each element of SIF can lead to the SIL number of a system, this SIL number determine if the system meets the requirement of the IEC standard. The system has Low Demand category because the demand frequency operation of the safety system is not more than one for each year, and not more than two times of proof test frequency. The Low Demand has own requirement based on IEC shown on Table 2.11

Table 2. 11 SIL and Required Safety System Performance for Low Demand Mode System [3]

Mode Low Demand Rate			
SIL	Availability	PFD	RRF
4	>99.99 %	10-5 s/d 10-4	100000 s/d 10000
3	99.90 – 99.99 %	10-4 s/d 10-3	10000 s/d 1000
2	99.00 – 99.90 %	10-3 s/d 10-2	1000 s/d 100
1	90.00 – 99.00 %	10-2 s/d 10-1	100 s/d 10

- *Hardware Fault Tolerance (HFT)*

In this unit, the valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD, which has 1/1, it means the use of the single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. The Table of HFT (Hardware Fault Tolerance) shown in Table 2.12.

Table 2. 12 Architecture Type A

Type A	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % < 90 %	SIL 2	SIL 3	SIL 4
90% < 99 %	SIL 3	SIL 4	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4

- *Average probability* of hazardous failures for a safety function on demand (PFDavg).

  Determine the value of the PDF (probability of failure on demand) of the components that support the same safety system on the node. PFDavg value as the main element of the calculation, while the value obtained from the equation PFDavg meet the standard of the architecture of a system, because the ESD unit is activated via a push button that located in the control room storage loading facilities, With the flow of the Push Button - Logic Solver - Final Elements, then the system goes into the category of system 1/1 (1 out of 1) and the equation used to PFDavg is:

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \tag{2.2}$$

Where;

PFDavg	: PFD average
λ^{DU}	: Failure Mode Danger Undetected
TI	: Time Interval per 1 year = 8760 hr

The calculation by using Simplified Method need the equation of:

$$\text{PFD}avg^{SIF} = \sum\text{PFD}avg^{LS} + \sum\text{PFD}avg^{FE} \tag{2.3}$$

Where;
$\text{PFD}avg^{SIF}$: PFD average of SIF
$\sum\text{PFD}avg^{LS}$: PFD average of Logic Solver
$\sum\text{PFD}avg^{FE}$: PFD average of Final Elements

Based on the calculation above, the result of this calculation is the SIL number of the storage tank.

2.9. SAFETY INSTRUMENT FUNCTION (SIF)

A set of equipment intended to reduce the risk due to a specific hazard (a safety loop). Its purpose is to 1. Automatically taking an industrial process to a safe state when specified conditions are violated; 2. Permit a process to move forward in a safe manner when specified conditions allow (permissive functions); or 3. Taking action to mitigate the consequences of an industrial hazard. It includes elements that detect an accident is imminent, decide to take action, and then carry out the action needed to bring the process to a safe state. Its ability to detect, decide and act is designated by the safety integrity level (SIL) of the function. Safety instrument function is the function of safety instrument system to reduce or minimize the consequence from operating deviation. The consequences can effect the loss of financial, fatalities, environment or the operation of the system is stopped.

2.10. SAFETY INTEGRATED LEVEL (SIL)

The SIL is a measure of the availability of a protection layer or barrier. Protection layers include critical alarms and human intervention, safety instrumented functions (SIF), physical protection and emergency response. All these mitigate the frequency of the occurrence of the potential unwanted end-consequence or mitigate the impact the end-consequence represents. Based on IEC 61511-1:2003 [2] safety integrity is the performance that can be done by SIS and SIF on every mode.

SIL is the equipment/system that designed to monitor the dangerous conditions on a plant and takes action in case of hazardous conditions or if not taking any action it will cause harm. Equipment/systems will produce output that will prevent the hazard or reduce the consequences. In general, the SIS is composed of sensors, logic solver or also called safety and final control element.

There are four discrete integrity levels associated with SIL. The higher the SIL level, the lower the probability of failure on demand for the safety system and the better the system performance. It is important to also note that as the SIL level increases, typically the cost and complexity of the system also increase.

CHAPTER 3
METHODOLOGY

The benefits of this bachelor thesis which determines the SIL some following step must be done as shown in Figure 3.1 Methodology Flowchart (next page). This chapter will describe step by step how to determine the safety Integrity level by using a layer of protection analysis method. The final result of this bachelor thesis are the safety level and the recommendation to fulfill the safety level.

3.1. STUDY LITERATURE

The first step is study literature. In this step can be done by searching and studying about something that related to the problems. Literature studies also can be done by reviewing the paper or a journal dealing with the problems to be solved.

3.2. DATA COLLECTION

From study literature, to solve the problem existed in this final project need some data, such as:

1. P&ID of the system
2. Failure Rates table

The data are taken from the company and used to analyze the plan.
Detail of the data can be found in **attachment 1.**

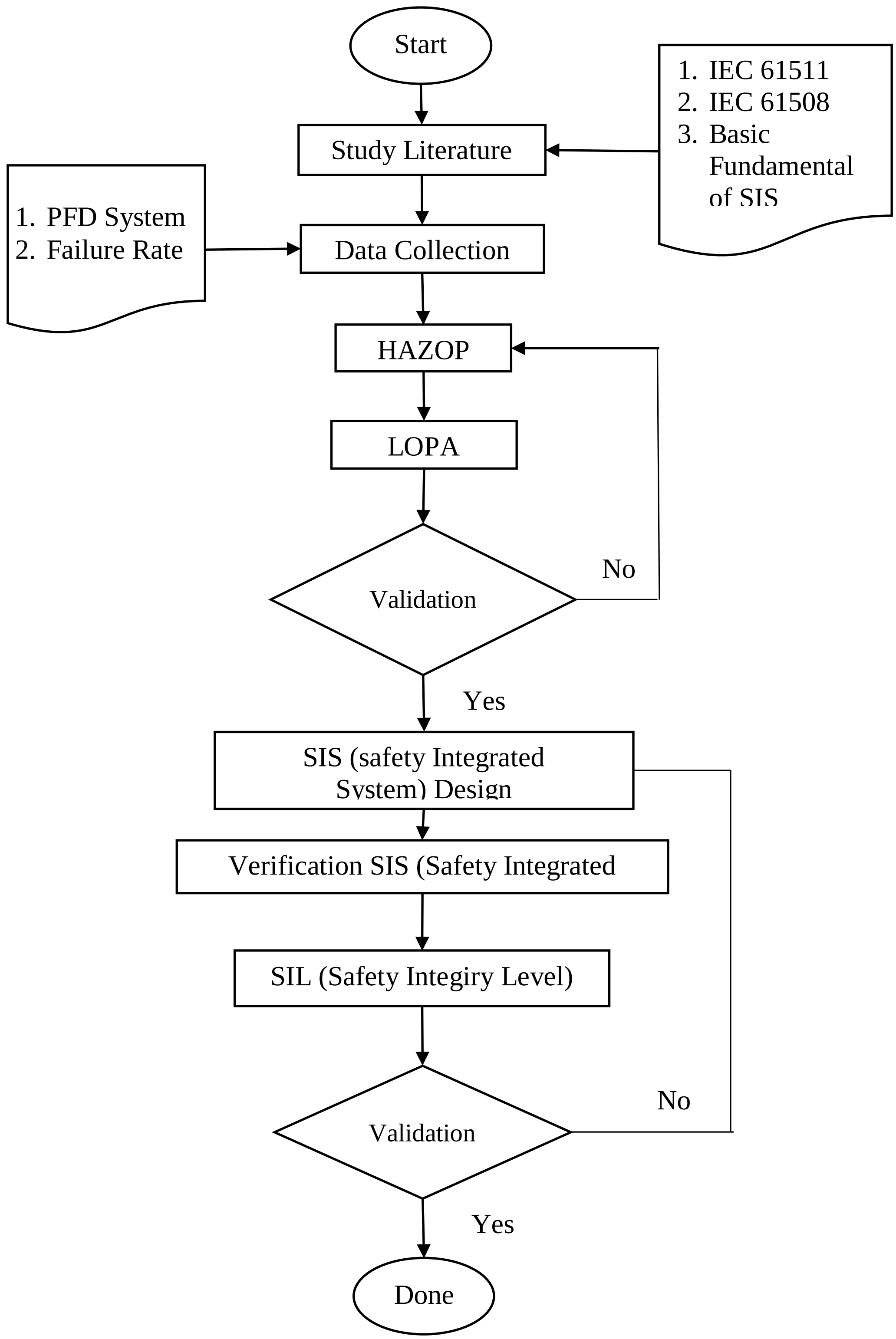


Figure. 3.1 Methodology Flowchart

3.3. HAZOP (Hazard and Operability)

HAZOP is a standard hazard analysis techniques used in the prepare the establishment of security on the new system or modifications to an existence of potential hazards or operation problem. To start HAZOP needed PFD / P&ID document from the unit that is going to be analyzed, it will be split into some stages according to the unit.

3.3.1. HAZOP Steps

HAZOP detail will be explained on the following step:

a. *Determination of Node*

Node is the point to mark the start and end point of the sub-system. HAZOP study will do on each sub-system.

b. *Determination of Deviation*

Based on IEC 61882 Hazard and Operability Studies (HAZOP studies) - Application guide [5].

c. *Determination of Parameter*

The parameter is the measure or limitation, also used to know as if the determined deviation will happen to each node. The parameter of each deviation of every node will different.

d. *Likelihood*

The likelihood is the chance of LNG released to the environment because of leakage or PVS (Pressure Safety Valve) activated because of overpressure. Based on the presentation of Daniel R. Lewin Hazard and Operability Studies [6].

e. *Severity Analysis*

Severity is the effect that might happen when the LNG released to the air. There are 3 possible effects that might be happened, for example to the human, to the operation and the financial effect.

f. Risk Ranking

The risk is when the cause of risk meets the source of risk. Risk based on the presentation of Daniel R. Lewin Hazard and Operability Studies categorized into 4 classes [6].

The output of HAZOP is a report, HAZOP worksheet will be used to complete LOPA worksheet. Data can be further seen in **attachment 1**.

3.4. LOPA (LAYER OF PROTECTION ANALYSIS)

LOPA (Layer of Protection Analysis) is an analysis method that works on the placement of protection layers to protect the plant adjusted to the possibility of what might happen if the plant in danger [8]. LOPA method used after completing HAZOP because the output results of HAZOP report on this method as the placement of protective layer to protect the plant. Layers of protection are Independent, means that if one layer has a problem then it will not affect the other layers so that there are still some others protective layer to anticipate.

3.5. SIS (SAFETY INSTRUMENTED SYSTEM) DESIGN

SIS design is made to meets the requirement IEC 61508 on Safety Life Cycle as guidance to SIS design. On this SIS design only has a plan and design, do not continue to installation and operation stage, and only about analysis and realization. Data needed to complete this stage are some detail data about the LNG, specification of the storage tank, and the specification of loading pump.

3.5.1. Conceptual Process Design

Research on the Storage Loading facilities, especially on storage and loading liquid LNG. This unit has divided into some parts, which are Storage Tank, Liquid LNG Storage and Loading Pump that will carry the LNG to the last part (Berth or port) where the LNG transfers from onshore to the LNG vessel.

3.6. VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM)

Verification of SIS aims to find out what is the SIL achieved, and the value of SIL represented the security level of the plant. The smaller the value of SIL, the greater the risk that would be obtained in the event of a catastrophic.

3.6.1. Develop Safety Requirement

To perform the verification analysis on Safety Instrumented System that must be done by collect some data that contains specifications, instrument number, piping systems, process systems and another data. Most of the data obtained from the PFD that contains a description of a process and the control of a unit. All of the data collected will be analyzed and classified into several categories according to running processes. At SIS analysis requires also the value of each instrument failure rate SIS on the field, this value will be calculated to obtain the value of SIL.

3.6.2. Perform SIS (Safety Instrumented System) Conceptual Design

SIS verification has some method; one of them is Simplified Method. In this case, Simplified Method will be used because it is easy to do. Simplified Method is a method used for verification and cannot be separated from the main elements of this method is PFD (Probability

Failure on Demand) number. PFD is a failure number that owned by the equipment when it needs to work. For example, failure to activated alarm when desired, or failure of the control valve to close when it is desirable to close. To determine SIL need some calculation of SFF and PFD. Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

- *The fraction of failures*

  Safety of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF).

- *Hardware Fault Tolerance (HFT)*

  The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset.

- *Average probability* of hazardous failures for a safety function on demand (PFDavg)

  Determine the value of the PDF (probability of failure on demand) of the components that support the same safety system on the node. PFDavg value as the main element of the calculation, while the value obtained from the equation PFDavg meet the standard of the architecture of a system.

3.7. SIL (SAFETY INTEGRITY LEVEL) TARGET

As follows the standard used by the IEC as an international organization that forms the standard of safety and followed by the entire world, in the standard IEC 61 058 EN 1473 : 2007 states "Standard required value of SIL 3 is EN 1473 : 2007, Installation of equipment for Liquefied Natural Gas - Design onshore installation, requiring SIL 3 systems for Emergency Shut Down Valve" [3]. “Discrete level (one out of a possible four) for specifying the probability of a SIS satisfactorily performing the required SIF under all of the stated conditions within a stated period of time." (Definition from ICM-DU-6025). Based on these standards, the authors follow that the entire SIF, SIS on the system to be made must meet SIL 3 value in terms of architecture, design, and the level of security.

This Page Intentionally Left Blank

CHAPTER 4
DATA ANALYSIS

In this chapter, the results of the analysis and verification of the existing SIS and SIS design of the new design will be explained in detail. Previously described prior analysis and verification of the SIS long, and after concluding the result will be explained in the design and analysis of the new SIS system

4.1. STUDY LITERATURE

The first step is study literature. In this step can be done by searching and studying about something that related to the problems. Literature studies also can be done by reviewing the paper or a journal dealing with the problems to be solved. Table 1.1 show the result of study literature reviewing.

Table 4. 1 Study Literature Result

Literature	Review
ABB	Guideline to the calculation step
IEC 61508	Guideline to step required
Layer of protection analysis (LOPA) for determination of safety integrity	Guideline to analyze the layer

4.2. HAZOP (Hazard and Operability)

HAZOP has the scenario and condition of the running operation of the unit, so based on several variable measured will cause a different effect on each running system. Also based on HAZOP the previous condition of the asset can be known as if it has not reached the safety level requirement. The previous system does not have many layers of protection on several conditions, mostly it only has BPCS and PSV on pressure and overflow. With this condition the system needs more layer of protection before sharply reaching the mitigation, the hazardous event happened and become too risky if the simple layer used to the system.

4.2.1. HAZOP Steps

HAZOP detail will be explained on the following step:

a. *Determination of Node*

Node is the point to mark the start and end point of the sub-system, on this plan, there are 3 subsystems consist of:

1. Storage Tank Input
2. Storage Tank Process
3. Storage Tank Output 1
4. Storage Tank Output 2

HAZOP study will do on each sub-system.

b. *Determination of Deviation*

Based on IEC 61882 Hazard and Operability Studies (HAZOP studies) - Application guide [5], there are 8 deviations that might happened along the operation of the plan, such as:

1. No Flow
2. Low Flow
3. More/High Flow
4. Reverse/Misdirected Flow
5. Less/Low Pressure
6. High Pressure
7. Less/Low Temperature
8. High Temperature

c. *Determination of Parameter*

The parameter is the measure or limitation, also used to know as if the determined deviation will happen to each node. So each node will have its own HAZOP based on 8 determined deviation, but the parameter of each deviation of every node will different.

d. *Likelihood*

The likelihood is the chance of LNG released to the environment because of leakage or PVS (Pressure Safety Valve) activated because of overpressure. Based on the presentation of Daniel R. Lewin Hazard and Operability Studies [6].

e. *Severity Analysis*

Severity is the effect that might happen when the LNG released to the air. There are 3 possible effects that might be happened, for example to the human, to the operation and the financial effect.

f. *Risk Ranking*

The risk is when the cause of risk meets the source of risk. Risk based on the presentation of Daniel R. Lewin Hazard and Operability Studies [6] categorized into 4 classes as mentioned in Chapter 2. Risk ranking determined from risk matrix. The risk matrix is the combination of likelihood number on the left side and severity number on the bottom. The example of risk matrix shown in Figure 2.11.

The output of HAZOP is a report; HAZOP worksheet will be used to complete LOPA worksheet. Data can be further seen in **attachment 2 .**

Figure 4. 1 HAZOP Worksheet

The output of HAZOP is a report, for example in Figure 4.1. HAZOP worksheet will be used to complete LOPA worksheet. HAZOP analysis and the risk analysis shown in **attachment 3.**

4.3. LOPA (Layer of Protection Analysis)

Layer of Protection Analysis (LOPA) focuses on the risk reduction effort towards the impact event and provide rational basis to allocate risk reduction resources efficiently. It is a consequence based method and first start using the data from HAZOP output and suggest screening values and methodology account for further risk reduction for each safeguard. Mitigated risk for impact event can be compared with the Clients criteria for unacceptable risk. The additional Independent Protection Layer (IPL) can then be added and required safety integrity level (SIL) for SIS can be determined.

On storage tank has some hazardous condition on some spot. On input and output has some flow parameter can possibly lead to hazardous condition and BPCS as first protection layer set up to cover the failure. If BPCS failed to cover, Alarm that operated by the operator will take place to cover it. If Alarm still failed SIS will replace the Alarm by using an automatic system to close the valve and isolated the flow so the flow will run normally again. If the system has some condition that SIS cannot handle, Passive Device will take place over SIS, but this situation also is known as mitigation to reduce the effect of the hazard.

The next step is to categorize based on new IPL. IPL should protect the plant from a hazardous situation. The more layer, the safer the plant. Each layer of protection can be the backup if the previous layer cannot cover the failure. This layer goes on from prevention to the mitigation. This conditions can reduce the number of casualties if the hazardous situation happened. (LOPA worksheet can be found on attachment. Table 4.2 shows the LOPA of storage tank input.

Table 4. 2 LOPA of Storage Tank Input

Layer of Protection Analysis (LOPA) - Storage Tank Input							
No	Parameter	Deviation	Scenario	Layer 1	Layer 2	Layer 3	Layer 4
1	Flow	None	Empty Pipe	BPCS	-	-	-
2	Flow	Less	Pressure Increasing	BPCS	Alarm	SIS	Passive
3	Flow	More	Pressure Decreasing	BPCS	Alarm	SIS	Passive
4	Flow	Reverse	Flow Turbulence	-	-	-	Passive
5	Temperature	More	LNG Evaporating	BPCS	-	-	-
6	Temperature	Less	LNG Freezing	BPCS	-	-	-
7	Pressure	More	Ruptured Pipe	BPCS	Alarm	SIS	Passive
8	Pressure	Less	Ruptured Pipe	BPCS	Alarm	SIS	Passive

LOPA worksheet can be found in **attachment 3.**

4.4. SIS (SAFETY INSTRUMENTED SYSTEM) DESIGN

SIS design is made to meets the requirement IEC 61508 on Safety Life Cycle as guidance to SIS design. On this SIS design only has plan and design, do not continue to installation and operation stage, so it is only about analysis and realization. Data needed to complete this stage are some detail data about the LNG, specification of the storage tank, and the specification of loading pump.

4.4.1. Conceptual Process Design

Research already was done on the Storage Loading facilities, especially on storage and loading liquid LNG. This unit has divided into some parts, which are Storage Tank, Liquid LNG Storage and Loading Pump that will carry the LNG to the last part (Berth or port) where the LNG transfers from onshore to the LNG vessel. The process occurs in storage that will proceed to the port through the pump as a medium that delivers the LNG through pipelines.

Based on data process and specification, the flow chart on Storage Loading Facilities on Figure 2.13 is done. Conceptual design is completed, data is completed so the next step can ben done based on this conceptual design.

4.5. VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM)

The appropriate standard of IEC 61058 is a method on the Safety of Life Cycle as a guide to verify the SIS. By analyzing the SIL of the SIS is intended to determine the value of existing systems. Some numbers of failure factors as consider the existing system.

4.5.1. Develop Safety Requirement

Grouping the data into ESD (Emergency Shutdown) shows which equipment that will be active when the ESD system is activated. ESD group used are ESD I, ESD II, and ESD III as shown in Table 4.3 and 4.4 and also Table 4.5 shows the Failure Rate number.

Table 4. 3 ESD Final Element Indicated with "V"

No	Equipment	Valve Type	ESD1	ESD2	ESD3
1	HV 6818-A	*Hydraulic* - Gate valve	v	v	
2	HV 6818-B	*Hydraulic* - Gate valve	v	v	
3	HV 6818-D	*Hydraulic* - Gate valve	v	v	
4	HV 6819-1	*Hydraulic* - Butterfly valve	v	v	
5	HV 6819-2	*Hydraulic* - Butterfly valve	v	v	
6	HV 6832-A	*Hydraulic* - Butterfly valve	v	v	v

Table 4. 4 ESD Final Element Indicated with "V" (continue)

No	Equipment	Valve Type	ESD1	ESD2	ESD3
7	HV 6832-B	*Hydraulic* - Butterfly valve	v	v	v
8	HV 6832-D	*Hydraulic* - Butterfly valve	v	v	v
9	HV 6832-E	*Hydraulic* - Butterfly valve	v	v	v
10	HV 6833-A	*Hydraulic* - Butterfly valve	v	v	v
11	HV 6833-B	*Hydraulic* - Butterfly valve	v	v	v
12	HV 6833-C	*Hydraulic* - Butterfly valve	v	v	v
13	HV 6833-E	*Hydraulic* - Butterfly valve	v	v	v
14	HV 68103-1	Solenoid - Gate valve	v	v	v
15	HV 68103-2	Solenoid - Gate valve	v	v	v

Table 4. 5 Failure Rate

No	Equipment	Valve Type	Interval (Hours)	λ^S Failure Safe	λ^{DD} Failure Danger Detected	λ^{DU} Failure Danger Undetected	Failure Rates
1	HV 6818-A	Hydraulic – Gate valve	8760	3.60E-06	0	1.40 E-06	5.00 E-06
2	HV 6818-B	Hydraulic – Gate valve	8760	5.50E-07	0	1.10 E-07	6.6-E-07
3	HV 6818-D	Hydraulic – Gate valve	8760	4.10E-07	0	1.20 E-07	5.30 E-07
4	HV 6819-1	Hydraulic – Butterfly valve	8760	3.43 E-06	0	1.40 E-07	3.57 E-06
5	HV 6819-2	Hydraulic – Butterfly valve	8760	3.40 E-06	0	1.80 E-06	5.20 E-06
6	HV 6832-A	Hydraulic – Butterfly valve	8760	4.65 E-06	0	3.80 E-07	5.03 E-06
7	HV 6832-B	Hydraulic – Butterfly valve	8760	7.27 E-06	0	4.45 E-07	7.27 E-06
8	HV 6832-D	Hydraulic – Butterfly valve	8760	4.21 E-06	0	1.89 E-06	6.10 E-06
9	HV 6832-E	Hydraulic – Butterfly valve	8760	4.69 E-06	0	1.62 E-06	6.31 E-06
10	HV 6833-A	Hydraulic – Butterfly valve	8760	4.43 E-06	0	2.36 E-07	4.67 E-06
11	HV 6833-B	Hydraulic – Butterfly valve	8760	4.04 E-06	0	1.54 E-06	5.58 E-06
12	HV 6833-C	Hydraulic – Butterfly valve	8760	3.90 E-06	0	2.05 E-06	5.95 E-06
13	HV 6833-E	Hydraulic – Butterfly valve	8760	3.39 E-06	0	1.26 E-07	3.52 E-06
14	HV 68103-1	Solenoid – Gate valve	8760	3.21 E-06	0	1.20 E-07	3.33 E-06
15	HV 68103-2	Solenoid – Gate valve	8760	4.41 E-06	0	6.52 E-06	1.09 E-05

Table of ESD grouping also can be found in **attachment 4** and failure rate table can be found in **attachment 5**.

4.5.2. Perform SIS (Safety Instrumented System) Conceptual Design

To determine SIL need some calculation of SFF and PFD. Data were taken from failure rates Table 3.11. Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

- *The fraction of failures* that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061 as mentioned on equation (2.1.).

  For example, the calculation of HV 6818-A Hydraulic - Gate valve, data can be found on Failure Rate Table row 1.

  $$\begin{aligned} SFF &= (\lambda^{S} + \lambda^{DD})/(\lambda^{SU} + \lambda^{DD} + \lambda^{DU}) \\ &= (3.60E\text{-}06 + 0)/(3.60E\text{-}06 + 0 + 1.40E\text{-}06) \\ &= 72\% \end{aligned}$$

  As the calculation of Failure Rate shows on Table 4.5 mostly the value of the instrument capable of SIL means capable of using SIL 1 or 2, is not the instrument has a value of SIL 1 or 2, capable only. With the conclusion of Table 4.4 shows that the amount of value SIL of each valve contained on the system ESD where value is dominated by the value of SIL 1, with a view maximum valve has a SIL 2, while based on the IEC standards for an industry major with a system that continuously as industry oil or gas should have a standard value for a field instrument with A type is capable of SIL 2 or 3. Table 4.6 shows the calculation result based on the valve.

Table 4. 6 Calculation Result Based on Valve

No	Equipment	SFF	SIL
1	HV 6818-A	72%	3
2	HV 6818-B	83%	3
3	HV 6818-D	77%	3
4	HV 6819-1	96%	3
5	HV 6831-A	65%	3
6	HV 6832-B	92%	3
7	HV 6831-D	94%	3
8	HV 6832-E	69%	3
9	HV 6833-1	74%	3
10	HV 6833-A	95%	3
11	HV 6833-B	72%	3
12	HV 6833-C	66%	3
13	HV 6833-E	96%	3
14	HV 68103-1	96%	3
15	HV 68103-2	40%	2

- *Hardware Fault Tolerance (HFT)*

  In this unit, the valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD, which has 1/1, it means the use of the single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset.

The Table of HFT (Hardware Fault Tolerance) shown in Table 4.7.

Table 4. 7 Architecture Type A

Type A	**0**	**1**	**2**
< 60 %	SIL 1	SIL 2	SIL 3
60 % < 90 %	SIL 2	SIL 3	SIL 4
90% < 99 %	SIL 3	SIL 4	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4

- *Average probability* of hazardous failures for a safety function on demand (PFDavg).

  Determine the value of the PDF (probability of failure on demand) of the components that support the same safety system on the node. PFDavg value as the main element of the calculation, while the value obtained from the equation PFDavg meet the standard of the architecture of a system, because the ESD unit is activated via a push button that located in the control room storage loading facilities, With the flow of the Push Button - Logic Solver - Final Elements, then the system goes into the category of system 1/1 (1 out of 1) and the equation used to PFDavg mentioned on equation (2.2).

  For example, the calculation of HV 6818-A Hydraulic - Gate valve, data can be found on Failure Rate Table of Logic Solver.

$$\begin{aligned} \text{PFDavg} &= [1\ (\lambda^{DU} \text{ x TI})] / 2 \\ &= [1\ (0.0000024 \text{ x } 8760)] / 2 \\ &= 0.00000613 \\ &= 6.13\text{E-}03 \end{aligned}$$

Table 4.8 shows the PFDavg of the logic solver and Table 4.9 shows the PFDavg of final elements.

Table 4. 8 PFD Average of Logic Solver

No	Element	Unit	PFDavg
1	Logic Solver	Yokogawa Prosafe-RS	1.68E-06
2	Push Button	PB-Yokogawa Prosafe-RS	1.60E-05

Total PFDavg = 1.68E-06 + 1.60E-05
= 1.77E-05

Table 4. 9 PFD Average of Final Elements

No	Equipment	Pfdavg
1	HV 6818-A	6.13E-03
2	HV 6818-B	4.82E-04
3	HV 6818-D	5.26E-04
4	HV 6819-1	6.13E-04
5	HV 6831-A	7.88E-03
6	HV 6832-B	1.66E-03
7	HV 6831-D	1.95E-03
8	HV 6832-E	8.28E-03
9	HV 6833-1	7.10E-03
10	HV 6833-A	1.03E-03
11	HV 6833-B	6.75E-03
12	HV 6833-C	8.98E-03
13	HV 6833-E	5.52E-04
14	HV 68103-1	5.26E-04
15	HV 68103-2	2.86E-02

The calculation by using Simplified Method need the equation mentioned on equation (2.3).

And the total calculation of PFDavg Logic Solver and Final Element as shown below:

$$\begin{aligned} \mathrm{PFD}avg^{SIF} &= \sum \mathrm{PFD}avg^{LS} + \sum \mathrm{PFD}avg^{FE} \\ &= 5.40\text{-}03 + 1.77\mathrm{E}\text{-}05 \\ &= 5.42\mathrm{E}\text{-}03 \end{aligned}$$

Detail of calculation can be found in **attachment 6**.

4.6. SIL (SAFETY INTEGRITY LEVEL) TARGET

Based on these standards, the authors follow that the entire SIF, SIS on the system to be made must meet SIL 3 value in terms of architecture, design, and the level of security. And based on the calculation of SFF and PFD average the system meets the requirement of IEC stardard.

This Page Intentionally Left Blank

ATTACHMENT I - DATA

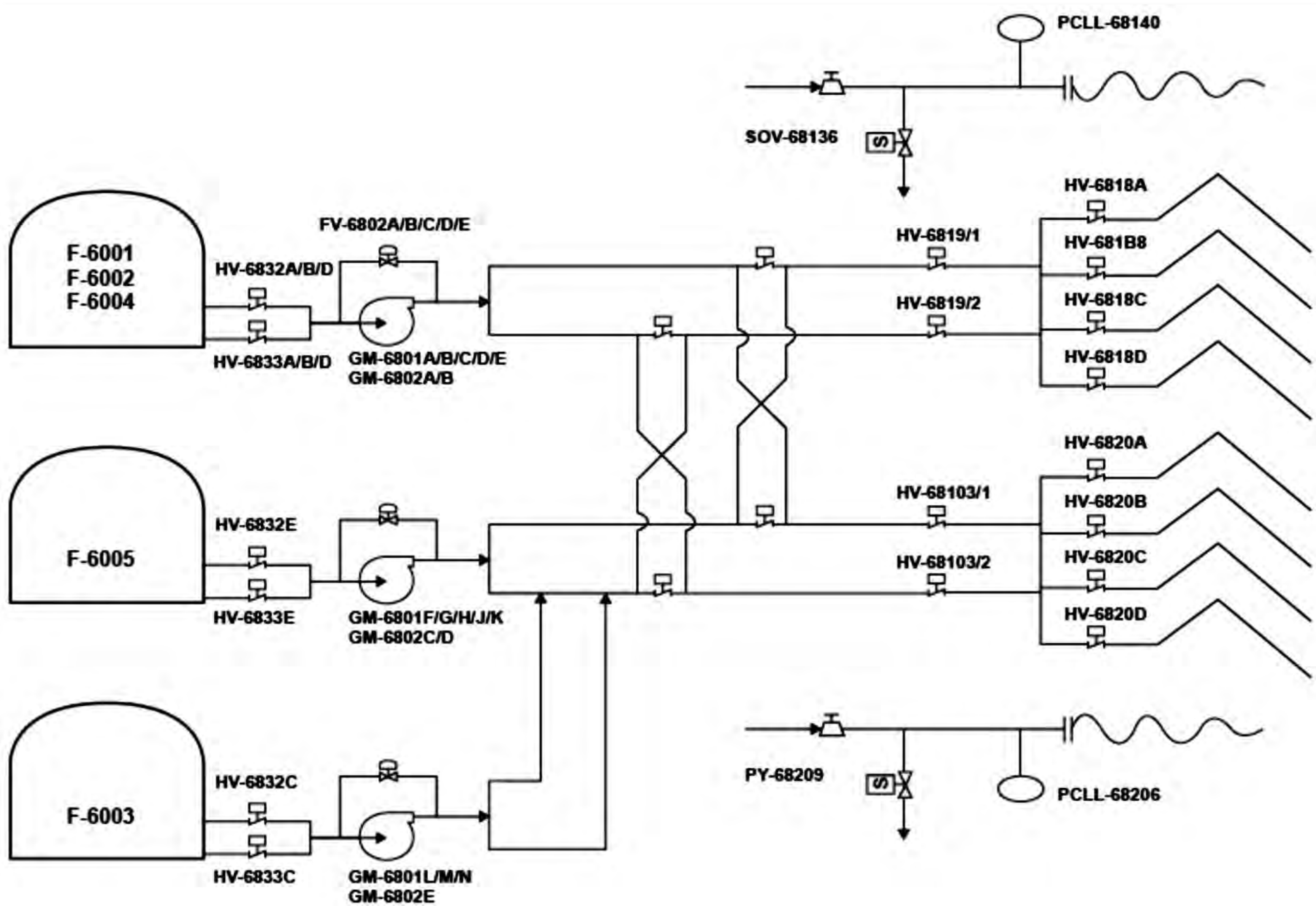


Figure 1. Overall PFD of SIS System

P.T. ARUN OPERATING MANUAL

UNIT 60 AND 68: PAGE:3

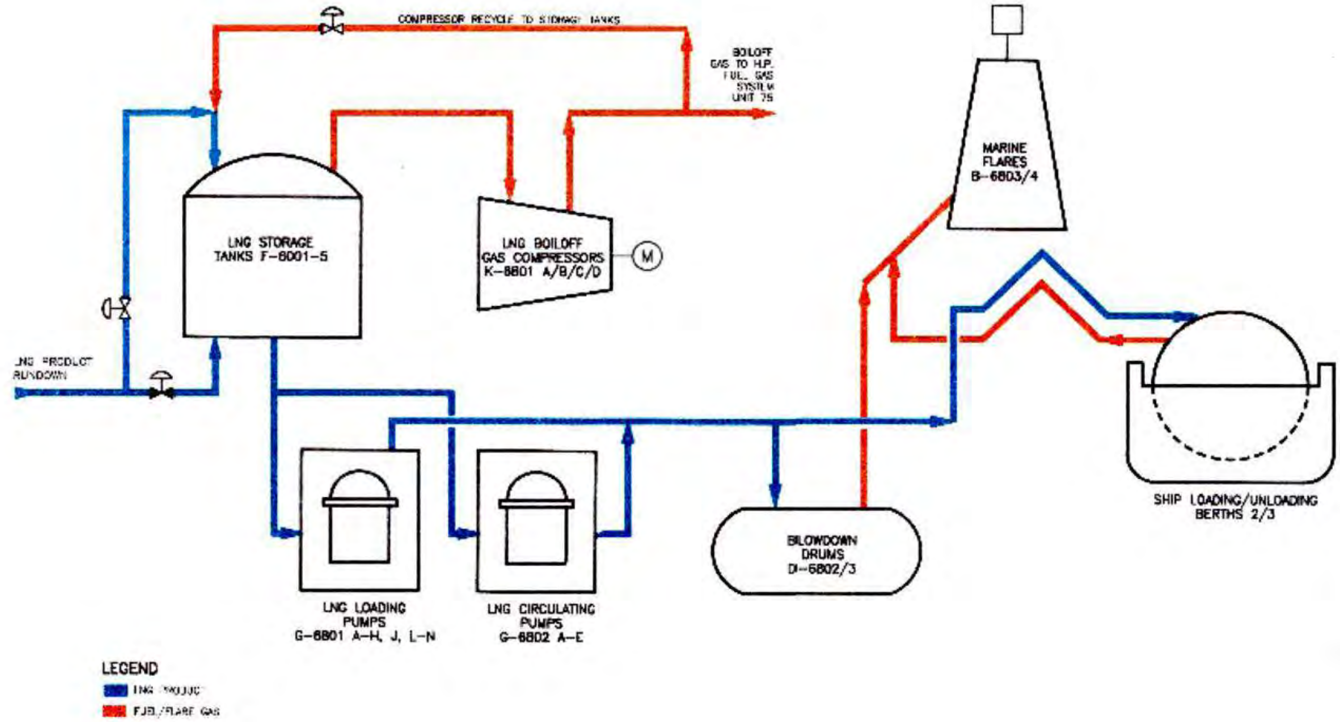


FIGURE 2.0 LNG STORAGE AND LOADING

9049066

Figure 2. PFD of Loading Facilities Storage Process

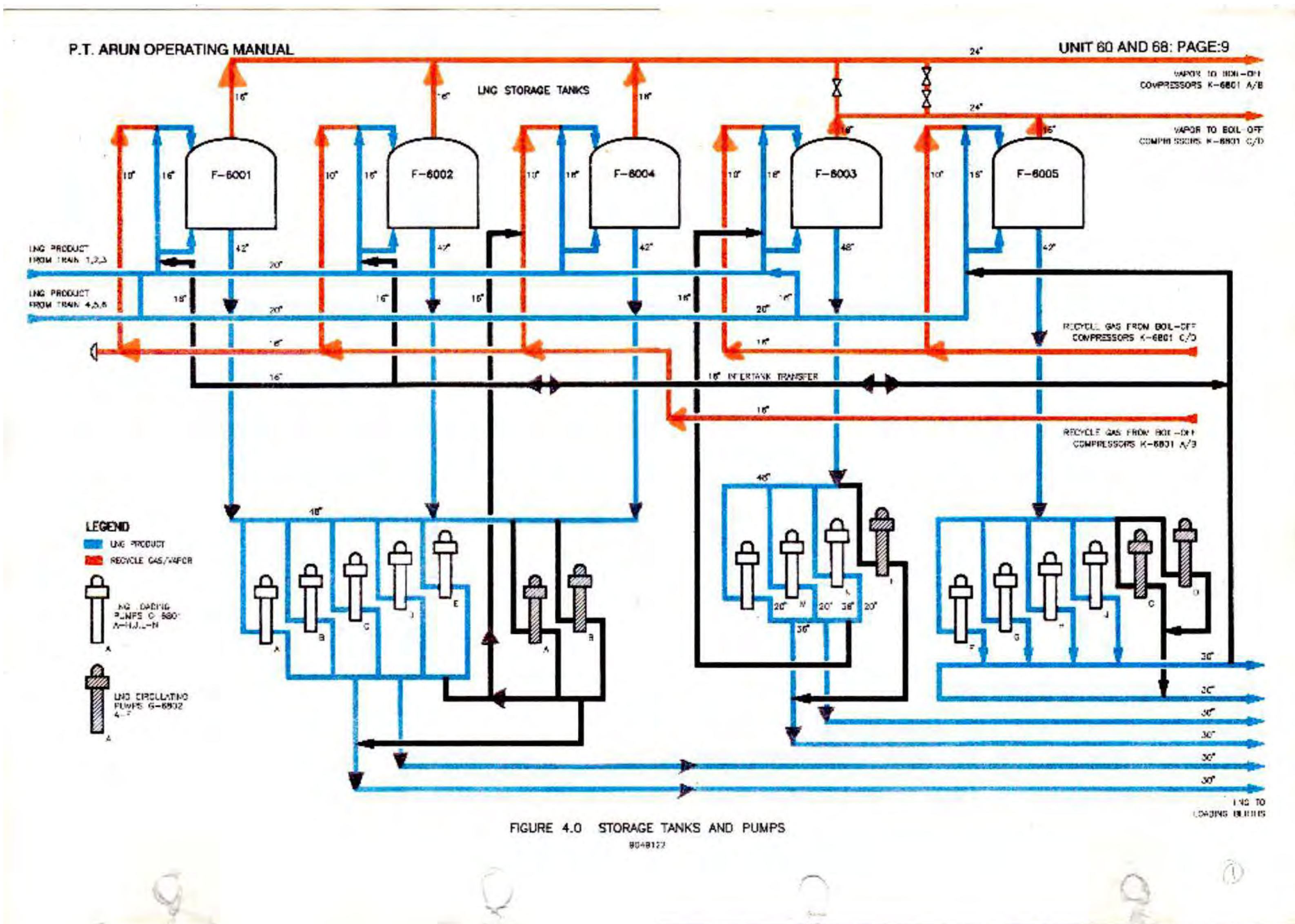


Figure 3. PFD of Process Storage Tank & Loading Pump

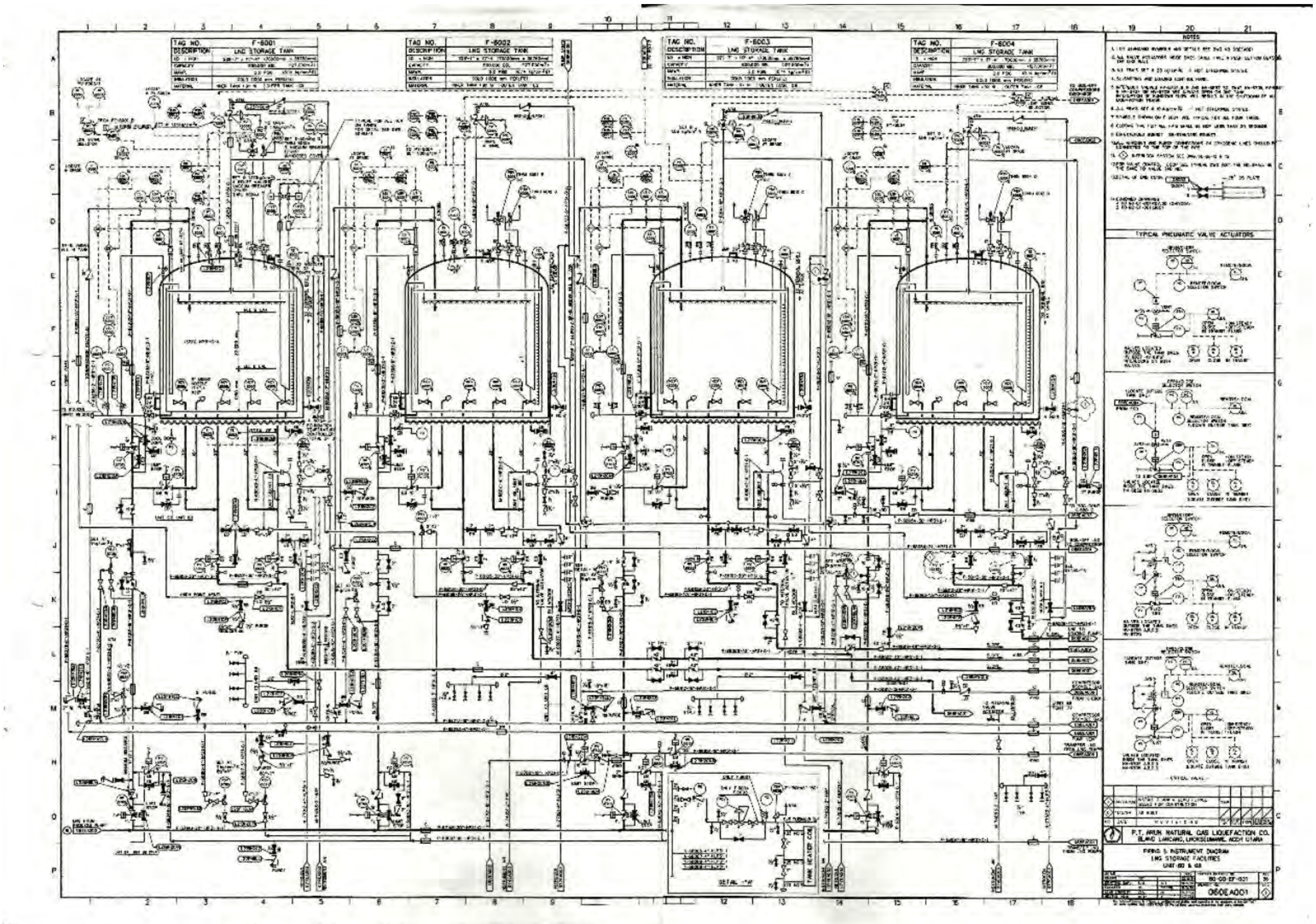


Figure 4. Piping and Instrument Diagrams for Storage Tank

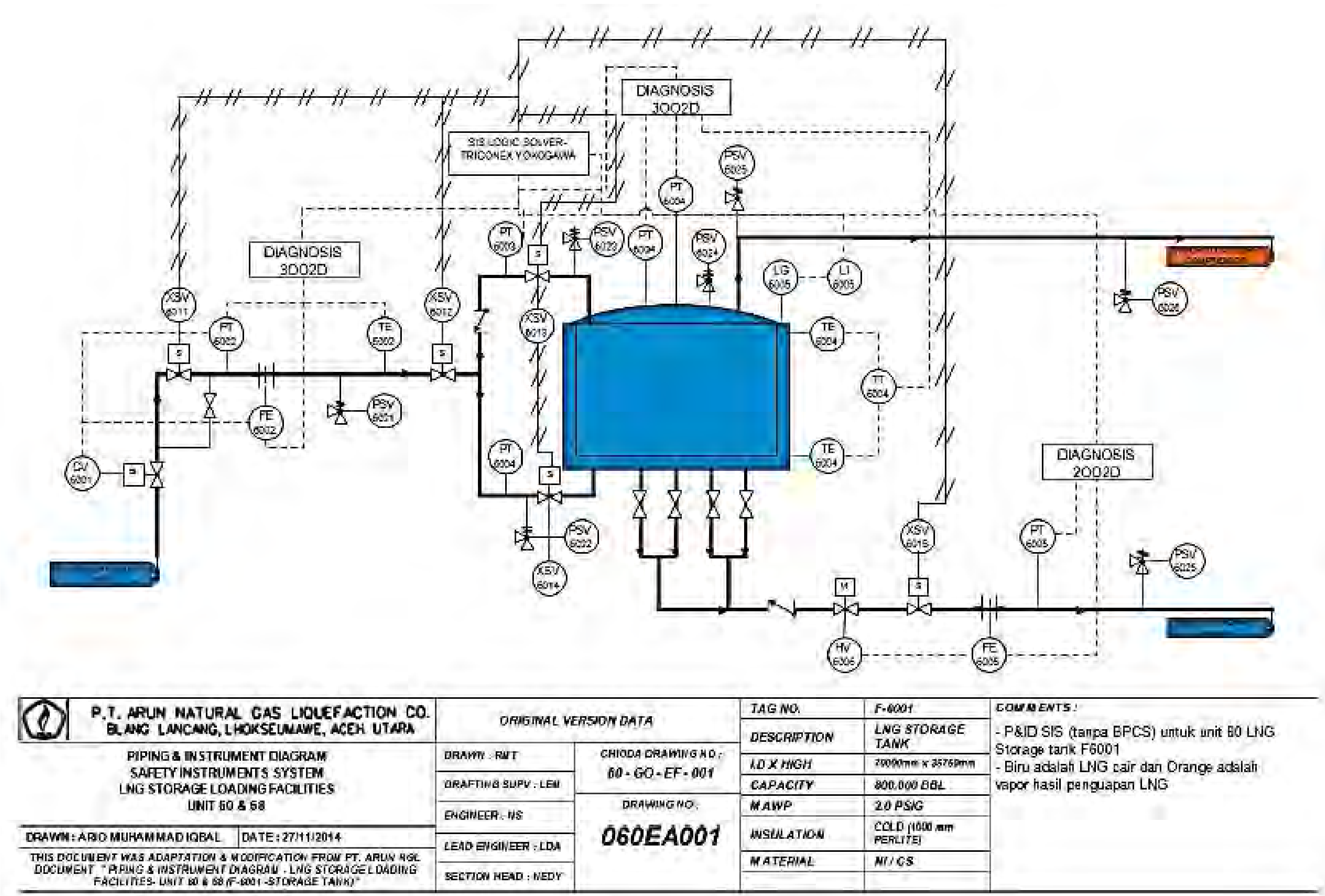
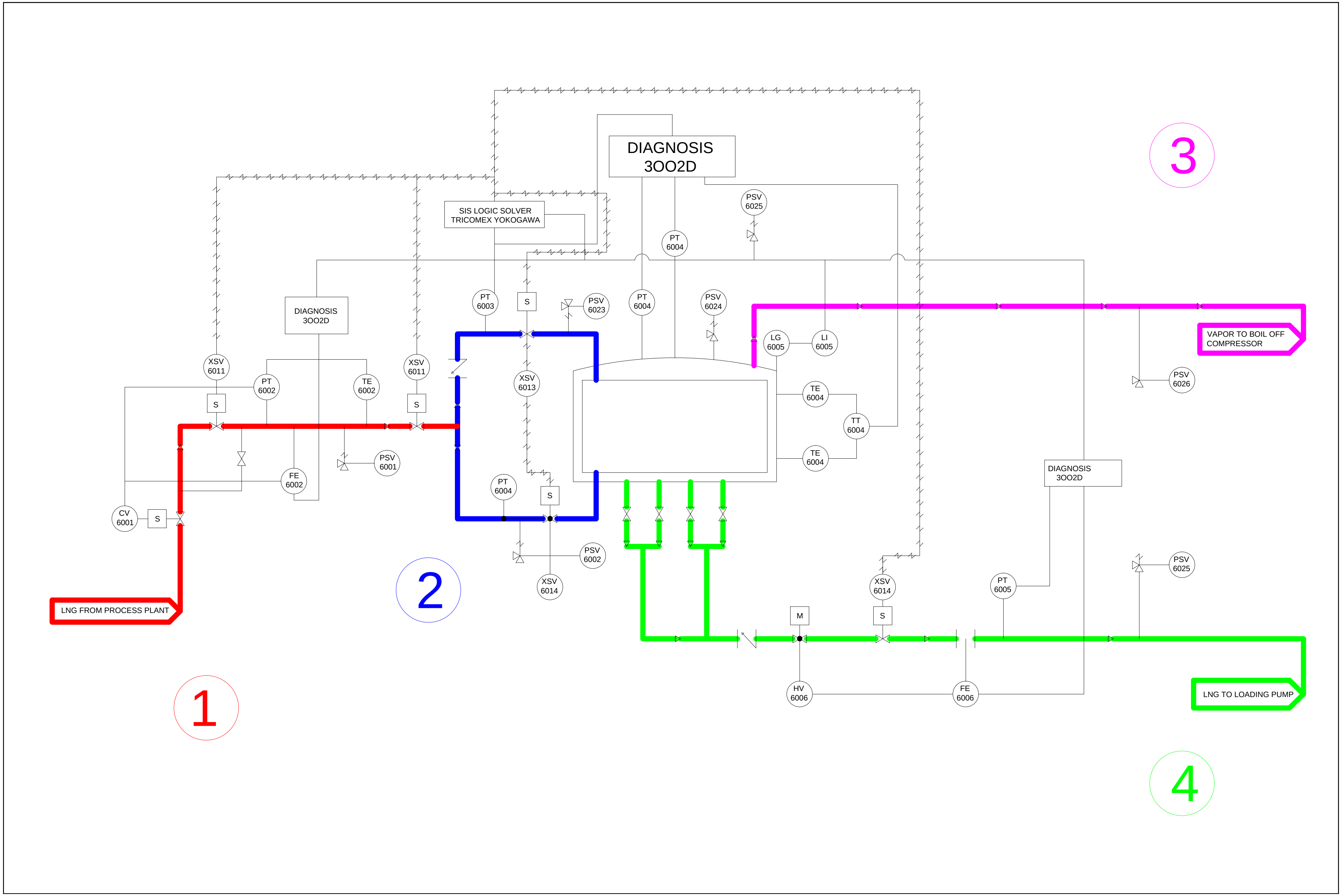


Figure 5 PFD of SIS on Storage Tank


DIAGNOSIS 3OO2D
SIS LOGIC SOLVER TRICOMEX YOKOGAWA
PSV 6025
PT 6004
DIAGNOSIS 3OO2D
PT 6003
S
PSV 6023
PT 6004
PSV 6024
XSV 6011
XSV 6011
LG 6005
LI 6005
VAPOR TO BOIL OFF COMPRESSOR
PT 6002
TE 6002
S
S
XSV 6013
TE 6004
PSV 6026
TT 6004
PSV 6001
FE 6002
TE 6004
DIAGNOSIS 3OO2D
PT 6004
S
CV 6001
S
PSV 6002
PSV 6025
XSV 6014
PT 6005
LNG FROM PROCESS PLANT
XSV 6014
M
S
HV 6006
FE 6006
LNG TO LOADING PUMP
1
2
3
4

No	Node	Deviation	Parameters
1	Storage Tank Input	No Flow	No LNG in pipeline
		Less Flow	Capacity of LNG less than 600.000BBL
		More Flow	Capacity of LNG more than 700.000BBL
		Reverse Flow	LNG is not through a Planned
		Less Pressure	Discharge Pressure less than 4 bar
		More Pressure	Discharge Pressure more than 8 bar
		Less Temperature	Temperature of storage tank less than -170°C
		More Temperature	Temperature of storage tank more than -120°C
2	Storage Tank Process	No Flow	No LNG in pipeline
		Less Flow	Capacity of LNG less than 600.000BBL
		More Flow	Capacity of LNG more than 700.000BBL
		Reverse Flow	-
		Less Pressure	Discharge Pressure less than 4 bar
		More Pressure	Discharge Pressure more than 8 bar
		Less Temperature	Temperature of storage tank less than -170°C
		More Temperature	Temperature of storage tank more than -120°C
3	Storage Tank Output	No Flow	No LNG in pipeline
		Less Flow	Capacity of LNG less than 600.000BBL

No	Node	Deviation	Parameters
		More Flow	Capacity of LNG more than 700.000BBL
		Reverse Flow	-
		Less Pressure	Discharge Pressure less than 4 bar
		More Pressure	Discharge Pressure more than 8 bar
		Less Temperature	Temperature of storage tank less than -170°C
		More Temperature	Temperature of storage tank more than -120°C

HAZOPS Worksheet for Node 1 "Storage Tank Input"

HAZOP STUDY RECORD SHEET					PROJECT : FRU			
			Node : 1				SYSTEM : LNG Storage Tank	
P&ID : *60 – GD – EF – oo1 "LNG Storage Tanks"*			**EQUIPMENT / LINE TAG:** LNG Storage Tanks (F-6001) Loading Pump (G-6801)				**DESIGN INTENT:**	
No	**Deviation**	**Causes**	**Consequences**	**Risk Ranking**			**Safeguards**	**Action Required**
				S	L	RR		
1	No Flow	CV-6001 XSV-6011 and XSV-6012 are closed	Empty pipe	2	2	A (4)	PSV-6021	Ensure valve are open in the order
2	Less Flow	CV-6001, XSV-8012 and XSV-8012 are not perfectly open	Pressure Increasing	4	2	C (8)	PSV-6021	Ensure CV-6001, XSV-6011 and XSV-8012 are opened

No	Deviation	Causes	Consequences	Risk Ranking			Safeguards	Action Required
				S	L	RR		
3	More flow	Flow from the train increasing	Pressure Decreasing	4	2	C (8)	PSV-6021, CV-6001	Monitor the flow
4	Reverse Flow	Instable pressure	Flow Turbulence	4	3	D (12)	-	Monitor the flow
5	Less pressure	PSV are opened	Ruptured pipe	2	2	A (4)	PT-6002	Monitor the pressure
6	More Pressure	XSV-6012 closed	Ruptured pipe	2	3	B (6)	PT-6002	Monitor the pressure
7	Less temperature	-	LNG Freezing	4	3	D (12)	FE-6002	-
8	More Temperature	-	LNG Evaporating	4	3	D (12)	FE-6002	-

HAZOPS Worksheet for Node 2 "Storage Tank Process"

HAZOP STUDY RECORD SHEET			PROJECT : FRU				
			Node : 2			SYSTEM : LNG Storage Tank	
P&ID : *60 – GD – EF – oo1 "LNG Storage Tanks"*			**EQUIPMENT / LINE TAG:** LNG Storage Tanks (F-6001) Loading Pump (G-6801)			**DESIGN INTENT:**	

No	Deviation	Causes	Consequences	Risk Ranking			Safeguards	Action Required
				S	L	RR		
1	No Flow	XSV-6013 and XSV-6014 are closed	Empty tank	2	2	A (4)	PSV-6022, PSV-6023 and PSV-6024	Ensure valve are open in the order
2	Less Flow	XSV-8013 and XSV-8014 are not perfectly open	Low Capacity	4	2	C (8)	PSV-6021	Ensure XSV-8013 and XSV-8014 are opened
3	More flow	Pressure on storage tank decreasing	Pressure Decreasing	4	2	C (8)	PSV-6021, CV-6001	Monitor the flow

No	Deviation	Causes	Consequences	Risk Ranking			Safeguards	Action Required
				S	L	RR		
4	Reverse Flow	-	Flow Turbulence	4	3	D (12)	PSV-6022, PSV-6023 and PSV-6024	Monitor the flow
5	Less pressure	-	Leakage on Tank	2	2	A (4)	PSV-6022, PSV-6023, PSV-6024, PT-6003 and PT-6004	Monitor the pressure
6	More Pressure	-	Leakage on Tank	2	3	B (6)	PSV-6022, PSV-6023, PSV-6024, PT-6003 and PT-6004	Monitor the pressure
7	Less temperature	-	LNG Freezing	4	3	D (12)	-	-
8	More Temperature	Leakage on Tank	LNG Evaporating	4	4	D (12)	-	-

HAZOPS Worksheet for Node 3 “Storage Tank Output 1“

HAZOP STUDY RECORD SHEET			PROJECT : FRU					
			Node : 3				SYSTEM : LNG Storage Tank	
P&ID : *(Number of drawing) “LNG Storage Tanks”*;			**EQUIPMENT / LINE TAG:** LNG Storage Tanks (F-6001) Loading Pump (G-6801)				**DESIGN INTENT:**	
No	**Deviation**	**Causes**	**Consequences**	**Risk Ranking**			**Safeguards**	**Action Required**
				S	L	RR		
1	No Flow	Empty Tank	Empty pipe	2	2	A (4)	PSV-6025	Ensure valve are open in the order
2	Less flow	-	Pressure Increasing	4	2	C (8)	PSV-6025	-
3	More flow	-	-	-	-	-	-	-
4	Reverse Flow	-	-	-	-	-	-	-
5	Less pressure	Pressure from storage tank increasing	Ruptured Pipe	2	3	B (6)	PSV-5025	Monitor the pressure

No	Deviation	Causes	Consequences	Risk Ranking			Safeguards	Action Required
				S	L	RR		
6	More Pressure	Pressure from storage tank decreasing	Ruptured Pipe	2	3	B (6)	PSV-5025	Monitor the pressure
7	Less temperature	-	LNG Evaporating	4	3	D (12)	TE-6004	Monitor the temperature
8	More Temperature	-	LNG Freezing	4	3	D (12)	TE-6004	Monitor the temperature

HAZOPS Worksheet for Node 4 “Storage Tank Output 2“

<table>
<tr><td colspan="3" rowspan="2">HAZOP STUDY RECORD SHEET</td><td colspan="6">PROJECT : FRU</td></tr>
<tr><td colspan="3">Node : 4</td><td colspan="3">SYSTEM : LNG Storage Tank</td></tr>
<tr><td colspan="3">P&ID :
(Number of drawing) “LNG Storage Tanks”;</td><td colspan="3">EQUIPMENT / LINE TAG:
LNG Storage Tanks (F-6001)
Loading Pump (G-6801)</td><td colspan="3">DESIGN INTENT:</td></tr>
<tr><td rowspan="2">No</td><td rowspan="2">Deviation</td><td rowspan="2">Causes</td><td rowspan="2">Consequences</td><td colspan="3">Risk Ranking</td><td rowspan="2">Safeguards</td><td rowspan="2">Action Required</td></tr>
<tr><td>S</td><td>L</td><td>RR</td></tr>
<tr><td>1</td><td>No Flow</td><td>HV-6006 and XSV-6015 are closed</td><td>Empty Pipe</td><td>2</td><td>2</td><td>A (4)</td><td>PSV-6025</td><td>Ensure valve are open in the order</td></tr>
<tr><td>2</td><td>Less flow</td><td>HV-6006 and XSV-6015 are not perfectly open</td><td>Pressure Increasing</td><td>4</td><td>2</td><td>C (8)</td><td>PSV-6025</td><td>-</td></tr>
<tr><td>3</td><td>More flow</td><td>Pressure on tank increasing</td><td>Pressure Decreasing</td><td>4</td><td>2</td><td>C (8)</td><td>PSV-5025</td><td>Monitor the flow, PT-5005</td></tr>
<tr><td>4</td><td>Reverse Flow</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td><td>-</td></tr>
</table>

No	Deviation	Causes	Consequences	Risk Ranking			Safeguards	Action Required
				S	L	RR		
5	Less pressure	Leakage on pipe	Ruptured Pipe	2	3	B (6)	PT-6005 and PSV-6025	Monitor the pressure
6	More Pressure	HV-6006 failed to open	Ruptured Pipe	2	3	B (6)	PT-6005 and PSV-6025	Ensure the valve are open in the order
7	Less temperature	-	LNG Evaporating	4	3	D (12)	TE-6004	Monitor the temperature
8	More Temperature	-	LNG Freezing	4	3	D (12)	TE-6004	Monitor the temperature

ATTACHMENT II – LOPA WORKSHEET

Table 1. Storage Tank Input

Layer of Protection Analysis (LOPA) - Storage Tank Input							
No	Parameter	Deviation	Scenario	Layer 1	Layer 2	Layer 3	Layer 4
1	Flow	None	Empty Pipe	BPCS	-	-	-
2	Flow	Less	Pressure Increasing	BPCS	Alarm	SIS	-
3	Flow	More	Pressure Decreasing	BPCS	Alarm	SIS	-
4	Flow	Reverse	Flow Turbulence	BPCS	Alarm	SIS	Passive
5	Pressure	Less	Ruptured Pipe	BPCS	-	-	-
6	Pressure	More	Ruptured Pipe	BPCS	Alarm	-	-
7	Temperature	Less	LNG freezing	BPCS	Alarm	SIS	Passive
8	Temperature	More	LNG evaporating	BPCS	Alarm	SIS	Passive

Table 2. Storage Tank Process

Layer of Protection Analysis (LOPA) - Storage Tank Process							
No.	Parameter	Deviation	Scenario-Effect	Layer 1	Layer 2	Layer 3	Layer 4
1	Flow	None	Empty tank	BPCS	-	-	-
2	Flow	Less	Low capacity	BPCS	Alarm	SIS	-
3	Flow	More	Pressure decreasing	BPCS	Alarm	SIS	-
4	Flow	Reverse	Flow Turbulence	BPCS	Alarm	SIS	Passive
5	Pressure	Less	Leakage on tank	BPCS	-	-	-
6	Pressure	More	Leakage on tank	BPCS	Alarm	-	-
7	Temperature	Less	LNG freezing	BPCS	Alarm	SIS	Passive
8	Temperature	More	LNG evaporating	BPCS	Alarm	SIS	Passive

Table 3. Storage Tank Output 1

Layer of Protection Analysis (LOPA) - Storage Tank Output							
No	Parameter	Deviation	Scenario-Effect	Layer 1	Layer 2	Layer 3	Layer 4
1	Flow	None	Empty pipe	BPCS	-	-	-
2	Flow	Less	Pressure increasing	BPCS	Alarm	SIS	-
3	Pressure	Less	Ruptured pipe	BPCS	Alarm	-	-
4	Pressure	More	Ruptured pipe	BPCS	Alarm	-	-
5	Temperature	Less	LNG freezing	BPCS	Alarm	SIS	Passive
6	Temperature	More	LNG evaporating	BPCS	Alarm	SIS	Passive

Table 4 Storage Tank Output 2

Layer of Protection Analysis (LOPA) - Storage Tank Output							
No	Parameter	Deviation	Scenario-Effect	Layer 1	Layer 2	Layer 3	Layer 4
1	Flow	None	Empty pipe	BPCS	-	-	-
2	Flow	Less	Pressure increasing	BPCS	Alarm	SIS	-
3	Flow	More	Pressure decreasing	BPCS	Alarm	SIS	-
4	Pressure	Less	Ruptured pipe	BPCS	Alarm	-	-
5	Pressure	More	Ruptured pipe	BPCS	Alarm	-	-
7	Temperature	Less	LNG freezing	BPCS	Alarm	SIS	Passive
8	Temperature	More	LNG evaporating	BPCS	Alarm	SIS	Pasive

ATTACHMENT IV – ESD TABLE

Table 1 ESD Final Element Indicated with "v"

No	Equipment	Valve Type	ESD1	ESD2	ESD3
1	HV 6818-A	*Hydraulic* - Gate valve	v	v	
2	HV 6818-B	*Hydraulic* - Gate valve	v	v	
3	HV 6818-D	*Hydraulic* - Gate valve	v	v	
4	HV 6819-1	*Hydraulic* - Butterfly valve	v	v	
5	HV 6819-2	*Hydraulic* - Butterfly valve	v	v	
6	HV 6832-A	*Hydraulic* - Butterfly valve	v	v	v
7	HV 6832-B	*Hydraulic* - Butterfly valve	v	v	v
8	HV 6832-D	*Hydraulic* - Butterfly valve	v	v	v
9	HV 6832-E	*Hydraulic* - Butterfly valve	v	v	v
10	HV 6833-A	*Hydraulic* - Butterfly valve	v	v	v
11	HV 6833-B	*Hydraulic* - Butterfly valve	v	v	v
12	HV 6833-C	*Hydraulic* - Butterfly valve	v	v	v
13	HV 6833-E	*Hydraulic* - Butterfly valve	v	v	v
14	HV 68103-1	Solenoid - Gate valve	v	v	v
15	HV 68103-2	Solenoid - Gate valve	v	v	v

ATTACHMENT V – FAILURE RATE TABLE

Table 1 Failure Rate Table

No	Equipment	Valve Type	Interval (Hours)	λ^S Failure Safe	λ^{DD} Failure Danger Detected	λ^{DU} Failure Danger Undetected	Failure Rates
1	HV 6818-A	Hydraulic – Gate valve	8760	3.60E-06	0	1.40 E-06	5.00 E-06
2	HV 6818-B	Hydraulic – Gate valve	8760	5.50E-07	0	1.10 E-07	6.6-E-07
3	HV 6818-D	Hydraulic – Gate valve	8760	4.10E-07	0	1.20 E-07	5.30 E-07
4	HV 6819-1	Hydraulic – Butterfly valve	8760	3.43 E-06	0	1.40 E-07	3.57 E-06
5	HV 6819-2	Hydraulic – Butterfly valve	8760	3.40 E-06	0	1.80 E-06	5.20 E-06
6	HV 6832-A	Hydraulic – Butterfly valve	8760	4.65 E-06	0	3.80 E-07	5.03 E-06
7	HV 6832-B	Hydraulic – Butterfly valve	8760	7.27 E-06	0	4.45 E-07	7.27 E-06
8	HV 6832-D	Hydraulic – Butterfly valve	8760	4.21 E-06	0	1.89 E-06	6.10 E-06
9	HV 6832-E	Hydraulic – Butterfly valve	8760	4.69 E-06	0	1.62 E-06	6.31 E-06
10	HV 6833-A	Hydraulic – Butterfly valve	8760	4.43 E-06	0	2.36 E-07	4.67 E-06
11	HV 6833-B	Hydraulic – Butterfly valve	8760	4.04 E-06	0	1.54 E-06	5.58 E-06

No	Equipment	Valve Type	Interval (Hours)	λ^{S} Failure Safe	λ^{DD} Failure Danger Detected	λ^{DU} Failure Danger Undetected	Failure Rates
12	HV 6833-C	Hydraulic – Butterfly valve	8760	3.90 E-06	0	2.05 E-06	5.95 E-06
13	HV 6833-E	Hydraulic – Butterfly valve	8760	3.39 E-06	0	1.26 E-07	3.52 E-06
14	HV 68103-1	Solenoid – Gate valve	8760	3.21 E-06	0	1.20 E-07	3.33 E-06
15	HV 68103-2	Solenoid – Gate valve	8760	4.41 E-06	0	6.52 E-06	1.09 E-05

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 1

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6818-A Hydraulic - Gate valve*, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.60E-06 + 0)/(3.60E-06 + 0 + 1.40E-06)

= 72%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6818-A = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI	=	Time Interval		
	=	1 year	=	8760 hours

Fox example the calculation of HV 6818-A Hydraulic - Gate valve, data can be found on Failure Rate Table of Final Element

PFDavg	=	[1 (λ^DU x TI)] / 2
	=	[1 (0.0000014 x 8760)] / 2
	=	0.006130
	=	6.13E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 2

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \qquad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6818-B Hydraulic - Gate valve*, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (5.50E-07 + 0)/(5.50E-07 + 0 + 1.10E-07)

= 83%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6818-B = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \qquad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6818-B Hydraulic - Gate valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.10E-06 x 8760)] / 2
= 4.82E-04

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 3

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6818-D Hydraulic* - *Gate valve*, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.10E-07 + 0)/(4.10E-07 + 0 + 1.20E-07)

= 77%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6818-D = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6818-D Hydraulic - Gate valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.20E-06 x 8760)] / 2
= 5.26E-04

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 4

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6819-1 Hydraulic - Butterfly valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.430E-06 + 0)/(3.43E-06 + 0 + 1.40E-07)

= 96%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6819-1 = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6819-1 Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.40E-06 x 8760)] / 2
= 6.13E-04

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 5

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \qquad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6819-2 Hydraulic - Butterfly valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.40E-06 + 0)/(3.40E-06 + 0 + 1.80E-07)

= 65%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6819-2 = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \qquad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6819-2 Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.80E-06 x 8760)] / 2
= 7.88E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 6

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6832-A Hydraulic - Butterfly valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.65E-06 + 0)/(4.65E-06 + 0 + 3.80E-07)

= 92%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6832-A = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval

= 1 year = 8760 hours

Fox example the calculation of HV 6832-A Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2

= [1 (3.80E-07 x 8760)] / 2

= 1.66E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 7

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6832-B Hydraulic - Butterfly valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (7.27E-06 + 0)/(7.27E-06 + 0 + 4.45E-07)

= 94%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6832-B = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6819-B Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (4.45E-07 x 8760)] / 2
= 1.95E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 8

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \qquad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6832-D Hydraulic - Butterfly valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.21E-06 + 0)/(4.21E-06 + 0 + 1.89E-06)

= 69%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6832-D = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \qquad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6832-D Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

$PFDavg = [1 (\lambda^{DU} \times TI)] / 2$

$= [1 (1.89E-06 \times 8760)] / 2$

$= 8.28E-03$

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 9

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6832-E Hydraulic - Butterfly valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.69E-06 + 0)/(4.69E-06 + 0 + 1.62E-06)

= 74%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6832-E = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6832-E Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.62E-06 x 8760)] / 2
= 7.10E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 10

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of HV 6833-A Hydraulic - Butterfly valve, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.43E-06 + 0)/(4.43E-06 + 0 + 2.36E-07)

= 95%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6833-A = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

	SIL (Safety Integrity Level)	Project	SIL
		Doc. No.	
		Rev. No.	
		Page	

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6833-A Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (2.36E-07 x 8760)] / 2
= 1.03E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 11

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of HV 6833-B Hydraulic - Butterfly valve, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.04E-06 + 0)/(4.04E-06 + 0 + 1.54E-06)

= 72%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6833-B = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval

= 1 year = 8760 hours

Fox example the calculation of HV 6833-B Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2

= [1 (1.54E-06 x 8760)] / 2

= 6.75E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 12

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S} + \lambda^{DD}}{\lambda^{SU} + \lambda^{DU} + \lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of HV 6833-C Hydraulic - Butterfly valve, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.90E-06 + 0)/(3.90E-06 + 0 + 2.05E-06)

= 66%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6833-C = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

ITS Institut Teknologi Sepuluh Nopember	SIL (Safety Integrity Level)	Project	SIL
		Doc. No.	
		Rev. No.	
		Page	

TI = Time Interval

= 1 year = 8760 hours

Fox example the calculation of HV 6833-C Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2

= [1 (2.05E-06 x 8760)] / 2

= 8.98E-03

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 13

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \qquad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of HV 6833-E Hydraulic - Butterfly valve, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.39E-06 + 0)/(3.39E-06 + 0 + 1.26E-07)

= 96%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 6833-E = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \qquad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 6833-E Hydraulic - Butterfly valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.26E-07 x 8760)] / 2
= 5.52E-04

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 14

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of HV 68103-1 Solenoid - Gate valve, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.21E-06 + 0)/(3.21E-06 + 0 + 1.20E-07)

= 96%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 68103-1 = SIL 3

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval
= 1 year = 8760 hours

Fox example the calculation of HV 68103-1 Solenoid - Gate valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (1.20E-07 x 8760)] / 2
= 5.26E-04

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) EQUIPMENT 15

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad -1.1$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of HV 68103-2 Solenoid - Gate valve, data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (4.41E-06 + 0)/(4.41E-06 + 0 + 6.52E-07)

= 40%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1/1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

HV 68103-2 = SIL 2

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad -1.2$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI	=	Time Interval		
	=	1 year	=	8760 hours

Fox example the calculation of HV 68103-2 Solenoid - Gate valve, data can be found on Failure Rate Table of Final Element

PFDavg	=	[1 (λ^DU x TI)] / 2
	=	[1 (6.52E-07 x 8760)] / 2
	=	2.86E-02

VERIFICATION SIS (SAFETY INSTRUMENTED SYSTEM) TOTAL CALCULATION

Based on ABB, he achievable SIL (Safety Integrity Level) is determined by the following safety-related parameters:

1.1 SFF

Fraction of failures that do not have the potential to put the safety-related system in a hazardous or fail-to-function state (SFF). The equation used to find SFF (Safe Failure Fraction) based on IEC 62061:

$$SFF = \frac{\lambda^{S}+\lambda^{DD}}{\lambda^{SU}+\lambda^{DU}+\lambda^{DD}} \quad \text{-1.1}$$

where:

λ^S = Failure Safe

λ^DD = Failure Danger Detected

λ^DU = Failure Danger Undetected

Fox example the calculation of *HV 6818-A Hydraulic - Gate valve,* data can be found on Failure Rate Table

SFF = (λ^S + λ^DD)/(λ^SU + λ^DD + λ^DU)

= (3.60E-06 + 0)/(3.60E-06 + 0 + 1.40E-06)

= 72%

1.2 Hardware Fault Tolerance (HFT)

The valve has a Hardware Fault Tolerance (HFT) = 1, as meet the architecture standard of the valve on ESD which has 1oo1, it means the use of single channel, a single error that occurred can directly lead to device failure. The greater HFT number is better to the system because the failure that occurs will not directly lead to failure of the asset. Table 3.4 shows the standard of IEC 61508 for devices with type A.

SFF	HFT		
Type A	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60 - 90%	SIL 2	SIL 3	SIL 4
90 - 99 %	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

1.3 Average probability of hazardous failures for a safety function on demand (PFDavg)

$$PFDavg - 1001 : \frac{1(\lambda^{DU} x\, TI)}{2} \quad \text{-1.2}$$

where:

PFDavg = Probability on Failure Demand average

λ^DU = Failure Danger Undetected

TI = Time Interval

= 1 year = 8760 hours

Fox example the calculation of HV 6818-A Hydraulic - Gate valve, data can be found on Failure Rate Table of Final Element

PFDavg = [1 (λ^DU x TI)] / 2
= [1 (0.0000014 x 8760)] / 2
= 0.006130
= 6.13E-03

The calculation of Logic Solver known from the data

PFDavg	=	Yokogawa Prosafe-RS	=	1.68E-06
PFDavg	=	PB-Yokogawa Prosafe-RS	=	1.60E-05
		Total	=	1.77E-05

Total PFDavg can be calculated by the equation below:

$$PFDavg^{SIF} = \sum PFDavg^{LS} + \sum PFDavg^{FE} \quad -1.3$$

where:

$PFDavg^{SIF}$ = PFD average of SIF
$\sum PFDavg^{LS}$ = PFD average of Logic Solver
$\sum PFDavg^{FE}$ = PFD average of Finel Element

And the total calculation of PFDavg Logic Solver and Final Element as shown below:

$PFDavg^{SIF}$ = $\sum PFDavg^{LS} + \sum PFDavg^{FE}$
= 5.40E-03 + 1.77E-05
= 5.42E-03

CHAPTER 5
CONCLUSION & RECOMENDATION

Based on analysis, the conclusion got from the analysis and verification SIL (Safety Integrity Level) are:

1. SIL of the asset meet the requirement, industry LNG should meet SIL 3 based on the IEC standard.
2. Based on failure rate found some equipment has 1/1 that means one failure lead to another failure. The equipment are HV 68103-2 and HV 6833-C.
3. Based on HAZOP some spot still has high potential of hazardous situation. Predictive maintenance will reduce the hazardous situation. By predictive maintenance the number of likelihood can be predicted and for severity can be increase because of the preventive action.

Recommendation of this final project is to continue the analysis to SIS.

This Page Intentionally Left Blank

REFERENCE

[1] SKK Migas Official Site, n.d. [Online] Available at: www.skkmigas.go.id

[2] ISA (International Society of Automation), 2004. IEC 61511-1 Functional Safety: Safety Instrumented System for the Process Industry Sector - Part 1. North Carolina: s.n.

[3] International Electrotechnical Commission, 2006. IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. s.l.:s.n.

[4] PGN Indonesia Official Site, n.d. [Online] Available at: www.pgn.co.id

[5] International Electrotechnical Commission, 2001. IEC 61882 – Hazard and Operability Studies (HAZOP)

[6] Lewin, D. R., n.d. Hazard and Operability Studies, s.l.: s.n.

[7] Irfansyah, W., 2009. Verifikasi Safety Integrity Level Menggunakan Metode Semi-Kuantitatif IEC 6151-1 Study Kasus : Tangki Timbun - Filling Shed Terminal LPG. Surabaya: s.n.

[8] Lassen, C. A., 2008. Layer of Protection Analysis (LOPA) for determination of Safety Integrity.. Norway: s.n.

[9] Reyes, G. Z., 2008. Layer of Protection Analysis Applied to Ammonia Refrigerator System. Texas: s.n.

[10] Takasana, H. A., 2009. Penentuan Safety Integrity Level (SIL) dari Safety Instrumented Function (SIF) pada Process Platform di Offshore Production Facilities. Surabaya: s.n.

This Page Intentionally Left Blank

BIOGRAPHY

The Author was born in Pekanbaru, February 4th 1994. The Author took her formal education from Cendana Primary School, Cendana Junior High School, and Cendana Senior High School at Duri, Riau. After graduated from Cendana Senior High School on 2012, The Author continue her higher education on Institut Teknologi Sepuluh Nopember, Faculty of Marine Technology, department Marine Engineering. The Author registered with student number 4212 101 033 on Double Degree Marine program with Hochschule Wismar Germany.

The author has keen of learning, not only in classes but also by doing job training, proved by job training at shipyard company, PT. PAL Indonesia (Persero) in 2014 and reliability engineering company, PT. Tiara Vibrasindo Pratama in 2015. The Author also joined on Institute of Marine Engineering, Science & Technology as a student member aThe author takes the Marine Reliability Availability Maintainability and Safety (RAMS) Laboratory for her concern to do research for this final project.

The author contact :
Phone : +6282163500066
Email : fitranikamilaa@gmail.com

This Page Intentionally Left Blank