PERANCANGAN SAFETY INSTRUMENTED SYSTEM (SIS) DI UNIT LNG LOADING BERTH MENGGUNAKAN DCS YOKOGAWA CENTUM 3000 DI PT. ARUN NGL

DESIGN *SAFETY INSTRUMENTED SYSTEM* (SIS) ON LNG LOADING BERTH UNIT USING DCS YOKOGAWA CENTUM 3000 AT PT. ARUN NGL

Ferdy Septieka[1], Erwin Susanto, Ph.D [2], Dr. Ir. Basuki Rahmat, M.T. [3]

Fakultas Teknik Elektro – Universitas Telkom
Jl. Telekomunikasi, Dayeuh Kolot Bandung 40257 Indonesia
[1]septiekaferdy@gmail.com [2]ews@telkomuniversity.com [3]bas@telkomuniversity.com

Abstrak

LNG Loading Berth merupakan salah satu unit utama di PT Arun NGL. Unit ini berfungsi sebagai unit untuk mendistribusikan LNG yang telah di proses dan disimpan dalam storage kedalam kapal pengankut LNG. Namun, unit ini terkadang terjadi kesalahan pada system, yang dapat mengakibatkan kesalahan fata jika terjadi pada skala besar dan terus menerus. Maka di setiap plant diberikan suatu *Safety Instrumented System (SIS)* atau disebut juga *ESD*. Dalam SIS dipaparkan, bahwa keadaan darurat, *Shutdown*.

Tugas Akhir ini di titik beratkan pada analisis verifikasi SIS yang telah ada di PT Arun NGL serta Perancangan *Safety Instrumented System (SIS)* pada unit 68 LNG Loading Berth menggunakan *DCS YOKOGAWA CENTUM 3000* yang terdapat di PT. ARUN NGL. Dengan berdasarkan spesifikasi serta sensor yang digunakan. System ini dapat mencegah terjadinya keadaan yang dapat mengakibatkan kerusakan pada system.

Tingkat pengujian system didasarkan pada ketepatan tindakan yang dilakukan system terhadap instruksi yang diberikan oleh user, ataupun secara otomatis oleh sensor. Pengujian juga dilakukan melalui virtual *DCS YOKOGAWA CENTUM 3000*. Diharapkan dengan penelitian SIS pada unit 68 ini dapat bekerja dengan baik serta menjadikan feedback bagi PT Arun NGL serta dapat meminimalisir kerusakan pada system.

Kata Kunci: ***SIS, SIF, SIL, Safety Life Cycle, BPCS & IEC***

Abstract

Loading Berth LNG is one of the main units in the PT Arun NGL. This unit serves as a unit for distributing LNG that has been processed and stored in a storage vessel into LNG carrier. However, this unit is sometimes an error occurs in the system, which can lead to fatal errors if it occurs in large-scale and continuous. Then at each plant is given a safety instrumented system (SIS) or also known as ESD. In the SIS presented, that a state of emergency, Shutdown.

This final project study emphasized on the analysis of the existing SIS verification in PT Arun NGL and Design of Safety instrumented system (SIS) in units of 68 LNG Loading Berth use DCS YOKOGAWA CENTUM 3000 contained in the PT. ARUN NGL. On the basis of the specification and the sensor used. This system can prevent the occurrence of circumstances that may cause damage to the system.

Level testing system based on the accuracy of the system action taken against the instructions given by the user, or automatically by the sensor. Testing is also done through virtual CENTUM DCS 3000. It is expected that with the SIS research on this 68 unit can work well and make feedback for PT Arun NGL and can minimize damage to the system.

Keywords: ***SIS, SIF, SIL, Safety Life Cycle, BPCS & IEC***

1. INTRODUCTION

PT Arun NGL as one of the international companies are always determined to respond to any existing technology advances. One way is to establish cooperation with Yokogawa Electric Hokushin Japan of Japan in the field of control technology by using the Distributed Control System for plant control system in PT Arun NGL. Distributed Control System is a computer-based control technology and electronic data communications. PT Arun NGL is currently using one of the latest Distributed Control System with the type of CENTUM CS 3000 as part of the control system of PT Arun NGL plant.

Safety instrumented system (SIS) play an important role in providing a protective layer in the process industry system to suppress the possibility of these risks become smaller. What is the SIS, emergency or safety system shutdown, or a safety interlock, the goal is to continue the process to the "safe state" when pre determinated set point has been exceeded or when a safe operating condition has been violated

Emergency Shut Down or ESD, another name of the SIS, is a system that serves to prevent or minimize a result of emergency situations, help prevent loss of life, damage to environment, and / or damage to the instrument. This system should be designed in such a way as to take into account various possible accidents that may occur either because the process trip, equipment failure, human error, or any other cause which is unknown to minimize the damage and losses incurred. ESD has a wide range of applications, from private cars to industrial plant.

The use of Distributed Control System applied to improve the productivity and efficiency of the company also increased security in the enterprise, both employee safety and security of the plant unit. One of the important unit in the PT Arun NGL plant is LNG Loading Berth (unit 68). If there are problems in the unit 68, it will have fatal consequences. In this final project, research will be carried Design Safety instrumented system (SIS) in LNG Loading Berth unit 68 PT Arun NGL plant and its application in the Distributed Control System.

2. Basic Theory

2.1 *Safety Instrumented System (SIS)*

Safety instrumented system (SIS) or also called ESD system, FNG system or many other naming play an important role in providing a protective layer in industrial process systems. Mentioned in the SIS, that a state of emergency or safety system shutdown, or a safety interlock, the goal is to continue the process to the "safe state" when pre determinated set point has been exceeded or when a safe operating condition has been violated. SIS serves to protect if there are unexpected events that cause fatal accidents, environmental pollution, and accidents in an industrial process instrumentation.

Safety instrumented system is designed and constructed to reduce the risk of accidents to a process control that can threaten the safety of human life and the environment. This system is not a system that guarantees regular control how the process can be run as desired process design engineer, but ensures safety as designed by Process Safety Engineer, the system will work when the alarm signal sent by the field devices showed a critical condition.

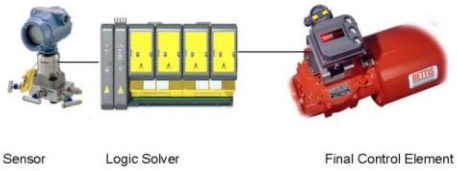


FIgure 2.1 Element at SIS

2.2 *Safety Integrity Level (SIL)*

Safety Integrity Level (SIL) is defined as the relative level of risk reduction provided by the security functions of an instrument and process tool, or to determine the level of risk reduction targets. In simple terms, SIL is a measurement of performance required for the safety instrumented system (SIF). Requirements for a given SIL is not consistent among all the functional safety standards. SIL itself is the target figure for the PFD (probability of failure on demand) of a SIF (safety instrumented function). The higher the value the higher the SIL availability of its safety function (easy: the better). There are four degrees SIL standards mentioned in the standards (SIL1, SIL 2, SIL 3, and SIL 4). Standard standard mentioned above provide a framework to carry out the determination of SIL in general.

Each mode has its own sense and has its own standards. Low Demand Mode as defined in 3.5.12 of IEC 61508-4, is where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.

Tabel 2.1 Tabel Low Demand Mode

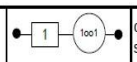
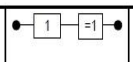
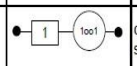
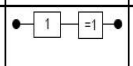
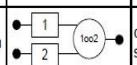
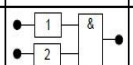
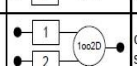
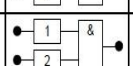
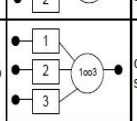
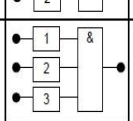
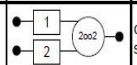
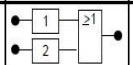
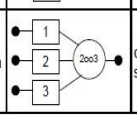
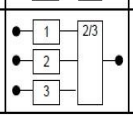
Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Safety Availability (1-PFD)	Risk Reduction Factor (1/PFD)
4	.0001 - .00001	99.99 – 99.999%	10,000 – 100,000
3	.001 - .0001	99.9 - 99.99%	1,000 - 10,000
2	.01 - .001	99 - 99.9%	100 - 1,000
1	.1 - .01	90 - 99%	10 - 100

The International Electrotechnical Commission's (IEC) standard IEC 61508, EN 61508 or IEC name for now, defines SIL grouped into two major categories of hardware safety integrity and systematic safety integrity. A device or system must meet the requirements for both categories to achieve a given SIL level is assigned after Integerity Safety Hazard Anayisis Process (AHP) has concluded that the safety instrumented system is required. A PHA performed to identify potential hazards in the plant. Analysis of PHA range from very simple screening analysis for Hazard and Operability Study (HAZOP). HAZOP itself is systematic, methodical examination of the design process that utilizes a multi-disciplinary team to identify hazards or operating problems that can lead to accidents. HAZOP provides a basic priority for implementation of risk mitigation strategies, such as emergency shutdown system (ESD).

2.3 Method to Determine SIL

To calculate the value of SIL using this method, there are several steps that must be done, first of all is to find the value PFDavg or PFD-average of a tool, to calculate PFDavg tailored to the architecture of the device. There are the types of common architecture that is often used is 1oo1, 1oo2, 1oo3, 2OO2, 2oo3, and so on. From some of the architecture of each has a different formula in determining PFDavg, can be seen from the following table:

Tabel 2.2 : PFDavg equation based architecture

safety archi-tecture	name	shortened definition (source: IEC 61508)	block diagram (source: IEC 61508)	trip input	logic relation for de-energized -to -trip configuration	PFD_{AVG} (excl. PC and β)	PFD_{AVG} (excl. PC, incl. β)
1oo1	one out of one	demand or failing element commands output to a safe state		"0"		$1/2x(\lambda_{DU}xT)$	$1/2x(\lambda_{DU}xT)$
1oo1	one out of one, inherent Fail Safe	demand or failing element commands output to a safe state		"0"		$\lambda_D xMTTR$	$\lambda_D xMTTR$
1oo2	one out of two	one demand or one failing element commands output to a safe state		"0"		$1/3x(\lambda_{DU}xT)^2$	$1/3x((1-\beta)x\lambda_{DU}xT)^2 + 1/2x\beta x\lambda_{DU}xT$
1oo2D	one out of two, with diagnostics	one demand or simultaneous failing elements command output to a safe state		"0"		$1/3x(\lambda_{DU}xT)^2$	$1/3x((1-\beta)x\lambda_{DU}xT)^2 + 1/2x\beta x\lambda_{DU}xT$
1oo3	one out of three	either demand or failing element commands a output to a safe state		"0"		$1/4(\lambda_{DU}xT)^3$	$1/4x((1-\beta)x\lambda_{DU}xT)^3 + 1/2x\beta x\lambda_{DU}xT$
2oo2	two out of two	two demands or simultaneous failing elements command output to a safe state		"0"		$\lambda_{DU}xT$	$(1-\beta)x\lambda_{DU}xT + 1/2x\beta x\lambda_{DU}xT$
2oo3	two out of three	two demands or two failing elements command output to a safe state		"0"		$(\lambda_{DU}xT)^2$	$((1-\beta)x\lambda_{DU}xT)^2 + 1/2x\beta x\lambda_{DU}xT$

After doing the calculations on the PFDavg of sebuat tool, we can calculate the value of a SIF SIL. As we know that there is a sensor-SIS logic solver-final element. After getting the value PFDavg of a tool, after summing the total PFDavg into the formula as the following equation:

Equation……. (2.1) $\square\square_{\square\square\square} = \Sigma\square\square_{\square\square\square} + \Sigma\square\square_{\square\square\square} + \Sigma\square\square_{\square\square\square}$

Where

Equation……. (2.2) $\square\square = \square^{\square\square} \square$

Meanwhile

Equation ……. (2.3) $\square\square = \frac{\square^{\square\square}\square^{\square}\square^{\square\square}}{\square\square \quad \square\square \quad \square\square \quad \square\square}$

From the results of data PFDavg-SIF above we've got the value and match these values into table SIL (table 2.0), which has been described previously.

3. Designing System

3.1 Safety Life Cycle

Safety Life Cycle (SLC) is the engineering process contains the steps required and must be met in order to achieve a high level of functional safety in the concept, planning, design, operation, and maintenance of the safety instrumented system. An automation system designed according to the requirements SLC is expected to reduce the risk of failure in the process industri.Safety Life Cycle begins with the conceptual design of a process and ended only after the SIS is de-comissioned. The key idea here is that safety must be considered from the beginning of the conceptual process design and should be maintained during all the design, operation, and maintenance activities.

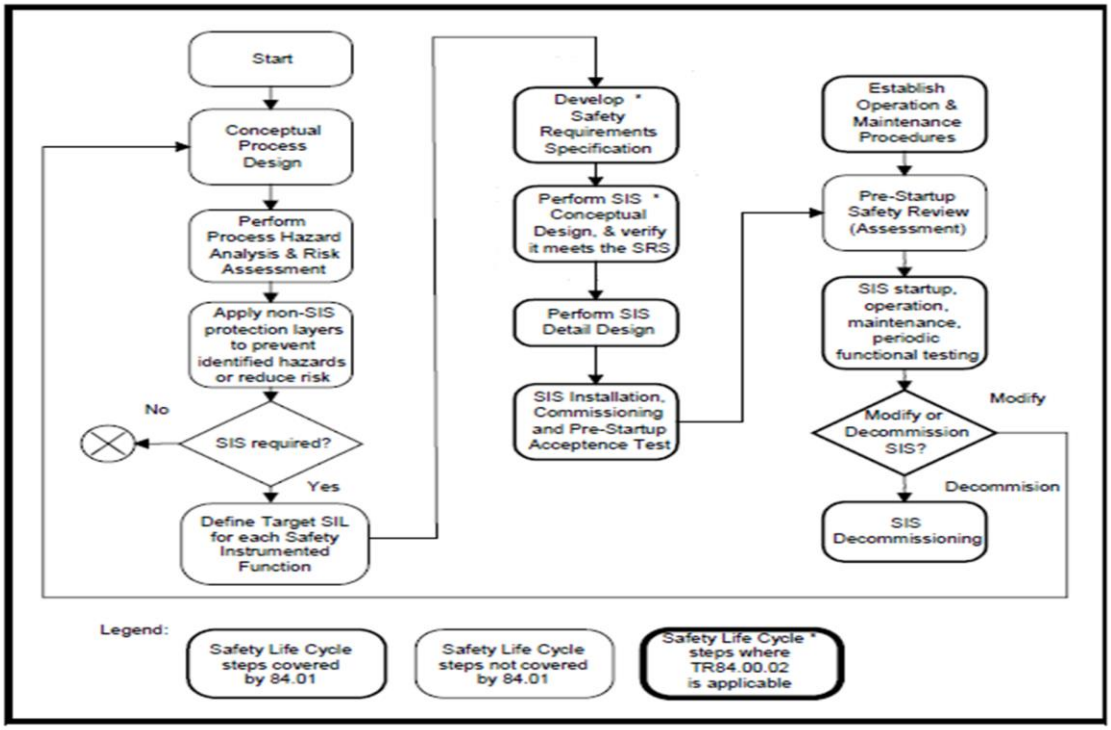


Figure 3.1 Safety Life Cycle Diagram

3.2 Verifikasi *Safety Instrumented System* Unit 68

Verification on SIS aims to find out what is the value achieved SIL and the SIL value represents the security level of the plant, as to which was discussed in the previous chapter on the value of SIL and level of security is achieved, the smaller the value of SIL, the greater the risk that would be obtained in the event of a catastrophic vice versa greater the value of SIL means the ability to reduce the level of risk, the better. The authors use the appropriate standard of IEC 61 058 is a method on the Safety of Life Cycle as a guide for verification of SIS. By analyzing the SIL of the SIS is intended to determine the value of existing systems, a number of factors into consideration is that existing systems are old systems with instrumentation everything is still using the same tool since it was first created.

Figure 3.2 System for Verification Value of SIL

4. Result and Analysis

4.1 SIS Verification – SIL, SIS Value

SIL verification is done by using the Simplified Method, without counting the human factor as the operator's participation in this system. The main elements used in the calculation using this method is that the value PFDavg obtained from the failure mode for each device. The whole system ESD PT ARUN included into the category of low demand, because of the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency for low system demand has qualification separately in accordance with IEC.

Tabel 4.1 SIL Value for Whole SIF

ESD	PFD Average	SIL	SIL IEC Recommendation
SIF-1	0,220311665	1	3
SIF-2	0,220311665	1	3
SIF-3	0,155671465	1	3
SIS		1	

4.2 Independent Protection Layer *(IPL) Analysis*

Independent Protection Layer serves to coat the plant in case of a disaster in the hope of the risk reduction that is large enough to prevent a failure that does not affect the plant, this layer independent saloing not related to one another. In connection with the opinion of the experts and IEC standards are now saying that the ESD system with human intervention can not be used as the main security system, meaning that the system should only be an additional security system that would mem back up the main SIS system when failure occurs.

But what happened in the PT Arun, because it still uses the old standard so that the security system ESD / SIS there are still using the system by a factor of human intervention as the main security system that should strongly discouraged by the IEC.

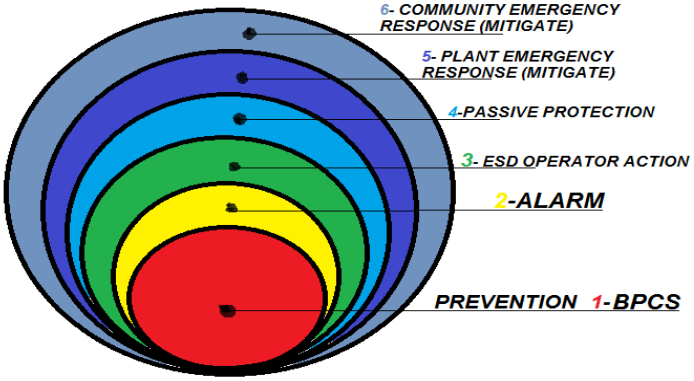
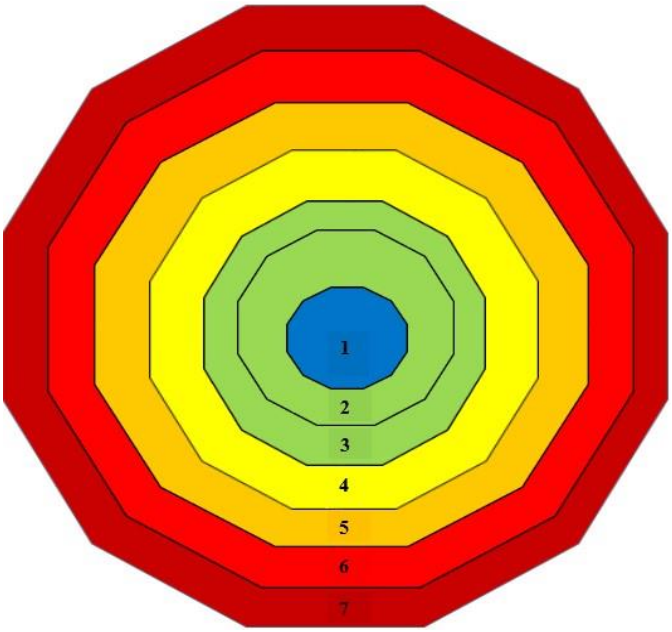


Figure 4.1 IPL Overview

In the figure 4.7 is an overview of Layer Protection owned by PT Arun, shows that in the third layer it shall be filled by the SIS / ESD automatic device but is occupied by the ESD system operator action that should go into the second layer together with the alarm. Thus meaning Layer Of Protection owned by PT ARUN less safe because of the lack of layer SIS and SIS should fill the layer with ESD -Operator Action, the average plant now uses an automated system terintegerasi as SIS.

4.3 Design Result SIS – LOPA Method

Lopa method used to determine the value of IPL is required as a protective layered on the plant in the event of failure, the method used by the results of HAZOP. Through the results of HAZOP after the group several conditions on each unit then divides into several categories for inclusion in the IPL, the result of Lopa found on some table, having formed a few tables and grouped and categorizing based on the hazard contained in the table and methods to mitigate them formed. Through methods Lopa get the results in the form of a layered IPL as in figure 4.2.



Gambar 4.2 Tabel Layer IPL from LOPA Result

No Layer	Nama Layer	Warna	Katagori
LAYER 1	*BPCS*		PREVENTION
LAYER 2	*ALARM*		PREVENTION
LAYER 3	*OPERATOR*		PREVENTION
LAYER 4	*SIS*		PREVENTION
LAYER 5	*PASSIVE*		MITIGATION
LAYER 6	*PASSIVE-OUTSIDE*		MITIGATION
LAYER 7	*EMERGE*		MITIGATION

Gambar 4.3 Description of IPL Layer from figure 4.1

4.3 SIS Conceptual Design

Based on some of the stages that have been analyzed and own the results, then the last step is the design desari of the new SIS. Previous new SIS should have a value of SIL 3 unlike previous SIL value is only worth SIL 1, it can be done by adjusting the architecture used to achieve SIL 3, in general, SIL 3 2OO3 architecture. SIS conceptual design took a whole the conclusions of the methods methods that have been implemented, at this stage the SIS must be able to withstand the strongest possible hazard situation so as not to penetrate into the category of mitigation, eaning safe state condition can still be taken over. Unit 68 SIS design to form P & ID, can be seen from Figure 4.3 below.

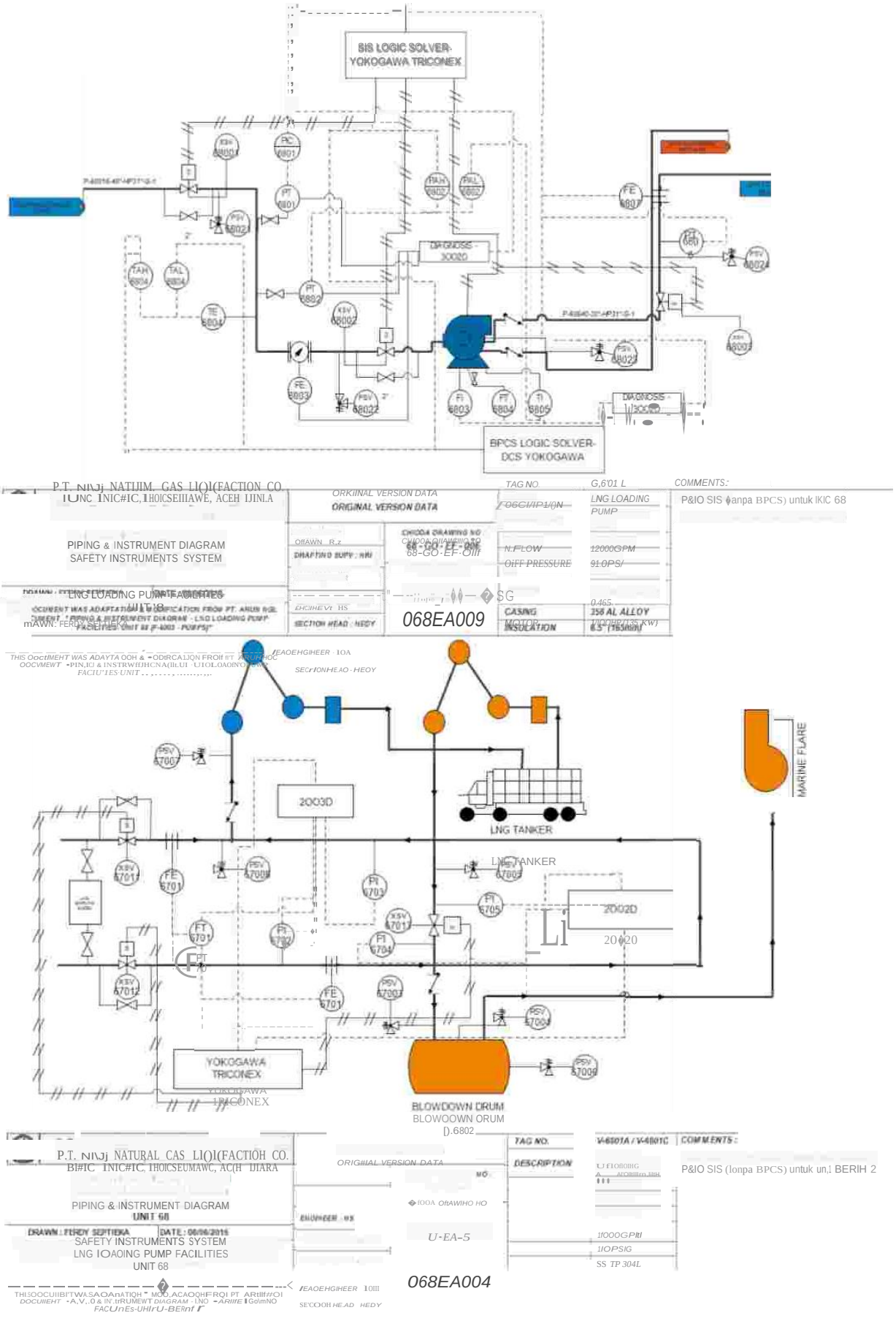


Figure 4.4 New P&ID Design

On input into the loading pump are architecture that meets SIL3 value is 2OO3D, consisting of PT-6801, PT-6802, FE-6803, the three main sensor becomes sensing elements for detecting the occurrence of extreme values, in case the value of the two extremes of the current sensor The new active will be able to activate the valve to close. For the valve itself, there are two input valve before and after the location of the sensor layout yaiut sensor are valve-68001 and XSV XSV-68002, uses two final element aims to better secure the system feared one final element failed. For the Loading Arm, is a very important part as described previously, loading arm aimed to transfer LNG into tankers, on the unit system used 2OO3D with the diagnosis, there is a sensor FE-6701 contained two and made a loop with the aim of comparison of the two sensors in the two areas can be taken into consideration accuracy, there are two other PI-6703/2 as feared in this area, the pressure will rise jumped two sensors is used as a safety. For the final element placed on two inputs and XSV XSV-60011-60 012 as security will close the track when danger occurs. Next is the design of Logic Solver for 3OO2D the SIS system storage tank section, shown in the figure 4.3

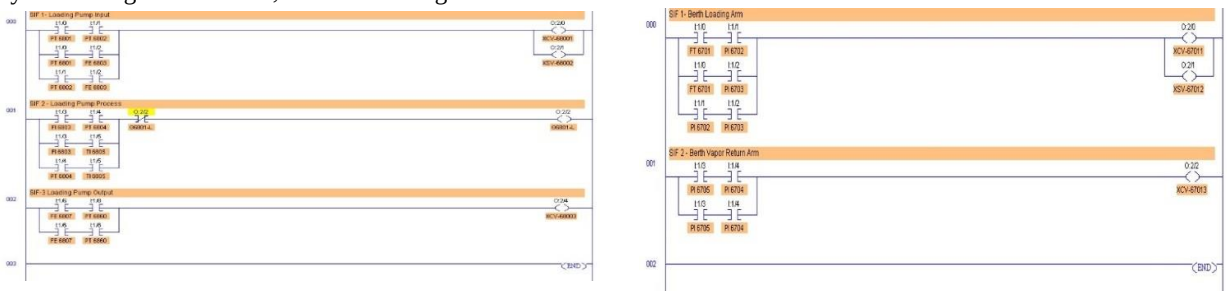


Figure 4.5 Logic Solver Configuration

In the picture above at the time of the testing of the system via the SIS logic solver is showing SIS system will be activated by closing some valves simultaneously and isolate one part of that failure does not spread to other systems. In the configuration of SIF-1 shows the system input into the LNG storage tank will be active if two sensors are activated at the same time and close the two valve input into the storage tank. SIF-2 configuration process with the same system that shows 3OO2 input via level sensors, and two pressure as comparison untuke ensure extreme conditions occur, and through testing appears also that the SIF-2 system will be active when both these sensors provide input. Through the system configuration, the SIS was formed with the architecture used for SIL3 and provide appropriate security used for LNG processing industry and it follows the latest standards specified by the IEC.

5. Final

5.1 Conclusion

Based on observations and analysis, the conclusions that can be drawn from the Analysis & Verification SIS SIS Unit Design Unit 60-68 and 60-68 are as follows.

• System SIS longer have to follow the architectural design standard IEC 1974 simple so that the problem of cost is cheaper than a new system that uses many instruments and diverse architecture, this makes it more expensive in matters of cost, SIL is to build a very high and plant safety requires a very large cost, but comparable to the security offered.

• SIL value from existing SIS PT ARUN is currently very small and not in accordance with the standards of the IEC for the LNG industry should be worth SIL3. While the new SIS was designed to have value SIL3 with a failure rate that is still the default by the vendor, the average system architecture in accordance with arssitektur to SIL3 is 2OO3D

• IPL on using the old SIS SIS with operator interference as the primary safety system that should not be recommended to the new standards, but the design of the new SIS SIS separated operator with an automated system, the more layers the more it will be able to stem the hazard occurs when conditions.

• In the long SIS Logic Solver incorporated with BPCS, and one unit logic solver mangambil over all the ESD system, for it is very dangerous in case of damage to the BPCS logic solver and then all three types of ESD will fail. In the new system there are 3 SIS Logic Solver separated apart from each SIS and BPCS, this reduces the risk of damage to the unit when it is still two units Logic Solver which takes over, more safety and risk more suppressed.

5.2 Advice

From this thesis, there are some suggestions for better future development, namely:
• At this final project researchers conduct research and analysis and design using only instrument engineer standpoint, the next use several disciplines will be more detailed and effective.
• At this final project researchers conduct research and analysis and design using only instrument engineer standpoint, the next use several disciplines will be more detailed and effective.
• In designing HAZOP should be done several disciplines in order to more complete results from all sides.
• Designing for SIS Logic Solver using PLC software more reliable advice from the author is Yokogawa Triconex software for Desai as more detailed and complete.

Bibliography :

1. PT ARUN NGL. *ARUN Manual Process Storage Loading Facilities. PT ARUN NGL*
2. PT ARUN NGL. Buku Panduan *Plant Site* PT ARUN NGL.
3. PERTAMINA, *Dasar Instrumentasi dan Proses Kontrol*. Jakarta. 2008
4. International Electrotechnical Commission (IEC), *IEC 61511-Functional safety – safety instrumented systems for the process industry sector.*
5. International Electrotechnical Commission (IEC), *IEC 61508-Functional safety of electrical/electronic/programmable electronic safety-related systems.* Geneva: Switzerland, 2000.
6. Arthur M. (Art) Dowell, III, P.E. Dennis C. Hendershot, *Simplified Risk Analysis – Layer of Protection Analysis (LOPA)*, American Institute of Chemical Engineers. 2002
7. Exida, *Failure Mode, Effect and Diagnostoc Analysis*, Exida, Cookeville : USA, 2008
8. Gordon Mckay PhD, DSc, *PROCESS SAFETY MANAGEMENT AND RISK HAZARD ANALYSIS-HAZOP*. Toronto : USA, 2008
9. KLM Technology Group, *PIPING AND INSTRUMENTATION DIAGRAMS (P&ID) (PROJECT STANDARDS AND SPECIFICATIONS*, KLM, Johor Baru: Malaysia, 2011
10. Yokogawa. *Distributed Control System: Yokogawa CS 3000 FF*. Gulf LNG and Sponge Iron Co. LLC: Electrical and Instrumentation Department.
11. Goble M William, Cheddie Harry, *Safety Instrumented System Verification: Practical Probabilistic Calculation*, ISA, 2009.
12. ANSI/ISA-84.01-1996, *Application of Safety Instrumented System for the Process Industries*, NC: Research Triangle Park, ISA, 1996.
13. Arthur M. (Art) Dowell, III, P.E. Dennis C. Hendershot, *Simplified Risk Analysis – Layer of Protection Analysis (LOPA)*, American Institute of Chemical Engineers. 2002
14. Gruhn Paul E, Cheddie Harry, *SAFETY INSTRUMENTED SYSTEMS: Design, Analysis, and Justification 2nd Edition*, ISA, 2007.