EVALUASI KEANDALAN KONFIGURASI PLC UNTUK SISTEM INSTRUMENTASI DAN KENDALI DI INSTALASI NUKLIR

Deswandri
Pusat Teknologi Reaktor dan Keselamatan Nuklir – BATAN
Kawasan PUSPIPTEK Gedung No. 80, Setu, Tangerang Selatan, Banten

ABSTRAK

EVALUASI KEANDALAN KONFIGURASI PLC UNTUK SISTEM INSTRUMENTASI DAN KENDALI DI INSTALASI NUKLIR. Sistem instrumentasi dan kendali (I&K) merupakan sistem yang sangat vital pada instalasi nuklir seperti PLTN. Fungsi utama sistem I&K adalah memberi informasi, memproses perintah serta melakukan pengendalian terhadap kondisi instalasi. Pada awalnya sistem I&K di instalasi nuklir menggunakan teknologi analog. Mengikuti perkembangan teknologi elektronika, penggunaan teknologi analog pada instalasi nuklir digantikan dengan teknologi digital yang sangat praktis, akurat dan mempunyai respon cepat. Penggunaan teknologi digital di instalasi nuklir diimplementasikan dalam bentuk *Programmable Logic Controller* (PLC). PLC ini tersusun dalam beberapa modul seperti Modul I/O, Modul Prosesor, Modul *Power Supply* dan modul pendukung lainnya. Karena instalasi nuklir sangat mementingkan faktor keselamatan, konfigurasi PLC harus tersusun dalam bentuk redundansi. Makalah ini bertujuan untuk mengevaluasi keandalan konfigurasi PLC untuk sistem I&K di instalasi nuklir. Ada tiga konfigurasi PLC yang dievaluasi dalam makalah ini, yaitu konfigurasi 1oo2, 1oo3 dan 2oo3. Evaluasi dilakukan dengan cara membuat model pohon kegagalan (*Fault Tree Analysis*) untuk masing-masing konfigurasi dan membandingkan hasil kuantifikasi model yang dihitung dengan perangkat lunak ITEM TOOLKIT. Hasil evaluasi menunjukkan bahwa konfigurasi 1oo3 mempunyai tingkat keandalan operasional yang tinggi tetapi berpotensi mengurangi availabilitas instalasi karena sinyal salah. Sebaliknya, konfigurasi 2oo3 mempunyai tingkat keandalan yang sedikit lebih rendah dari konfigurasi 1oo2, tetapi dapat menjaga availabilitas instalasi terhadap sinyal salah.

Kata Kunci: Sistem Instrumentasi dan Kendali, PLC, Keandalan, Model Pohon Kegagalan.

ABSTRACT

RELIABILITY EVALUATION of PLC CONFIGURATION FOR INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR INSTALLATIONS. *Instrumentation and Control (I&C) Systems are very vital in nuclear installations such as nuclear power plants. The main function of I& C systems are to provide information, to process a respond and to control over the installation conditions. At first, I&C systems in nuclear installations used the analog technology. Following the progress of electronic technology, application of the analog technology in nuclear installations has been replaced with the digital technology, which is very practical, accurate, and quick response. The application of digital technology in nuclear installations is implemented in the form of a Programmable Logic Controller (PLC). PLC is structured in several modules such as I/O module, Processor Module, Power Supply Module and other supporting modules. Since nuclear plants are very concerned with the safety, PLC configuration must be arranged in the form of redundancy. This paper aims to evaluate the reliability of the PLC configuration for I &C systems in nuclear installations. There are three PLC configurations that are evaluated in this paper, i.e. the configuration 1oo2, 1oo3 and 2oo3. The evaluation is done by making the fault tree model (Fault Tree Analysis) for each configuration and compared the results calculated by software ITEMTOOLKIT. The evaluation shows that the 1oo3 configuration has a high reliability value, but potentially reduces the installation availability due to the spurious signal. Instead, the 2oo3 configuration has a reliability values lightly lower than the 1oo2 configuration, but can keep the installation availability due to the spurious signal.*

Key Words: Instrumentation and Control System, PLC, Reliability, Fault Tree Analysis

PENDAHULUAN

Sistem instrumentasi dan kendali (I&K) merupakan sistem yang sangat vital pada instalasi nuklir seperti PLTN. Fungsi utama sistem I&K adalah memberikan informasi tentang kondisi instalasi, memproses perintah dan tanggapan dari operator terhadap kondisi instalasi, serta melakukan pengendalian (baik secara otomatis maupun manual) terhadap operasi instalasi. Tampilan dan rekaman data informasi tentang kondisi instalasi dari sistem I&K memberikan pedoman bagi operator untuk mengoperasikan instalasi secara aman dan efisien dalam setiap kondisi. Pemprosesan perintah dan

tanggapan dari operator akan menjaga instalasi untuk beroperasi secara aman dan mengembalikan kondisi operasi instalasi dari kondisi tidak aman (baik karena insiden maupun kecelakaan) ke kondisi yang aman. Sedangkan fungsi pengendalian bertujuan untuk menjaga supaya instalasi tetap beroperasi secara normal.

Pada awalnya sistem I&K dalam instalasi nuklir dibangun dengan menggunakan teknologi analog. Teknologi analog ini dapat ditemukan pada sistem I&K reaktor generasi lama. Dengan kemajuan teknologi elekronika, teknologi analog telah ditinggalkan dan digantikan dengan teknologi digital yang sangat praktis, akurat, andal dan mempunyai respons cepat. Teknologi digital telah diterapkan pada desain sistem I&K reaktor daya generasi yang lebih maju (Gen. III^{+}), seperti pada reaktor APR1400 dari Korea[1], AP1000 dari USA[2] dan EPR dari Eropa[3]. Penerapan teknologi I&K pada reaktor tersebut tidak hanya pada sistem I&K yang tidak terkait dengan keselamatan (*non-safety related system*), tetapi juga pada sistem-sistem yang terkait dengan keselamatan seperti *Reactor Protection System*(RPS) [1,2,3], *Qualified Data Processing System* (QDPS) [2] dan sistem-sistem lainnya. Pada beberapa reaktor generasi lama, sistem I&K terkait keselamatan (khususnya RPS) analog juga telah dimodifikasi dengan menggunakan teknologi digital, misalnya pada reaktor Temelin (Rep. Ceko) [4] dan Ringhals 1&2 (Swedia) [5].

Perangkat utama sistem I&K digital pada instalasi nuklir diimplementasikan dalam seperangkat *Programmable Logic Controller* (PLC). PLC adalah suatu perangkat khusus berbasis mikroprosesor yang digunakan untuk mengontrol suatu proses berdasarkan program yang ditanamkan dalam memorinya. Perangkat PLC terdiri dari Modul *Input* yang berfungsi untuk menampung masukan yang berasal dari sensor atau tranduser yang memonitor variabel proses, Modul Prosesor (CPU) yang berfungsi untuk mengolah variabel proses berdasarkan program yang ditanamkan pada modul tersebut, Modul *Output* yang merupakan perangkat antar muka antara PLC dengan peralatan pengontrol (seperti katup, motor, dan lain-lain), serta modul-modul lain untuk mendukung fungsi perangkat tersebut.

Konfigurasi modul-modul dalam sebuah PLC bervariasi tergantung pada aplikasinya. Untuk aplikasi di instalasi nuklir yang menempatkan faktor keselamatan sebagai prioritas utama, konfigurasi sebuah perangkat PLC haruslah menyediakan redundansi pada masing-masing modulnya. Konfigurasi tersebut dapat berupa konfigurasi beredundansi dua, yaitu satu perangkat PLC tersusun dari dua Modul *Power Supply*, dua Modul Prosesor, dua Modul *Input*, dua Modul *Output*dan dua *I/O bus*. Selain itu konfigurasi PLC tersebut dapat juga beredundansi tiga, dimana masing-masing modul yang menyusun satu perangkat PLC berjumlah tiga. Modus operasi PLC yang berkonfigurasi redundansi tiga dapat berupa satu kanal beroperasi dan dua kanal lainnya sebagai cadangan (*1 out of 3*), dan dapat juga berupa dua kanal beroperasi dan satu kanal sebagai cadangan (*2 out of 3*).

Beberapa metoda analisis sudah digunakan untuk mengevaluasi keandalan perangkat PLC. Portinale dan Bobbio (1999) [6] menggunakan Metoda *Bayesian Networks*sertaGaeta dkk (2001) [7] menggunakan metoda *Parametric Fault Tree* dan *High Level Petri Net* untuk menganalisis keandalan PLC berkonfigurasi 2 *out of* 3. Siwach dan Sharma (2012) [8] menganalisis PLC berkonfigurasi 1 *out of* 2 dengan menggunakan *Markov Model.*

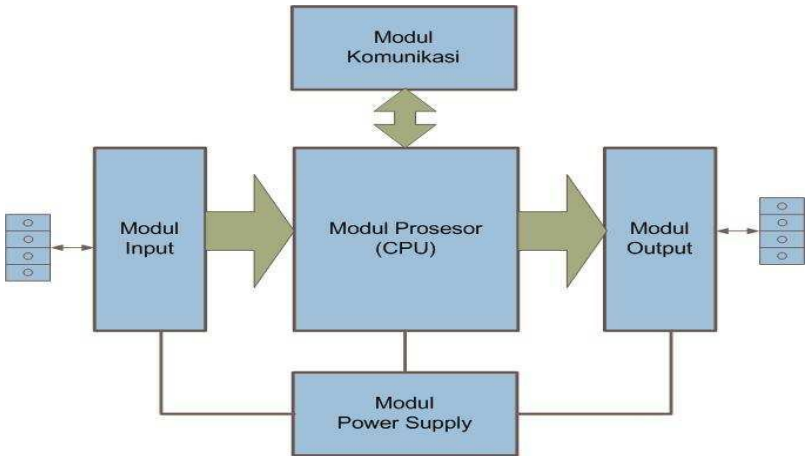
Tujuan dari makalah ini adalah untuk membandingkantingkat keandalantiga konfigurasi PLC dengan menggunakan Metoda Analisis Pohon Kegagalan (FTA). Langkah pertama adalah membuat model pohon kegagalan untuk masing-masing konfigurasi PLC. Kuantifikasi model pohon kegagalan dilakukan dengan menggunakan data-data keandalan setiap modul penyusun perangkat PLC yang diperoleh dari literatur[9,13,14]. Evaluasi dilakukan berdasarkan hasil kuantifikasi ketiga model pohon kegagalan tersebut.

PROGRAMMABLE LOGIC CONTROLLER (PLC)

PLC adalah perangkat kendali khusus berbasis mikroprosesor yang dirancang untuk diaplikasikan dalam lingkungan industri. Pada awalnya PLC didesain untuk menggantikan sistem kendali relay-relay dalam industri otomotif. Namun saat ini PLC telah berkembang menjadi sebuah peralatan kendali yang mampu mengerjakan fungsi-fungsi kompleks seperti sebuah komputer.

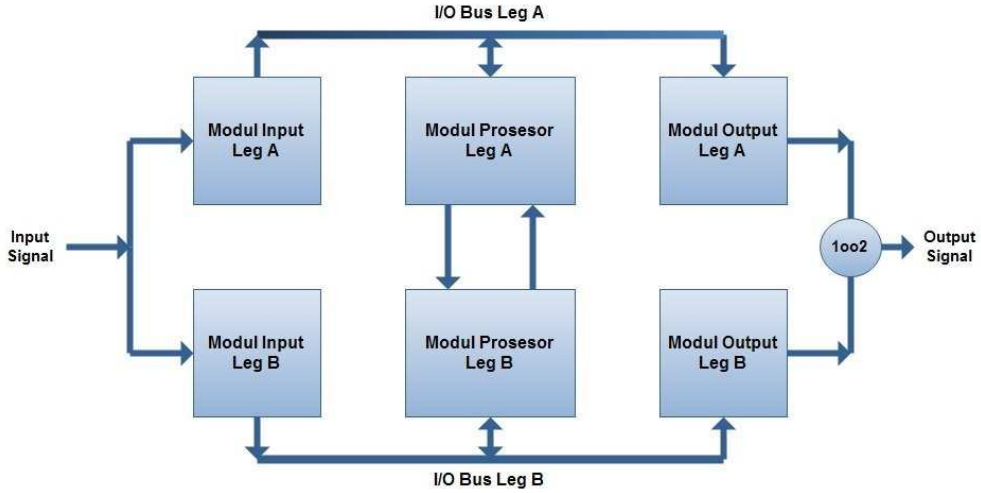
Pada dasarnya PLC terdiri dari sebuah Modul *Input*, Modul Prosesor (CPU), Modul *Output*, Modul Komunikasi, *I/O Bus* dan Modul *Power Supply*, seperti yang terlihat pada Gambar 1. Modul *Input* dan Modul *Output* terkoneksi secara langsung pada peralatan di lapangan. Modul *Input*

menampung dan memproses data dari sensor atau tranduser yang memonitor variabel proses di lapangan, untuk dapat dibaca oleh Modul Prosesor. Modul *Output* memproses dan meneruskan data dari Modul Prosesoragar dapat mengaktuasi peralatan di lapangan untuk mengendalikan proses. Modul Prosesor melakukan tiga fungsi, yaitu: membaca data lapangan melalui Modul *Input*, mengolah atau mengeksekusi perintah berdasarkan program yang ditanamkan dalam memori, dan meng*update* atau mengirim data perintah pada peralatan di lapangan melalui Modul *Output*.



Gambar 1. Diagram Blok PLC Standar

Untuk aplikasi di instalasi yang mementingkan faktor keselamatan seperti di instalasi nuklir, konfigurasi PLC haruslah menyediakan redundansi. Redundansi dapat berupa redundansi dua (*duplex system*) atau redundansi 3 (*triplex system*). PLC *duplex system* tersusun dalam bentuk dua kanal, yang masing-masing kanal terdiri dari Modul *Input*, Modul *Output*, Modul Prosesor, Modul *Power Supply*, Modul Komunikasi dan *I/O Bus*. PLC *triplex system*tersusun dalam bentuk tiga kanal, yang masing-masing kanal terdiri dari Modul *Input*, Modul *Output*, Modul Prosesor, Modul Komunikasi dan *I/O Bus*. Satu pengecualian dalam *triplex system* ini adalah bahwa Modul *Power Supply* tetap berjumlah dua.

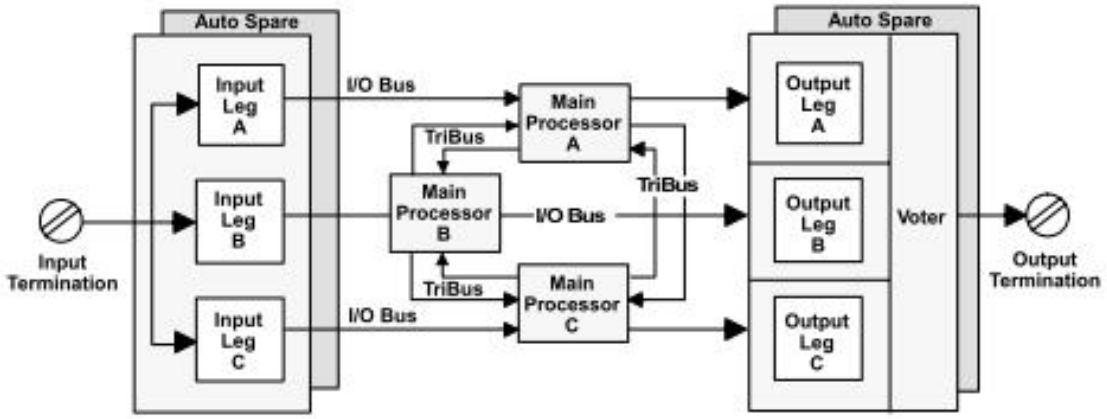


Gambar 2. Blok Diagram PLC *Duplex System*[9]

Gambar 2 memperlihatkan diagram PLC berkonfigurasi *duplex system*. Pada gambar tersebut terlihat Modul I/O terdiri dari dua modul dan masing-masing terkoneksi dengan dua Modul Prosesor melalui dua *I/O Bus*. Modus operasional PLC ini berupa *1 out of 2* (1*oo*2), yaitu keberhasilan operasional PLC ditentukan oleh minimal salah satu kanal dapat berfungsi.

Gambar 3 memperlihatkan diagram PLC *triplex system*. Gambar ini merupakan arsitektur dari *Nuclear Qualified PLC* merek Tricon dari perusahaan Invensys [10]. Seperti yang terlihat pada

gambar, PLC ini terdiri dari tiga kanal (disebut *Leg*), yang masing-masingnya terdiri dari Modul *Input*, Modul *Output*, Modul Prosesor, dan *I/O Bus*. *Power Supply* (tidak terlihat dalam gambar) terdiri dari dua modul. Modus operasional PLC ini dapat berupa *1 out of 3* (1*oo*3), yaitu keberhasilan operasional PLC ditentukan oleh minimal satu dari tiga kanal sukses berfungsi. Modus operasional lain dari PLC tipe ini adalah *2 out of 3* (2*oo*3), PLC sukses beroperasi apabila dua atau lebih kanal dapat berfungsi. Modus 2*oo*3 digunakan oleh PLC Tricon.



Gambar 3. Blok Diagram PLC *Triplex System*[10]

METODA ANALISIS POHON KEGAGALAN

Metoda Analisis Pohon Kegagalan (*Fault Tree Analysis*; FTA) awalnya dikembangkan untuk analisis keselamatan sistem pada industri ruang angkasa dan industri nuklir di Amerika Serikat pada sekitar tahun 60-an. Metoda ini kemudian berkembang dan hingga saat ini menjadi salah satu metoda yang paling sering digunakan dalam analisis keselamatan dan keandalan sistem.

Teknik penerapan metoda FTA meliputi dua fase, yaitu fase sintesis model pohon kegagalan dan fase analisis pohon kegagalan [11]. Sintesis pohon kegagalan dilakukan berdasarkan diagram fungsional dan pemahaman tentang sistem yang dianalisis. Model dimulai dengan mengasumsikan suatu kejadian bersifat umum yang menjadi topik untuk dianalisis (misalnya kegagalan suatu sistem). Kejadian ini kemudian dievaluasi untuk menentukan kejadian perantara yang menyebabkan kejadian umum tersebut. Evaluasi terus berlanjut ke kejadian berikutnya yang menjadi penyebab kejadian perantara. Evaluasi berakhir sampai pada tingkat kejadian paling mendasar, seperti kejadian kegagalan komponen atau kegagalan manusia. Interaksi antara satu kejadian dengan beberapa kejadian yang menjadi penyebab dalam pohon kegagalan, dihubungkan dalam gerbang logika OR, AND, dan lain-lain. Gerbang OR menyatakan bahwa satu kejadian dapat terjadi apabila satu atau lebih kejadian penyebab terjadi. Sebaliknya, gerbang AND menyatakan bahwa satu kejadian dapat terjadi hanya jika seluruh kejadian penyebab terjadi. Kejadian paling puncak (kejadian paling umum) dalam pohon kegagalan disebut *Top Event*, kejadian perantara disebut *Intermediate Event* dan kejadian yang paling mendasar disebut *Basic Event*.

Fase analisis pohon kegagalan dapat dilakukan secara kualitatif dan kuantitatif. Analisis kualitatif dilakukan untuk memperoleh *cutset* dengan menyelesaikan kombinasi logik model pohon kegagalan berdasarkan hukum aljabar *boolean*. *Cutset* adalah kombinasi beberapa *basic event* yang menyebabkan kejadian *top event* atau kegagalan sistem. *Minimal cutset* adalah kombinasi terkecil *basic event* yang menyebabkan kejadian *top event*. Evaluasi kualitatif melakukan perankingan *minimal cutset* untuk menentukan komponen kritis terhadap fungsi sistem atau titik lemah dalam desain sistem.

Analisis kuantitatif dilakukan untuk menghitung probabilitas kejadian *top event* berdasarkan probabilitas kejadian *basic event*. Untuk menghitung probabilitas kejadian *basic event*, kegagalan *basic event* atau komponen perlu dimodelkan terlebih dahulu. Ada beberapa model kegagalan komponen, seperti*fixed model*, *rate model*, *MTTF model*, *dormant model*, *standby model*, dan lain-lain [12].

Dalam makalah ini, komponen dimodelkan berdasarkan *rate model*. Persamaan matematis *rate model* dapat ditulis seperti pada Persamaan 1.

$$Q(t) = \frac{\lambda}{\lambda + \mu}\left[1 - e^{-(\lambda+\mu)t}\right] \quad (1)$$

dengan:
Q(t) = *unavailability* komponen
λ = laju kegagalan komponen
μ = laju perbaikan komponen
t = waktu komponen beroperasi

Probabilitas kejadian *top event* dapat dihitung dengan metoda *rare event* atau Esary-Proschan[12]. Metoda Esary-Proschan menghasilkan perhitungan yang lebih akurat dan digunakan dalam makalah ini. Persamaan matematis untuk menghitung probabilitas kejadian *top event* berdasarkan metoda Esary-Proschan diberikan dalam bentuk seperti pada Persamaan 2dan 3.

$$Q_{Sys} = \prod_{i=1}^{m} Q_i \left[1 - \prod_{j=1}^{n} \left(1 - Q_{Cutset\ j}\right)\right] \quad (2)$$

$$F_{Sys}(t) = 1 - e^{-(1-Q_{Sys}(t))} \quad (3)$$

dengan:
F_{Sys} = *unreliability*sistem
Q_{Sys} = *unavailability* sistem
Qi = *unavailability* kejadian *common* ke i
$Q_{Cutset\ j}$ = *unavailability cutset* j dengan mengeluarkan kejadian *common*
M = jumlah kejadian *common* dalam seluruh *cutset*
n = jumlah *cutset*.
t = waktu sistem beroperasi.

Untuk menghitung probabilitas kejadian *top event*, perlu didapatkan data dari masing-masing komponen/modul, berupa: laju kegagalan, waktu rata-rata perbaikan, waktu satusiklusoperasi (*mission time*) dan model kegagalan komponen/modul. Data laju kegagalan berasal dari Referensi 13& 14 dan asumsi waktu rata-rata perbaikan diambil dari Referensi9, seperti yang terlihat dalam Tabel 1. Model kegagalan masing-masing modul diasumsikan mengikuti *rate model*, yang persamaan matematisnya diberikan oleh Persamaan 1 di atas. Masing-masing model dikuantifkasi dengan waktu misi dari 1 bulan sampai dengan 12 bulan. Perhitungan dengan memvariasikan waktu misi PLC ini ditujukan untuk melihat *trend* keandalan masing-masing arsitektur PLC (arsitektur 1*oo*2, 1*oo*3 dan 2*oo*3) sebagai fungsi waktu misi. Dalam perhitungan ini juga diasumsikan bahwa perangkat lunak (*software*) dari PLC berfungsi secara sempurna.

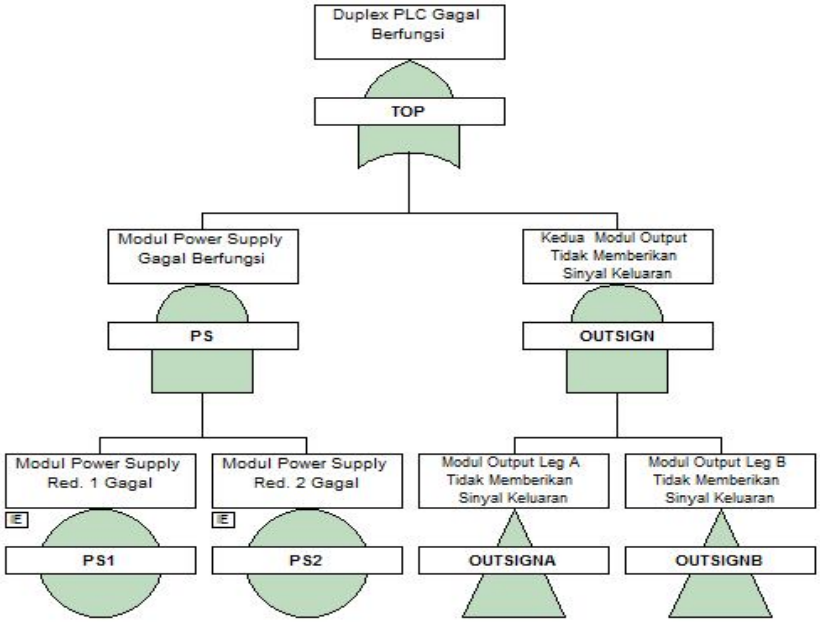
Tabel 1. Laju Kegagalan dan Waktu Rata-Rata Perbaikan Modul-Modul PLC

No.	Modul	Laju Kegagalan (/jam)	Waktu Rata-Rata Perbaikan (jam)
1.	*Processor (CPU/memory)*	1.5×10^{-04} [13]	4 [9]
2.	*Input/Output Modules*	1.1×10^{-05} [13]	4 [9]
3.	*Power Supply (Single Source)*	5.9×10^{-05} [13]	4 [9]
4.	*I/O Bus*	2.0×10^{-9} [14]	4 [9]
5.	*Internal Bus*	2.0×10^{-9} [14]	4 [9]

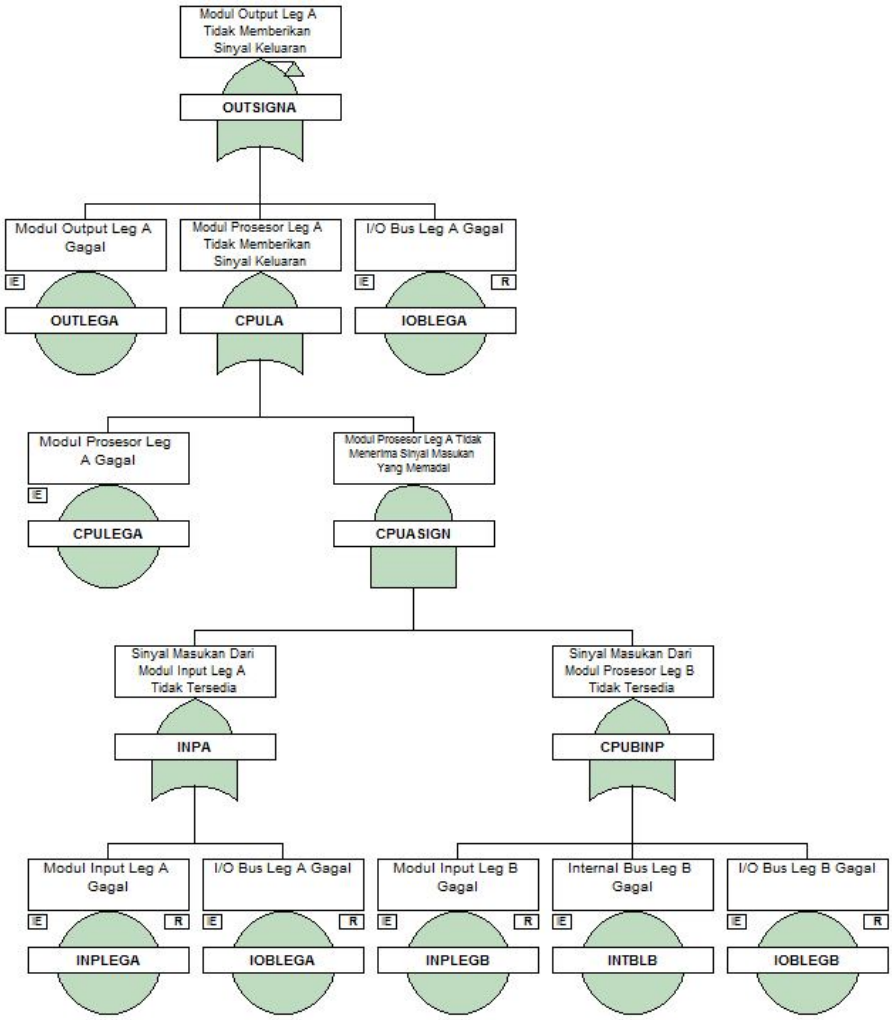
PENGEMBANGAN MODEL POHON KEGAGALAN

Pengembangan model pohon kegagalan didasarkan pada gambar diagram perangkat PLC seperti di atas. Ada tiga model pohonkegagalan yang dikembangkan dalam makalah ini. Model pertama dikembangkan berdasarkan Gambar 2, yaitu model pohon kegagalan untuk PLC berarsitektur 1*oo*2. Model kedua dan ketiga dikembangkan berdasarkan Gambar 3, yaitu model pohon kegagalan PLC berarsitektur 1*oo*3 dan 2*oo*3.

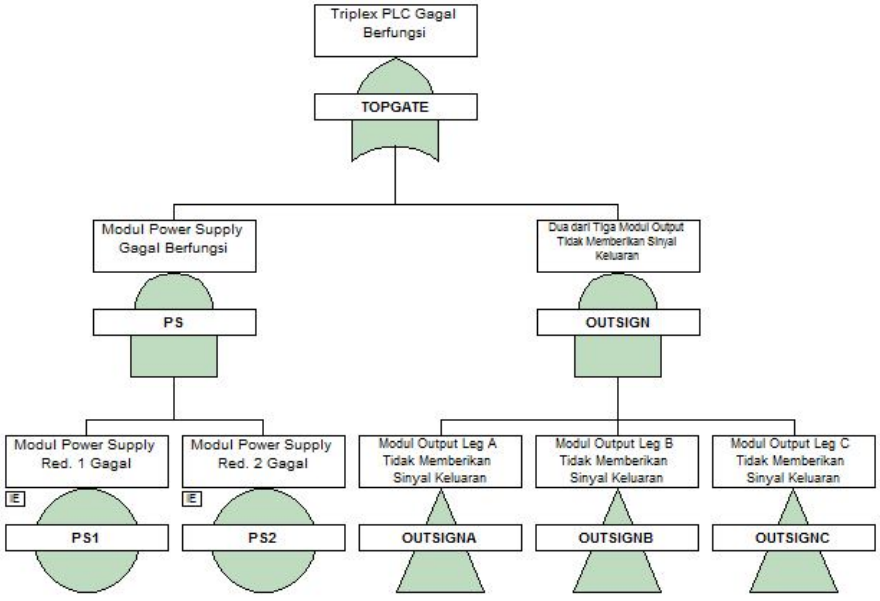
Gambar 4 menunjukkan model pohon kegagalan PLC berarsitektur 1*oo*2. *Top event* dari model ini adalah PLC gagal berfungsi. Top event ini terjadi apabila Modul *Power Supply* (*power supply* 1 dan 2) gagal berfungsi atau kedua Modul *Output* tidak memberikan sinyal. Kegagalan Modul *Output* untuk memberikan sinyal dapat disebabkan oleh kegagalan perangkat Modul *Output*, kegagalan *I/O bus*, kegagalan Modul Prosesor atau kegagalan Modul *Input* memberikan sinyal ke Modul Prosesor (Modul Prosesor tidak menerima sinyal *Input*).Kegagalan Modul *Input* memberikan sinyal *Input* disebabkan oleh kegagalan Modul *Input*, kegagalan I/O bus atau kegagalan *internal bus* dari kanal lain. Model pohon kegagalan Modul *Output* memberikan sinyal *output* untuk kanal A diberikan dalam Gambar 5. Untuk kanal B, pola model pohon kegagalannya sama dengan Gambar 5, dimana kegagalan *basic event*nya terkait dengan modul-modul di kanal B.



Gambar 4. Model Pohon Kegagalan PLC Berarsitektur 1oo2

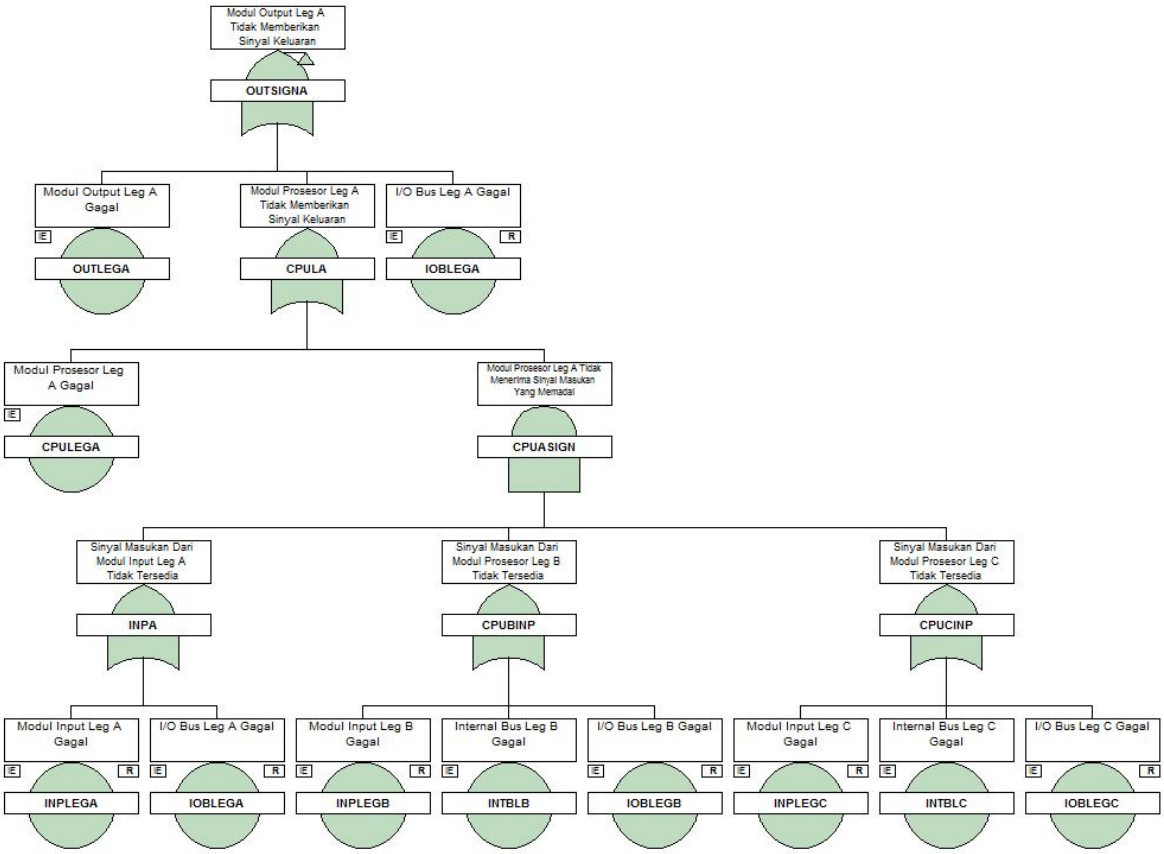


Gambar 5. Model Pohon Kegagalan "Intermediate Event" Modul Output PLC Kanal A Gagal Memberikan Sinyal Output pada PLC 1oo2.



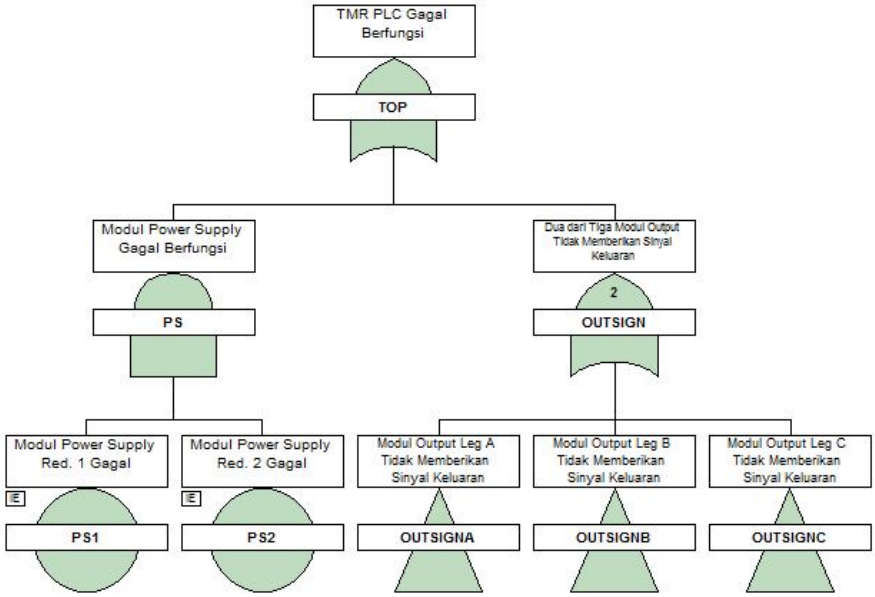
Gambar 6. Model Pohon Kegagalan PLC Berarsitektur 1oo3.

Model pohon kegagalan untuk PLC berarsitektur 1*oo*3 diberikan dalam Gambar 6. Membandingkan dengan Gambar 4, model pohon kegagalan untuk PLC berarsitektur 1*oo*3 sama dengan PLC 1*oo*2, kecuali ada tambahan satu kanal cadangan. Dengan demikian, kegagalan PLC baru terjadi apabila ketiga kanal (*Leg* A, B dan C) mengalami kegagalan secara bersamaan. Pola model pohon untuk kegagalan Modul *Output* memberikan sinyal keluaran untuk kanal A ditunjukkan seperti pada Gambar 7. Sedangkan model pohon kegagalan untuk kanal B dan C, polanya sama dengan Gambar 7, tetapi asumsi kegagalan diterapkan pada modul-modul yang terkait pada masing-masing kanal.

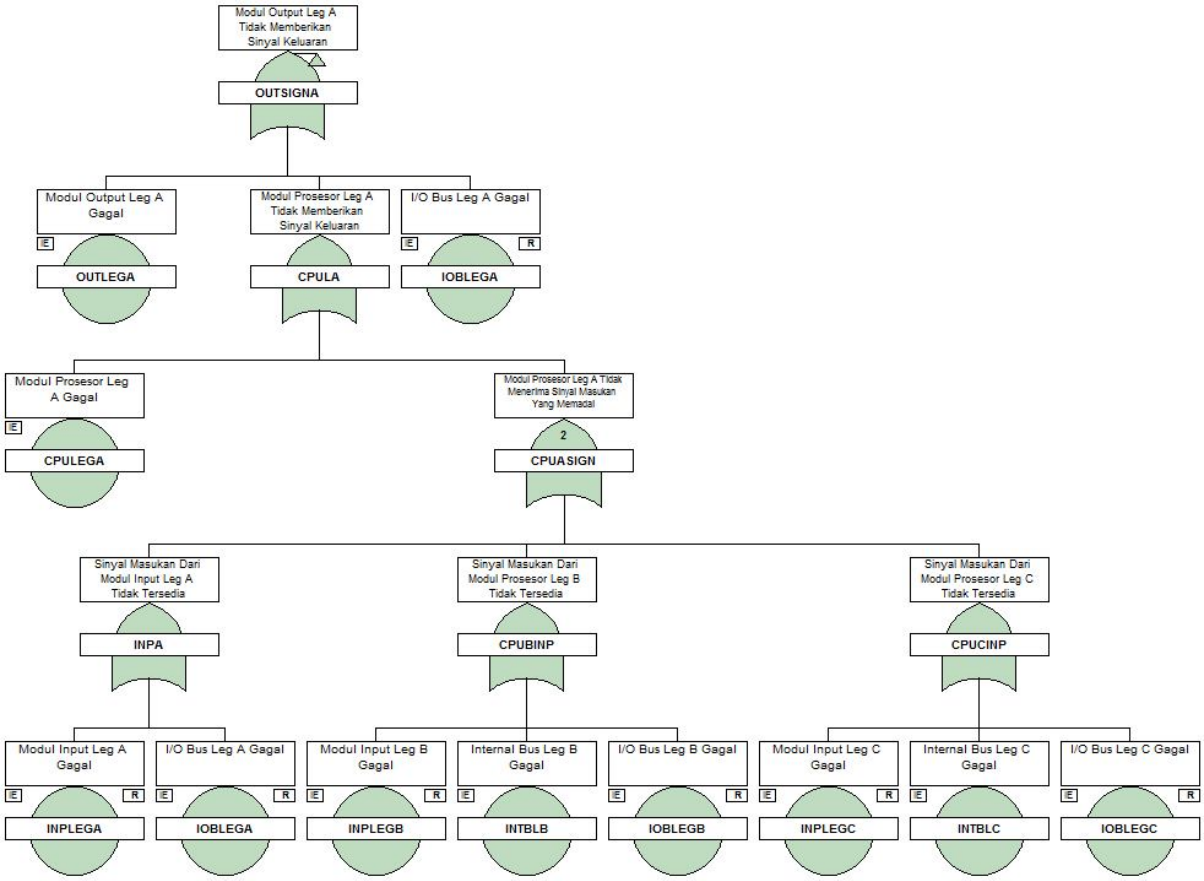


Gambar 7. Model Pohon Kegagalan "Intermediate Event" Modul Output PLC Kanal A Gagal Memberikan Sinyal Output pada PLC 1oo3.

Berbeda dengan model pohon kegagalan PLC berarsitektur 1*oo*2 dan 1*oo*3, kegagalan Modul *Output* memberikan sinyal pada PLC 2*oo*3 terhubung dengan gerbang voting logik 2*oo*3 dengan *intermediate event*nya.*Intermediate event* tersebut adalah kegagalan Modul *Outputleg* A, *leg* B serta *leg* C memberikan sinyal keluaran.Model pohon kegagalan untuk PLC berarsitektur 2*oo*3 diberikan pada Gambar 8 dan *intermediate eventleg* A diberikan pada Gambar 9. Seperti terlihat pada Gambar 9, Modul Prosesor *leg*A tidak menerima sinyal masukan dari Modul *Input* terhubung dengan gerbang voting logik 2*oo*3 dengan penyebabnya. *Intermediate event leg* B dan C mengikuti pola pohon kegagalan seperti pada Gambar 9, dimana asumsi kegagalan berasal dari modul-modul penyusun masing-masing *leg*.



Gambar 8. Model Pohon Kegagalan PLC Berarsitektur 2oo3.



Gambar 9. Model Pohon Kegagalan "Intermediate Event" Modul Output PLC Kanal A Gagal Memberikan Sinyal Output pada PLC 2oo3.

 ISSN : 0854-2910

HASIL DAN PEMBAHASAN

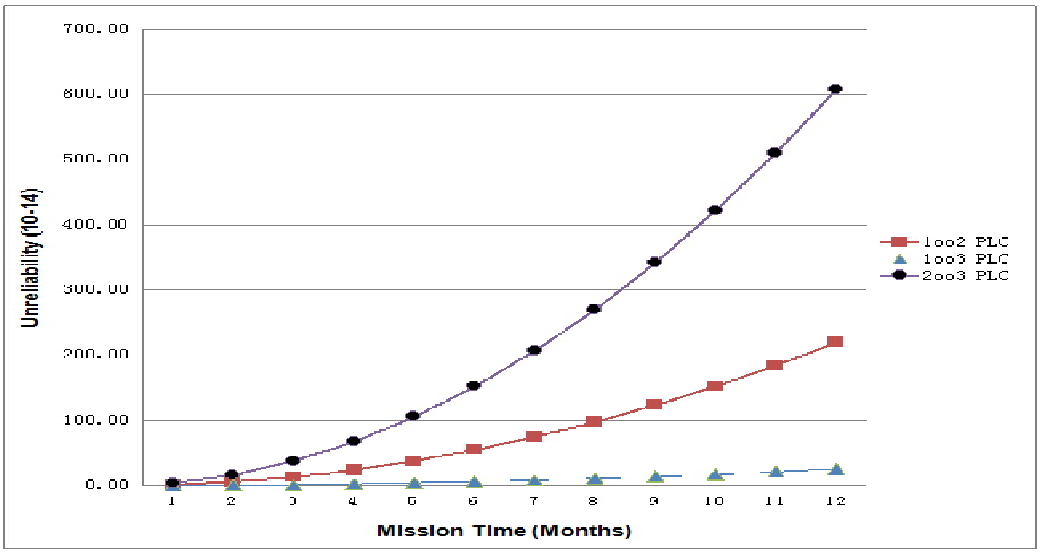
Hasil Perhitungan

Berdasarkan data dan asumsi seperti yang telah dijelaskan pada bagian Metodologi, masing-masing pohon kegagalan dikuantifikasi dengan menggunakan perangkat lunak ITEM TOOLKIT. Hasil perhitungan untuk probabilitas ketidakandalan (*unreliability*) PLC karena kegagalan modul-modulnya diberikan pada Tabel 2.

Tabel 2. Unreliability PLC Berarsitektur 1oo2, 1oo3 dan 2oo3 Terhadap Fungsi Waktu Misi

Mission Time (*Months*)	*Unreliability* (x 10^{-14})		
	PLC 1*oo*2	PLC 1*oo*3	PLC 2*oo*3
1	1,54	0,18	4,27
2	6,12	0,72	16,90
3	13,76	1,62	38,03
4	24,47	2,89	67,60
5	38,21	4,51	105,60
6	55,03	6,50	152,10
7	74,90	8,83	207,00
8	97,80	11,54	270,00
9	123,80	14,59	342,00
10	152,80	18,01	422,30
11	184,80	21,79	510,80
12	219,90	25,93	607,90

Kecendrungan (*trend*) *unreliability* PLC sebagai fungsi waktu dibutuhkan operasi PLC ditunjukkan oleh grafik seperti pada Gambar 10.



Gambar 10. Grafik Trend Unreliability PLC Sebagai Fungsi Waktu Misi

Pembahasan

Dalam mengevaluasi konfigurasi PLC di atas serta dampaknya terhadap keberhasilan fungsi sistem I&K tempat PLC tersebut terpasang,perlu dipertimbangkan dua tipe kegagalan berikut[15]. Tipe pertama adalah sistem I&K gagal berfungsi ketika tindakan kontrol/aktuasi diperlukankarena kegagalan perangkat PLC membangkitkan sinyal kontrol/aktuasi. Tipe kedua adalah sistem I&K berfungsi meskipun tindakan kontrol/aktuasi tidak diperlukan karena perangkat PLC membangkitkan sinyal kontrol/aktuasi yang salah (*spurious signal*).

Seperti yang terlihat pada Tabel 2, untuk setiap waktu misi, PLC berarsitektur 1*oo*3 mempunyai nilai *unreliability* terendah dan PLC berarsitektur 2*oo*3 mempunyai nilai *unreliability* tertinggi. Hal ini menunjukkan bahwa, sebagaimana nilai *reliability* merupakan kebalikan dari *unreliability*, probabilitas PLC 1*oo*3 berhasil melaksanakan fungsinya disepanjang waktu misi lebih besar dari PLC 1oo2 atau PLC 2*oo*3, dan probabilitas PLC 1*oo*2 lebih besar dari PLC 2*oo*3.

Perbedaannilaikeandalanmasing-masingkonfigurasi PLC di atasdapat dijelaskansebagaiberikut.PLC 1oo3 adalah PLCberedundansi 3, dimana satu kanal beroperasi dan dua kanal lain berfungsi sebagai *backup*.Kegagalan satu kanal dapat digantikan oleh kanal lainnya, dengan demikian kegagalan fungsi PLC 1*oo*3 baru terjadi apabila ketiga kanal gagal secara serempak. Lain halnya dengan PLC berarsitektur 2*oo*3. Meskipun PLC ini terdiri dari tiga kanal, akan tetapi probabilitas keberhasilan fungsi disepanjang waktu misi lebih kecil dari PLC 1*oo*2. Pada PLC 1*oo*2, satu kanal beroperasi dan satu kanal mem*backup*. PLC 1*oo*2 mengalami kegagalan ketika kedua kanal mengalami kegagalan secara serempak. Untuk PLC 2*oo*3, dua kanal beroperasi dan satu kanal mem*backup* kegagalan salah satu kanal yang sedang beroperasi. Kegagalan dua kanal secara serempak menyebabkan kegagalan fungsi PLC 2*oo*3, karena salah satu kanal yang gagal tidak mempunyai *backup*. Kombinasi seperti inilah yang menyebabkan probabilitas keberhasilan fungsi PLC 2*oo*3 lebih rendah dari PLC 1*oo*2.

Seperti yang terlihat pada Gambar 10, *unreliability* masing-masing PLC mempunyai kecendrungan meningkat dengan meningkatnya waktu satusiklusoperasi (waktu misi). Perbedaan nilai *unreliability* di antara ketiganya juga semakin membesar dengan meningkatnya waktu misi, dimana pada waktu misi 1 bulan perbedaan nilai*unreliability* tidak terlalu besar tetapi pada waktu misi 12 bulan perbedaannya menjadi cukupbesar.

Perludicatatbahwakeberhasilanfungsi PLC seperti yang dijelaskan di atasadalahkeberhasilanfungsi PLC untukmembangkitkansinyalkontrol/aktuasi.Jika kita menginginkan sebuah sistem yang harus selalu berfungsi disepanjang waktu misinya (terlepassinyalaktuasi yang dibangkitkansalahataubenar), PLC 1*oo*3 merupakan pilihan sangat menguntungkan. PLC 2*oo*3 merupakan pilihan yang mubazir, karena biaya yang dikeluarkan (untuk menyediakan 3 kanal) lebih besar akan tetapi peluang keberhasilan fungsi lebih rendah dari PLC 1*oo*2.

Akan tetapi, jika PLC diaplikasikan untuk sistem keselamatan pada instalasi yang mementingkan *availability* tinggi (misalnya instalasi pembangkit listrik seperti PLTN), maka pertimbangannya menjadi lain. Dalam instalasi ini, disamping kegagalan tipe pertama, kegagalan tipe kedua juga harus diperhatikan. Hal ini adalah karena sistem yang berfungsi pada saat tidak diperlukan (*spurious function*) akan menurunkan *availability* instalasi. Sebagai contoh kasus, PLC konfigurasi1*oo*3 diaplikasikan untuk pen-*shutdown*-an reaktor (sistem proteksi reaktor). PLC ini akanmempunyai probabilitas keberhasilan yang tinggidalammen*shutdown* reaktor karena ketika salah satu kanal membangkitkan sinyal *trip*, maka reaktor segera*trip*. Dalam aplikasi riil, sinyal yang terdeteksi atau terbangkitkan pada salah satu kanal tidak selalu merupakan sinyal yang benar-benarmerupakanperintah/persyaratanuntuk*trip*. Akibatnya reaktor lebih berpeluang untuk sering *trip* karena sinyal yang salah (*spurious trip*). Hal ini tidak menguntungkan secara ekonomis, karena PLTN membutuhkan waktu yang cukup lama untuk dapat *start-up* kembali setelah *shutdown*.

Untuk PLC 2*oo*3, ketika salah satu kanal membangkitkan sinyal *trip*, reaktor tidak langsung*shutdown*. *Trip* baru terjadi apabila minimal dua kanal membangkit sinyal *trip*. Probabilitas terjadinya sinyal yang salah secara bersamaan pada dua kanal relatif kecil. Dengan demikian, peluang *spurious trip* yang terjadi pada sistem proteksi yang ber*platform* PLC 2*oo*3relatif kecil, karena masing-masing kanal saling mengkonfirmasi akan validitas sinyal yang dibangkitkan.

Dengan demikian, dalam instalasi yang mementingkan*availability* operasi danjuga keselamatan, penggunaan sistem yang berplatform PLC 2*oo*3 lebih menguntungkan, karena dari segi keandalan (keberhasilan fungsi) sistemdi sepanjang waktu misi cukup tinggi (seperti ditunjukkan dalam Tabel 2) dan mampu mengurangi probabilitas tindakan trip yang tidak perlu karena *spurious signal*terhadap instalasi (meningkatkan*availability* instalasi).

KESIMPULAN

Perhitungan keandalan konfigurasi PLC dengan menggunakan Metoda Pohon Kegagalan memperlihatkan bahwa PLC berkonfigurasi 1*oo*3 mempunyai nilai keandalan yang lebih tinggi dari konfigurasi 1*oo*2 dan 2*oo*3,serta konfigurasi 1*oo*2 lebih tinggi dari konfigurasi 2*oo*3. Perhitungan juga menunjukkan bahwa perbedaan nilai keandalan masing-masing konfigurasi semakin membesar apabila waktu misi (panjang waktu dalam satu siklus operasi) diperbesar.

Meskipun PLCberkonfigurasi 2*oo*3 mempunyai nilai keandalanlebih rendah (2,76 kali lebih rendah dari PLC 1*oo*2 dan 23,44 kali lebih rendah dari PLC 1*oo*3), PLC 2*oo*3 ini cocok digunakan pada system keselamatan untuk instalasi yang menghendaki tingkat *availability* tinggi, karena konfigurasi ini mampu mengurangi probabilitas tindakan aktuasi yang salah dan masih mempunyai tingkat keandalan yang cukup tinggi.

DAFTAR PUSTAKA

1. Korean Hydro & Nuclear Power Company, "Standard Safety Analysis Report for Advanced Power Reactor (APR) 1400", 2002.
2. AP1000 Design Control Document Ch. 7, Revision 14, Westinghouse Electric Company LLC, 2004.
3. Anonim, The UK EPR Digital I&C System, Nuclear Engineering International Magazine 15 April 2013. http://www.neimagazine.com/features/featurethe-uk-eprtm-digital-ic-system/. Di*upload* Tanggal 14 Mei 2013.
4. NUREG / CR7007, Diversity Strategies fot Nuclear Power Plant Instrumentation and Control Systems, U.S. NRC, 2010.
5. Authen, S., et. al., Guidelines for reliability analysis of digital systems in PSA context; Phase 1 Status Report, NKS-230 Report, NKS, Denmark, 2010.
6. Portinale, L. dan Bobbio, A., Bayesian Networks for Dependability Analysis: an Application to Digital Control Reliability, Proceedings of the Fifteenth Conference on Uncertainty in Artificial Intelligence, Hal. 551-558, Morgan Kaufmann Publishers Inc.San Francisco, 1999.
7. Gaeta, R., et. al., Dependability Assessment of an Industrial Programmable Logic Controller via Parametric Fault-Tree and High Level Petri Net,Proceedings of the 9th International Workshop on Petri Nets and Performance Models (PNPM'01), Hal. 29, IEEE Computer Society Washington, 2001.
8. Siwach, A. dan Sharma, K.K., Analysis of PLC System Based On Markov Model, International Journal of Advanced Research in Electrical, Electronics andInstrumentation Engineering, Vol. 1, Issue 1, Hal. 35, 2012.
9. Palomar, J. and Wyman, R., The Programmable Logic Controller and Its Application in Nuclear Reactor System, NUREG-CR 6090, US NRC, 1993.
10. Anonim, Technical Product Guide Tricon System, Invensys System 2006.
11. Madden, M.G., and Nolan, P.J., Monitoring and Diagnosis of Multiple Incipient Faults Using Fault Tree Induction, IEE Proceedings-Control Theory and Applications 146: hal. 204–212, 1999.
12. Anonim, ITEM TOOLKIT User Manual; Fault Tree Module, Item Software Inc., 2005.
13. Chu, T.L., et. al., Traditional Probabilistic Risk Assessment Methods for Digital Systems, NUREG/CR-6962, US NRC, 2008.
14. Bologna, S., et. al., Comparison of Methodologies for Safety and Dependability Assessment of an Industrial PLC, in: European Safety Dependability Conference (ESREL2001), September 2001.
15. Muhlheim, D. M., et. al., Evaluation of I&C Architecture Alternatives Required for the Jupiter Icy Moons Orbiter (JIMO) Reactor. Tersedia di www.ornl.gov/~webworks/cppr/y2001/pres/125272.pdf. Didownloadtanggal 9 Mei 2013.

 ISSN : 0854-2910

DISKUSI / TANYA JAWAB :

PERTANYAAN : (Johnhy Situmorang, PTRKN – BATAN)

- Bagaimana model 1 out of 3, 1 out of 2, 2 out of 3 sesungguhnya dapat menjadi pilihan, karena dari perhitungan akan memeberikan hasil perhitungan.

JAWABAN ; (Deswandri, PTRKN-BATAN)

- Analisis terhadap model ini dilakukan pada tahap perancangan sistem. Hasil perhitungan dan analisis digunakan untuk menetapkan pilihan konfigurasi mana yang akan dipakai tergantung pada tujuan atau fungsi sistem.

PERTANYAAN : (Syaiful Bakhri, PTRKN-BATAN)

- Mohon penjelasan detail bagian mana yang redudanprosesor, input atau outputnya ? perbedaannya apa terhadap kehandalan ?

JAWABAN ; (Deswandri, PTRKN-BATAN)

- Konfigurasi redudansi diterapkan pada Modular PLC dengan demikian redudansi tersebut berlaku untuk semua modul-modulnya. Sebagai contoh, konfigurasi 1 out of 2 terdiri dari 2 model input, 2 model CPU, 2 model output dan lain-lain. Perbedaan terhadap keandalan adalah semakin besar jumlah redudansi (yang digunakan sebagai backup system) semakin tinggi keandalannya