PERANCANGAN *SAFETY INSTRUMENTED SYSTEM* (SIS) PADA PIPELINE ONSHORE-OFFSHORE MENGGUNAKAN DCS YOKOGAWA CENTUM 3000 DI PT. ARUN NGL

DESIGN AND IMPLEMETATION OF SAFETY INSTRUMENTED SYSTEM (SIS) ON PIPELINE ONSHORE TO OFFSHORE WITH DCS CENTUM CS 3000 AT PT ARUN NGL

Ario Muhammad Iqbal[1], Junartho Halomoan, ST. MT [2], Edi Rakhman,Ir.,M.Eng [3]

Fakultas Teknik Elektro – Universitas Telkom
Jl. Telekomunikasi, Dayeuh Kolot Bandung 40257 Indonesia
[1]**muhammadiqbalario@gmail.com** [2]**juned_new@yahoo.com** [3]**ediman27@gmail.com**

Abstrak

Safety Instrumented System (SIS) atau disebut juga ESD system, FNG system atau banyak penamaan lainnya memainkan peran penting dalam menyediakan layer pelindung dalam sistem proses industri. Disebutkan dalam SIS, bahwa keadaan darurat ataukah sistem safety shutdown, ataukah interlock pengaman, tujuannya adalah untuk melanjutkan proses ke "safe state" ketika pre determinated set point telah terlampaui atau bila kondisi aman operasi telah dilanggar. SIS berfungsi melindungi jika ada kejadian tak terduga yang menyebabkan kecelakaan fatal, polusi lingkungan, serta kecelakaan pada suatu proses instrumentasi industry

Tugas akhir ini di titik beratkan pada analisis verivikasi SIS yang sudah ada dan perancangan system SIS pada PT ARUN NGL. Untuk penanganan safety apabila terjadinya situasi yang mengakibatkan failure pada seluruh system digunakan *SIS*, sementara untuk pengontrolan proses utama dari sebuah plant menggunakan system *BPCS* yang terdapat di pabrik pengolahan gas alam di PT. ARUN.

Tingkat pengujian sistem didasarkan pada ketepatan tindakan yang dilakukan sistem SIS dalam menengeksekusi terhadap informasi yang diberikan secara otomatis oleh sensor yang akan langsung diuji di lapangan. Pengujian system SIS dilakukan melalui virtual DCS CENTUM 3000. Diharapkan dengan penelitian pada SIS ini dapat bekerja dengan baik serta menjadikan feedback bagi PT ARUN untuk meminimalisir kerusakan pada system apabila terjadinya kondisi ekstrem

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

Abstract

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

This research emphasized on the analysis of verification SIS and SIS system design in PT ARUN NGL. For safety when handling the situation which resulted in the failure of the whole system is used SIS, while for controlling the main process of a plant using BPCS system.

The level of accuracy of the testing system is based on actions performed in the SIS system execution the information supplied automatically by sensors that will be directly tested in the field. It is expected that the research on this SIS can work well and make feedback for PT ARUN to minimize damage to the system.

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

1. PENDAHULUAN

Dalam setiap suatu proses pastilah terdapat resiko, dalam hal industry besar seperti ini resiko dari suatu sistem proses yang berjalan kontinyu sangat lah banyak mulai dari kesalahan pembacaan pada sensor sehinga menimbulkan *false trip alarm*, hingga resiko lain yaitu meledaknya suatu unit akibat *over flow* atau *over pressure*, semua hal itu sangat memungkinkan terjadi pada industry manapun, resiko pasti ada dan mutlak, tidak bisa dihilangkan hanya masalah waktu saja kapan datangnya, untuk itu tugas para engineer adalah memperkecil resiko tersebut dan mengantisipasi apabila resiko tersebut terjadi

Safety Instrumented System (SIS) memainkan peran penting dalam menyediakan layer pelindung dalam sistem proses industry untuk menekan kemungkinan resiko tersebut menjadi lebih kecil. Apakah yang disebut dalam SIS, keadaan darurat ataukah sistem safety shutdown, ataukah interlock pengaman, tujuannya adalah untuk melanjutkan proses ke *"safe state"* ketika *pre determinated set point* telah terlampaui atau bila kondisi aman operasi telah dilanggar.

Emergency Shut Down atau ESD, sebutan lain dari SIS, adalah sebuah sistem yang berfungsi untuk mencegah atau meminimalisir akibat dari situasi darurat, membantu mencegah timbulnya korban jiwa, kerusakan pada lingkunagn, dan/atau kerusakan pada instrumen. Sistem ini harus dirancang sedemikian rupa dengan memperhitungkan berbagai

kemungkinan kecelakaan yang mungkin terjadi baik karena process trip, kerusakan alat, human error, maupun penyebab lainnya yang tidak diketahui untuk meminimalisir kerusakan dan kerugian yang terjadi. ESD memiliki rentang penerapan yang luas, dari mobil pribadi hingga plant industri.

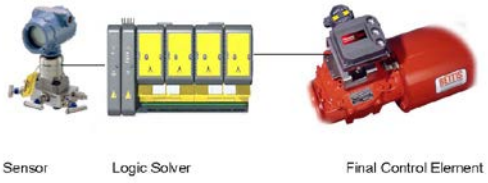
Pada pengolahan Liquid Natural Gas, atau LNG, ESD wajib dimiliki oleh setiap komponennya, termasuk pada LNG *Berth and Loading Facilities*. Di sini, ESD berfungsi untuk mencegah kecelakaan dan meangamankan sistem penanganan muatan.

1. DASAR TEORI

2.1 *Safety Instrumented System (SIS)*

Safety Instrumented System (SIS) atau disebut juga ESD system, FNG system atau banyak penamaan lainnya memainkan peran penting dalam menyediakan layer pelindung dalam sistem proses industri. Disebutkan dalam SIS, bahwa keadaan darurat ataukah sistem safety shutdown, ataukah interlock pengaman, tujuannya adalah untuk melanjutkan proses ke “safe state” ketika pre determinated set point telah terlampaui atau bila kondisi aman operasi telah dilanggar. SIS berfungsi melindungi jika ada kejadian tak terduga yang menyebabkan kecelakaan fatal, polusi lingkungan, serta kecelakaan pada suatu proses instrumentasi industri.

Safety Instrumented System dirancang dan dibangun untuk mengurangi resiko terjadinya kecelakaan pada suatu kontrol proses yang dapat mengancam kehidupan manusia dan keselamatan lingkungan hidup. System ini bukan merupakan sistem kontrol reguler yang menjamin bagaimana proses dapat berjalan sebagaimana yang diinginkan desain proses engineer, tetapi menjamin keselamatan sebagaimana didesign oleh Proses Safety Engineer, sistem akan bekerja apabila alarm signal yang dikirim oleh field devices menunjukan kondisi kritis.



Gambar 2.0 Element Pada SIS

2.2 *Safety Integrity Level (SIL)*

Safety Integrity Level (SIL) didefinisikan sebagai tingkat relatif pengurangan risiko disediakan oleh fungsi keamanan dari sebuah alat instrument dan proses, atau untuk menentukan tingkat target pengurangan risiko. Dalam istilah sederhana, SIL adalah pengukuran kinerja yang diperlukan untuk Safety Instrumented System (SIF). Persyaratan untuk SIL yang diberikan tidak konsisten di antara semua standar keselamatan fungsional. SIL sendiri adalah angka target untuk PFD (probability failure on demand) dari suatu SIF (safety instrumented function). Semakin tinggi nilai SIL semakin tinggi ketersediaan fungsi safety nya (mudahnya : semakin bagus). Ada empat derajat SIL yang disebutkan di standard standards tersebut (SIL1, SIL 2, SIL 3, dan SIL 4). Standard standard yang telah disebutkan di atas menyediakan bingkai kerja untuk melakukan penentuan SIL secara umum .

Setiap mode memiliki pengertian tersendiri dan memiliki standar tersendiri. Low Demand Mode sebagaimana didefinisikan dalam 3.5.12 dari IEC 61508-4, adalah di mana frekuensi tuntutan untuk operasi yang dilakukan pada sistem yang terkait dengan keselamatan tidak lebih besar dari satu per tahun dan tidak lebih besar dari dua kali frekuensi proof test.

Tabel 2.0 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) standar IEC 61508, atau IEC EN 61508 nama untuk sekarang, mendefinisikan SIL dikelompokkan menjadi dua kategori besar hardware safety integrity and systematic safety integrity. Sebuah perangkat atau sistem harus memenuhi persyaratan untuk kedua kategori untuk mencapai SIL diberikan Safety Integerity level ditugaskan setelah Process Hazard Anayisis (PHA) telah menyimpulkan bahwa sistem keamanan diinstrumentasi diperlukan. Sebuah PHA dilakukan untuk mengidentifikasi potensi bahaya dalam plant. Analisis PHA berkisar dari analisis skrining sangat sederhana untuk Hazard and Operability Study (HAZOP). HAZOP sendiri adalah sistematis, pemeriksaan metodis dari desain proses yang memanfaatkan sebuah tim multi-disiplin untuk mengidentifikasi

bahaya atau masalah pengoperasian yang dapat mengakibatkan kecelakaan. HAZOP menyediakan dasar diprioritaskan untuk implementasi strategi mitigasi risiko, seperti sistem shutdown darurat (ESD).

2.3 Metode Menentukan SIL

Untuk menghitung nilai SIL menggunakan metode ini, ada beberapa langkah yang harus dilakukan, pertama-tama adalah dengan mencari nilai PFDavg atau PFD-rata rata dari sebuah alat, untuk menghitung PFDavg disesuaikan dengan arsitektur dari alat tersebut. Terdapat jenis jenis arsitektur umum yang sering digunakan yaitu 1oo1, 1oo2, 1oo3, 2oo2, 2oo3, dst. Dari beberapa arsitektur tersebut masing masing memiliki rumus yang berbeda dalam menentukan PFDavg, bisa dilihat dari table berikut:

Table 2.1 : Persamaan PFDavg berdasarkan arsitektur

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

Setelah melakukan perhitungan pada PFDavg dari sebuat alat, kita bisa menghitung nilai SIL dari sebuah SIF. Sebagaimana yang kita ketahui bahwa dalam suatu SIS terdapat sensor-logic solver-final element. Setelah mendapatkan nilai PFDavg dari suatu alat, setelahnya menjumlahkan kedalam rumus PFDavg total sebagaimana perwsamaan berikut:

Persamaan……. (2.1) $$PFDavg^{SIF} = \Sigma PFDavg^{SN} + \Sigma PFDavg^{LS} + \Sigma PFDavg^{FE}$$

Dimana

Persamaan……. (2.2) $$PFD = \lambda^{DU} x\, TI$$

Sementara

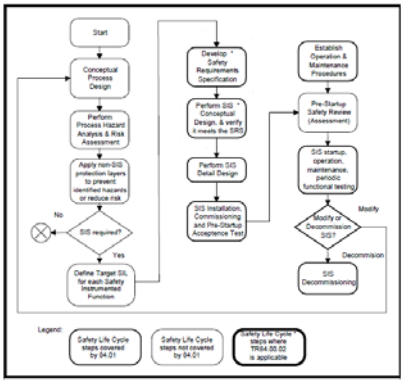
Persamaan……. (2.3) $$SFF = \frac{\lambda^{SU}+\lambda^{SD}+\lambda^{DD}}{\lambda^{SU}+\lambda^{SD}+\lambda^{DU}+\lambda^{DD}}$$

Dari hasil data PFDavg-SIF diatas kita sudah mendapatkan nilainya lalu mencocokan nilai tersebut kedalam table SIL (table 2.0) yang sudah dijelaskan sebelumnya.

2. PERANCANGAN SISTEM

3.1 Safety Life Cycle

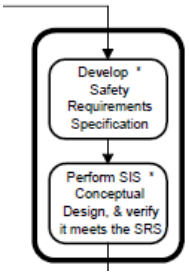
Safety Life Cycle (SLC) adalah proses engineering berisi tentang langkah-langkah yang diperlukan dan harus dipenuhi untuk mencapai tingkat keamanan yang tinggi secara fungsional dalam konsep, perancangan, desain, operasi, dan pemeliharaan Safety Instrumented System. Sebuah sistem otomatisasi yang dirancang sesuai dengan SLC persyaratan diperkirakan akan mengurangi risiko terjadinya kegagalan dalam proses industri.Safety Life Cycle dimulai dengan desain konseptual dari suatu proses dan berakhir hanya setelah SIS adalah de-comissioned. Ide kunci di sini adalah bahwa keselamatan harus dipertimbangkan sejak awal dari proses konseptual merancang dan harus dipertahankan selama semua desain, operasi, dan kegiatan pemeliharaan.



Gambar 3.1 Safety Life Cycle Diagram

3.2 Verifikasi *Safety Instrumented System* Unit 60-68

Verifikasi pada SIS ini bertujuan untuk mengetahui berapakah nilai SIL yang dicapai, dan nilai SIL tersebut merepresentasikan tingkat keamanan dari plant, sebagai mana telah dibahas pada bab sebelumnya mengenai nilai SIL dan tingkat keamanan yang dicapai, semakin kecil nilai SIL maka semakin besar resiko yang akan didapatkan apabila terjadi sebuah *catastrophic* begitu juga sebaliknya semakin besar nilai SIL berarti kemampuan untuk menekan tingkat resiko semakin baik. Penulis menggunakan standard sesuai dari IEC 61058 yaitu metode pada Safety Life Cycle sebagai panduan untuk verifikasi SIS. Dengan menganalisis SIL dari SIS ini ditujukan untuk mengetahui nilai dari sistem yang sudah ada, beberapa faktor menjadi pertimbangan adalah sistem yang sudah ada merupakan sistem lama dengan instrumentasi semuanya masih menggunakan alat yang sama sejak pertama kali dibuat.



Gambar 3.2 sistem untuk verifikasi nilai SIS

4. HASIL & ANALISIS

4.1 Verifikasi SIS-Nilai Capable SIL

Hasil kalkulasi SIL dengan data data dari *failure mode* yang menggunakan persamaan SFF berikutnya dicocokan dengan table 4.3 untuk menentukan golongan SIL dari *field instrument* tersebut. Hasilnya setelah kalkulasi dan pencocokan nilai SFF berdasarkan table diatas dirangkum pada table dibawah ini:

No	Tag Number	Valve Type	ESD I	ESD II	ESD III
1	HV 6818-A	*Hydraulic*- Gate valve	X	X	
2	HV 6818-B	*Hydraulic*- Gate valve	X	X	
3	HV 6818-D	*Hydraulic*- Gate valve	X	X	
4	HV 6819-1	*Hydraulic*-Butterfly valve	X	X	
5	HV 6819-2	*Hydraulic*-Butterfly valve	X	X	
6	HV 6832-A	*Hydraulic*-Butterfly valve	X	X	X
7	HV 6832-B	*Hydraulic*-Butterfly valve	X	X	X
8	HV 6832-C	*Hydraulic*-Butterfly valve	X	X	X
9	HV 6832-E	*Hydraulic*-Butterfly valve	X	X	X
10	HV 6833-A	*Hydraulic*-Butterfly valve	X	X	X
11	HV 6833-B	*Hydraulic*-Butterfly valve	X	X	X
12	HV 6833-C	*Hydraulic*-Butterfly valve	X	X	X
13	HV 6833-E	*Hydraulic*-Butterfly valve	X	X	X
14	HV 68103-1	Solenoid – Gate valve	X	X	X
15	HV 68103-2	Solenoid – Gate valve	X	X	X

No	Tag Number	Valve Type	Time Interval (*hours*)	λ^{S} Failures-Safe	λ^{DD} Failures-Danger Detected	λ^{DU} Failures-Danger Undetected	λ^{TOTAL} Failure rates
1	HV 6818-A	*Hydraulic*- Gate valve	8760	3.6 E-06	0	2.4 E-06	$6{,}00\times10^{-6}$
2	HV 6818-B	*Hydraulic*- Gate valve	8760	0.35 E-06	0	2.1 E-06	$2{,}45\times10^{-6}$
3	HV 6818-D	*Hydraulic*- Gate valve	8760	0.21 E-06	0	0.22 E-06	$0.433\times10^{-}$
4	HV 6819-1	*Hydraulic*-Butterfly valve	8760	5.43 E-06	0	3.14 E-06	$8{,}57\times10^{-6}$
5	HV 6819-2	*Hydraulic*-Butterfly valve	8760	1.4 E-06	0	1.8 E-06	$5{,}00\times10^{-6}$
6	HV 6832-A	*Hydraulic*-Butterfly valve	8760	1.65 E-06	0	0.8 E-06	$2{,}45\times10^{-6}$
7	HV 6832-B	*Hydraulic*-Butterfly valve	8760	7.27 E-06	0	5.45 E-06	12,72x10
8	HV 6832-C	*Hydraulic*-Butterfly valve	8760	4.21 E-06	0	3.89 E-06	$8{,}11\times10^{-6}$
9	HV 6832-E	*Hydraulic*-Butterfly valve	8760	2.69 E-06	0	2.62 E-06	$5{,}31\times10^{-6}$
10	HV 6833-A	*Hydraulic*-Butterfly valve	8760	2.43 E-06	0	4.36 E-06	$6{,}79\times10^{-6}$
11	HV 6833-B	*Hydraulic*-Butterfly valve	8760	2.04 E-06	0	4.54 E-06	$6{,}63\times10^{-6}$
12	HV 6833-C	*Hydraulic*-Butterfly valve	8760	1.9 E-06	0	2.05 E-06	$3{,}95\times10^{-6}$
13	HV 6833-E	*Hydraulic*-Butterfly valve	8760	1.39 E-06	0	2.56 E-06	$4{,}33\times10^{-6}$
14	HV 68103-1	Solenoid – Gate valve	8760	1.21 E-06	0	3.12 E-06	$5{,}95\times10^{-6}$
15	HV 68103-2	Solenoid – Gate valve	8760	2.41 E-06	0	3.52 E-06	$3{,}95\times10^{-6}$

Tag Number	SFF (Safety Failure Fraction)	Capable for SIL
HV 6818-B	14%	1
HV 6818-D	48%	1
HV 6819-1	63%	2
HV 6819-2	28%	1
HV 6832-A	67%	2
HV 6832-B	57%	1
HV 6832-C	51%	1
HV 6832-E	50%	1
HV 6833-A	35%	1
HV 6833-B	30%	1
HV 6833-C	48%	1
HV 6833-E	32%	1
HV 68103-1	20%	1
HV 68103-2	60%	2
HV 6818-A	60%	2

Gambar 4.1 (kanan-kiri) Final Element pada ESD, Nilai Failure Rate, Hasil SIL Capable

Dari hasil kalkulasi nilai *capable SIL* berarti instrument tersebut *capable* untuk digunakan dengan SIL 1 atau 2 bukan instrument terssebut memiliki nilai SIL 1 atau 2 , hanya *capable* saja. Dengan dihasilkannya table diatas menunjukan bahwa kecilnya nilai SIL dari setiap valve yang terdapat di sistem ESD PT Arun ini, dimana nilainya didominasi oleh nilai SIL 1, dangan meksimal valve memiliki SIL 2, sementara berdasarkan standar IEC untuk sebuah industry besar dengan sistem yang kontinyu seperti industry minyak atau gas layaknya PT. ARUN ini semestinya memiliki standar nilai untuk field instrument dengan type A adalah capable SIL 2 atau 3, yang berarti instrument tersebut cukup aman dan resiko akan terjadinya kegagalan sedikit. Maka dari hasil analisis berdasarkan SIL capability dari field instrument tersebut membuktikan bahwa nilai valve pada ESD di PT ARUN ini kurang baik.

4.2 Verifikasi SIS- Nilai SIL SIS

Verifikasi untuk SIL dilakukan dengan menggunakan *Simplified Method*, tanpa menghitung human factor sebagai partisipasi operator pada sistem ini. Unsur utama yang digunakan dalam kalkulasi menggunakan metode ini

adalah PFDavg yang nilainya didapat dari failure mode pada setiap device. Seluruh sistem ESD di PT ARUN termasuk kedalam katagori low demand, karena frekuensi tuntutan untuk operasi yang dilakukan pada sistem yang terkait dengan keselamatan tidak lebih besar dari satu per tahun dan tidak lebih besar dari dua kali frekuensi proof test untuk sistem low demand ini memiliki syarat kualifikasi tersendiri sesuai dengan IEC.

Tabel 4.2 Nilai SIL seluruh SIS

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	

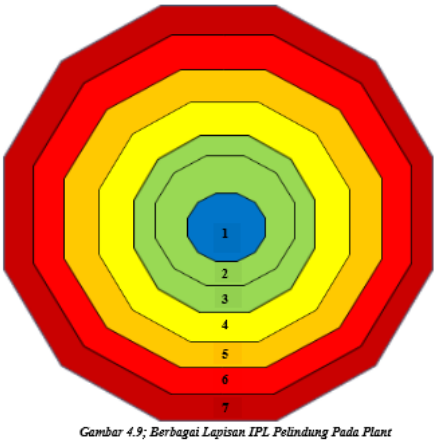
4.3 Hasil & Analisis *Hazard Analysis and Risk Assessment (HAZOP method)*

Metode HAZOP memberikan gambaran mengenai scenario dan kondisi pada saat berjalannya sebuah proses pada satu unit, dengan melakukan metode ini maka hasilnya adalah kondisi kondisi tertentu yang terjadi pada saat variable variable yang diukur dalam kondisi yang berbeda akan berdampak beberapa efek yang berbeda pada sistem. Melalui HAZOP terdapat beberapa kondisi yang plant sebelumnya menerapkan sistem yang kurang aman dan kurang berlapis bagi beberapa kondisi, dalam hal ini bisa dilihat pada kondisi saat pressure dan over flow contohnya, sistem sebelumnya hanya mengandalkan BPCS dan PSV sebagai langkah antisipatif, seharusnya terdapat sistem integerasi lapisan tambahan berbentuk SIS diantara kedua sistem tersebut untuk megamankan agar tidak langsung memasuki katagori mitigation artinya apabila memasuki katagori ini, hazardous event telah terjadi dan itu membuat terlalu riskan apabila menggunakan layer yang sangat sederhana seperti ini, dengan begitu dari kesimpulan HAZOP study ini maka harus ditambahkan lapisan IPL untuk melindungi plant dari hazardous event

4.4 Hasil Perancangan SIS – LOPA Method

Metode LOPA digunakan untuk menentukan nilai IPL yang dibutuhkan sebagai pelindung berlapis pada plant apabila terjadi kegagalan, metode ini digunakan melalui hasil dari HAZOP. Melalui hasil dari HAZOP setelah itu mengelompokkan beberapa kondisi pada setiap unit lalu membagi dalam beberapa katagori untuk dimasukkan kedalam IPL, hasil dari LOPA terdapat pada beberapa table, setelah terbentuk beberapa table dan dikelompokkan lalu pengkatagorian berdasarkan dari hazard yang terdapat pada table tersebut dan metode untuk menanggulanginya dibentuk. Melalui metode LOPA mendapatkan hasil berupa IPL yang berlapis seperti pada gambar 4.1.

Gambar 4.1 Tabel Lapisan IPL hasil LOPA



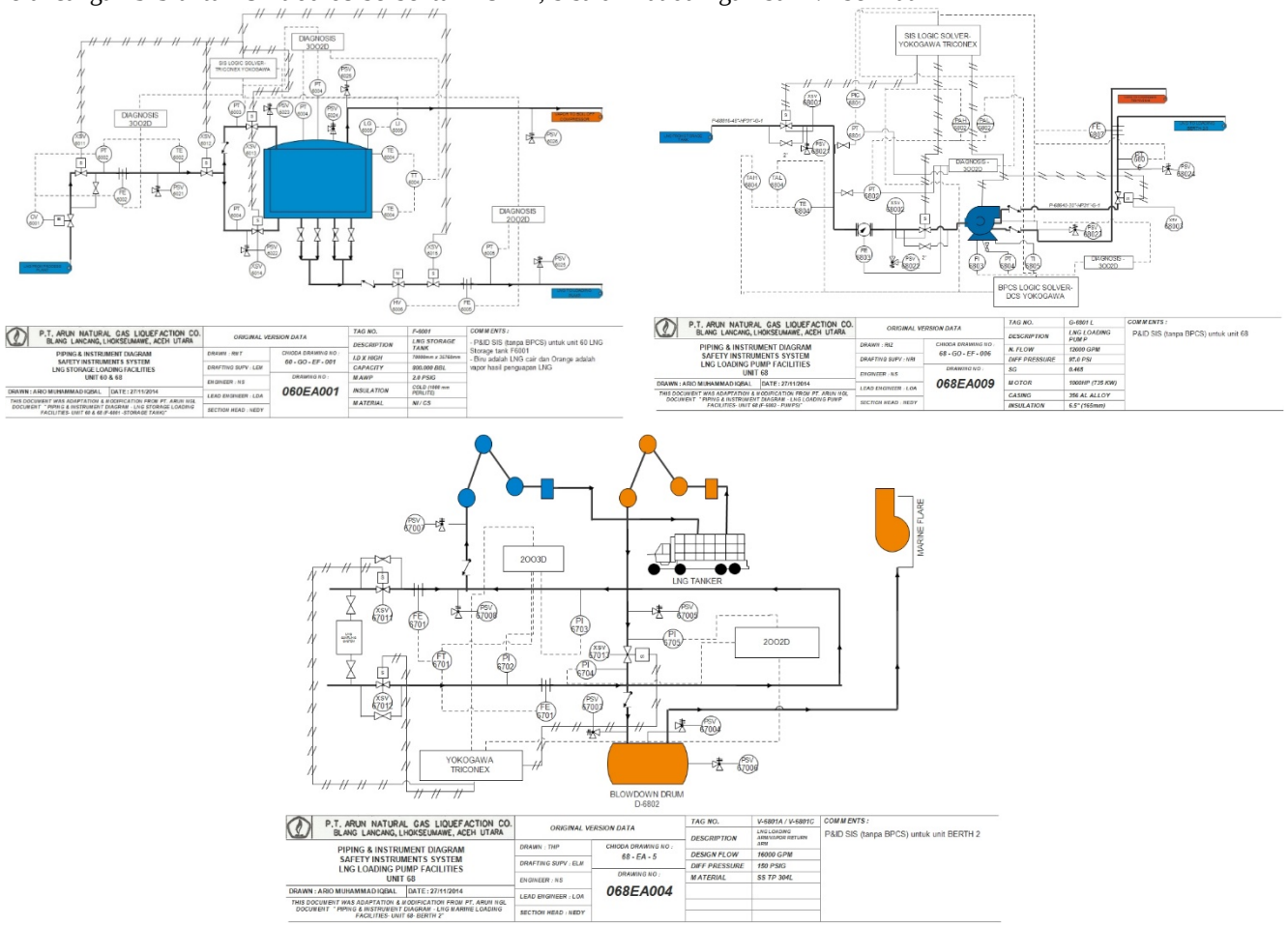
Gambar 4.9; Berbagai Lapisan IPL Pelindung Pada Plant

Tabel 4.18: Keterangan Lapisan IPL Pada Gambar xx

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

4.5 *SIS Conceptual Design*

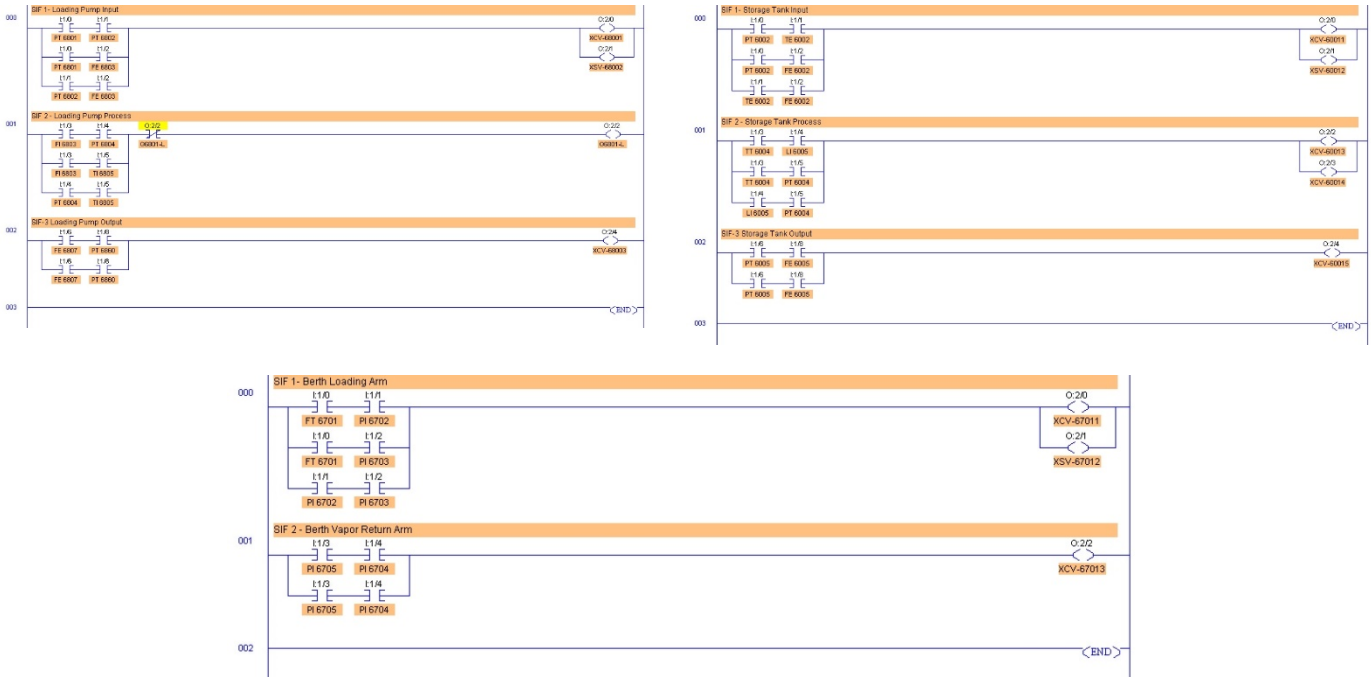
Berdasarkan beberapa tahap yang sudah dilakukan analisis dan sudah memiliki hasil, maka tahap terkahir adalah perancangan desari dari SIS yang baru. Sebelumnya SIS baru ini harus memiliki nilai SIL 3 tidak seperti nilai SIL sebelumnya yang hanya bernilai SIL 1, itu bisa dilakukan dengan menyesuaikan arsitektur yang digunakan untuk mencapai SIL 3, pada umumnya SIL 3 menggunakan arsitektur 2OO3. SIS conceptual desain mengambil seluruh hasil kesimpulan dari metode metode yang sudah dilaksanakan, pada tahap ini SIS harus bisa untuk menahan sekuat mungkin situasi hazard agar tidak tembus ke dalam katagori mitigation, artinya kondisi safe state masih bisa diambil alih. Perancangan SIS untuk Unit 60-68 berbentuk P&ID , bisa dilihat dari gambar 4.1 berikut



Gambar 4.2 Hasil Rancangan P&ID untuk SIS baru

Pada gambar hasil konsep baru dari SIS diatas menunjukan penggunaan arsitektur 2003D sebagai arsitektur yang mendukung digunakan pada SIF untuk level SIL3, artinya sistem SIS tersebut akan bekerja pada saat 2 sensor memberikan sinyal yang sama bahwa dalam kondisi ekstrem, keuntungan lainnya adalah dengan sistem seperti ini maka akan menghindari terjadinya false trip alarm yang mudah akan terjadi pada sistem 1OO1. Pada sistem sebelumnya PT ARUN menggunakan sistem 1OO1 artinya mudah terjadi false trip dan apabila terjadi kegagalan pada satu sensor maka akan memberikan kegagalan pada SIF tersebut. Pada sistem 3OO2D apabila terjadi kegagalan pada satu sensor maka masih terdapat dua sensor lainnya yang masih akan bekerja dan merubah sistem mennjadi 2OO2 dan sistem ini tetap aman hingga kedua sensor rusak tanpa ada pengecekan, namun hal ini sangat jarang terjadi pastinya sudah ada pengecekan pada saat sala satu sensor rusak terlebih dahulu.

Berikutnya adalah perancangan Logic Solver untuk sistem 3OO2D pada SIS bagian storage tank, terdapat pada gambar 4.3



Gambar 4.3 Konfigurasi Logic Solver

Pada gambar diatas pada saat pengujian dari sistem SIS melalui logic solver tersebut menunjukan sistem SIS akan aktif dengan menutup beberapa valve secara bersamaan dan mengisolasi pada satu bagian agar kegagalan tidak menjalar pada sistem lainnya. Pada konfigurasi SIF-1 menunjukan sistem input LNG ke dalam storage tank akan aktif apabila dua sensor diaktifkan sekaligus dan menutup dua valve input menuju Storage Tank. Konfigurasi proses SIF-2 dengan sistem yang sama yaitu 3OO2 menunjukan input melalui sensor level, dan dua tekanan sebagai pembanding untuke memastikan kondisi ekstrem terjadi, dan melalui pengujian tampak juga bahwa sistem SIF-2 akan aktif apabila kedua sensor tersebut memberikan input. Terakhir untuk SIF-3 bagian storage tank menunjukan konfigurasi sistem 2OO2, hal ini dikarenakan untuk penghematan dan efektifitas menggunakan sistem dengan arsitektur lainnya karena sudah menggunakan 3OO2. Pada sistem 2OO2 artinya sistem akan aktif saat kedua sensor memberikan sinyal untuk mengaktifkan valve, melalui pengujian hal itu dibuktikan bahwa pada saat kedua sensor aktif, efeknya adalah valve akan menutup dengan kedua perintah tersebut.

Melalui konfigurasi sistem tersebut maka SIS terbentuk dengan arsitektur yang digunakan untuk SIL3 dan memberikan keamanan yang sesuai digunakan untuk industry pengolahan LNG dan hal ini mengikuti standar terbaru yang telah ditentukan oleh IEC.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan pengamatan dan analisis yang dilakukan, maka kesimpulan yang dapat diambil dari *Analisis & Verifikasi SIS Unit 60-68* dan *Perancangan SIS Unit 60-68* adalah sebagai berikut.

- Nilai SIL dari SIS yang sudah ada di PT ARUN saat ini sangat kecil dan tidak sesuai dengan Standar dari IEC untuk industry kilang LNG seharusnya bernilai SIL3. Sementara SIS baru dirancang memiliki nilai SIL3 dengan failure rate yang masih default melalui vendor, arsitektur sistem rata rata sesuai dengan arssitektur untuk SIL3 yaitu 2OO3D
- Pada SIS lama Logic Solver tergabung dengan BPCS , dan satu unit logic solver mangambil alih semua sistem ESD, untuk hal ini sangat berbahaya apabila terjadi kerusakan pada logic solver maka seluruh BPCS dan ketiga jenis ESD akan gagal. Pada sistem SIS baru terdapat 3 Logic Solver yang dipisahkan setiap SIS dan terpisah dari BPCS, ini mengurangi resiko apabila rusaknya satu unit maka masih ada dua unit Logic Solver yang mengambil alih, lebih safety dan resiko lebih ditekan.
- Sistem SIS lama memiliki arsitektur desain yang mengikuti standar IEC tahun 1974 yang sederhana sehingga dalam masalah cost lebih murah dibanding sistem baru yang menggunakan banyak instrument dan arsitektur beragam, ini membuat lebih mahal dalam urusan cost, memang untuk membangun SIL tinggi dan plant yang sangat safety membutuhkan cost yang sangat besar namun sebanding dengan keamanan yang ditawarkan.
- IPL pada SIS lama menggunakan SIS dengan interferensi operator sebagai sistem keselamatan utama yang seharusnya tidak dianjurkan pada standar yang baru, namun pada perancangan SIS baru dipisahkan operator

dengan sistem SIS yang otomatis, semakin banyak layer maka akan semakin bisa membendung apabila kondisi hazard terjadi.

5.2 Saran

Dari tugas akhir ini, terdapat beberapa saran untuk pengembangan lebih baik kedepannya yaitu:

- Pada Tugas akhir ini peneliti menjalankan penelitian dan analisis serta perancangan hanya menggunakan sudut pandang instrument engineer, berikutnya menggunakan beberapa disiplin ilmu akan lebih detail dan efektif.
- Pada perancangan HAZOP seharusnya dilakukan beberapa disiplin ilmu agar hasil lebih lengkap dari semua sisi.
- Perancangan Logic Solver untuk SIS menggunakan PLC software yang lebih handal saran dari penulis adalah Yokogawa Triconex software untuk desai karena lebih detail dan lengkap
- Kalkulasi untuk perancangan lebih detail dengan besaran failure rates dari vendor yang akan digunakan agar nilai SIL yang diinginkan benar dapat tercapai.

Daftar Pustaka:

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