EVALUASI KEANDALAN SISTEM INSTRUMENTASI DIGITAL PADA SISTEM KESELAMATAN PLTN

Sudarno
Pusat Teknologi Reaktor dan Keselamatan Nuklir (PTRKN) - BATAN
Kawasan PUSPIPTEK Gd. No. 80 Serpong, Tangerang Selatan 15310
e-mail: sudarno@batan.go.id

ABSTRAK

EVALUASI KEANDALAN SISTEM INSTRUMENTASI DIGITAL PADA SISTEM KESELAMATAN PLTN. Penerapan sistem instrumentasi dan kontrol digital dilakukan pada desain PLTN secara bertahap terutama untuk sistem yang berkaitan dengan keselamatan, dengan alasan karena mengutamakan keselamatan, sehingga teknologi yang digunakan harus sudah terbukti (proven) dengan keandalan yang memenuhi persyaratan. Hal lain yang membedakan teknologi digital dengan analog adalah penggunaan perangkat lunak (software) pada teknologi digital, yang tidak dijumpai pada teknologi analog. Dalam makalah ini dibahas evaluasi sistem instrumentasi digital untuk sistem keselamatan PLTN. Tujuan penelitian adalah untuk mengetahui pengaruh fitur-fitur teknologi digital terhadap keandalan sistem. Evaluasi dilakukan dengan melakukan analisis model pohon kegagalan pada sistem instrumentasi analog dan digital yang mempunyai fungsi yang sama. Hasil evaluasi menunjukkan bahwa penerapan fitur penanganan kegagalan software dan multi-tasking pada sistem instrumentasi digital dapat ditingkatkan keandalannya melalui keandalan watchdog timer dan penambahan redundansi sistem.

Kata Kunci: Sistem Instrumentasi Digital, Sistem Keselamatan, PLTN, Keandalan Sistem, Redundansi

ABSTRACT

RELIABILITY EVALUATION OF DIGITAL INSTRUMENTATION SYSTEM OF NPP SAFETY SYSTEM. *Application of digital instrumentation and control system on the design of nuclear power plant was done gradually, especially for systems related to safety. For safety reason, the technology used for safety system must be proven technology with a reliability that meets the requirements. Another thing that distinguishes between and digital technology is the use of software in digital technology, which is not found in analog technology. In this paper, reliability evaluation of digital instrumentation system for nuclear power plant (NPP) safety systems is discussed. The research objective was to investigate the effect of the features of digital technology on the system reliability. The evaluation is done by fault tree analysis of the analog and digital instrumentation system that perform the same function. Evaluation results showed that the realiability of on the digital instrumentation systems, related to the application of software fault-tolerant and multi-tasking features, could be improved by using reliable watchdog timer and system redundancy configuration.*

Keywords: *Digital Instrumentation System, Safety System, NPP, System Reliability, Redundancy*

1. PENDAHULUAN

Perkembangan teknologi mikro elektronika dan teknologi digital telah merambah ke berbagai kebutuhan manusia, dari yang sederhana hingga yang sangat kompleks. Teknologi prosesor digital yang awalnya ditujukan untuk unit pemroses pada komputer (PC atau *mainframe*), kemudian berkembang ke aplikasi yang lain, seperti alat-alat rumah tangga, telekomunikasi, automotif, dan sebagainya.

Aplikasi teknologi prosesor digital juga digunakan dalam industri. Prosesor digital tidak hanya digunakan dalam komputer untuk administrasi, komputasi dan pemrosesan data saja, tapi juga

untuk pengendalian proses (*digital control*). Dengan *digital control* akan mempermudah *monitoring* data proses, perubahan nilai setting dan pemilihan teknik kontrol yang sesuai.

Produk dari fabrikan juga mengikuti perkembangan teknologi. Perangkat instrumentasi lama yang mengalami kerusakan dan perlu diganti, biasanya sudah sulit mencari pengganti perangkat baru dengan spesifikasi yang sama. Oleh karena itu perangkat instrumentasi analog yang digunakan di industri banyak yang diretrofit dengan teknologi instrumentasi yang *up to date.*

Penerapan sistem instrumentasi dan kontrol digital juga dilakukan pada desain PLTN secara bertahap terutama untuk sistem yang berkaitan dengan keselamatan. Alasannya adalah karena mengutamakan keselamatan, sehingga teknologi yang digunakan harus sudah terbukti (*proven*) dengan keandalan yang memenuhi persyaratan. Hal lain yang membedakan teknologi digital dengan analog adalah penggunaan perangkat lunak (*software*) pada teknologi digital, yang tidak dijumpai pada teknologi analog. Dalam makalah ini akan dibahas evaluasi sistem instrumentasi digital untuk sistem keselamatan PLTN. Tujuan penelitian adalah untuk mengetahui pengaruh fitur-fitur teknologi digital seperti *multi-tasking* dan *penanganan kegagalan software*, terhadap keandalan sistem.

1.1. Kriteria Sistem Keselamatan

Desain sistem instrumentasi digital sebagai bagian dari sistem keselamatan, harus mempertimbangkan kriteria untuk sistem keselamatan. Sesuai dengan standard IEEE 603-2009 tentang "*Criteria for Safety Systems for Nuclear Power Generating Stations*", sistem keselamatan harus mempunyai presisi dan keandalan tertentu untuk menjaga parameter-parameter operasi reaktor dalam batas yang dapat diterima untuk setiap *Design Basis Events* (DBE). Kriteria yang harus dipenuhi oleh sistem keselamatan adalah [1]:

1. Kegagalan tuggal.
   Kegagalan tuggal dapat terjadi sebelum atau selama DBE, dimana sistem keselamatan disyaratkan untuk berfungsi. Kriteria kegagalan tunggal berlaku untuk sistem keselamatan baik secara otomatis atau manual. Penerapan kriteria kegagalan tunggal dapat mengacu pada standard IEEE 379-2000.
2. Kelengkapan tindakan protektif
   Sistem keselamatan harus didesain sedemikian, sehingga begitu diaktifkan baik secara otomatis ataupun manual, maka sekuensi tindakan protektif akan berlangsung hingga selesai semuanya. Setelah itu, untuk mengembalikan lagi sistem keselamatan ke keadaan *normal* perlu tindakan operator secara khusus.
3. Kualitas
   Komponen dan modul harus memenuhi kualitas yang konsisten dengan persyaratan perawatan minimum dan laju kegagalan yang rendah. Peralatan sistem keselamatan harus didesain, difabrikasi, diinspeksi, dipasang, diuji, dioperasikan dan dirawat sesuai dengan program jaminan kualitas yang dibuat untuk komponen atau modul tersebut.

4. Kualifikasi peralatan

   Peralatan sistem keselamatan harus dikualifikasi dengan tipe uji, pengalaman pengoperasian yang telah dilakukan, analisis atau kombinasi dari ketiga hal tersebut, agar memenuhi kinerja seperti yang dipersyaratkan dalam basis desain.

5. Integritas sistem

   Sistem keselamatan harus didesain untuk memenuhi fungsi keselamatan dalam seluruh jangkauan dari kondisi yang disebutkan dalam basis desain.

6. Independensi
   - Bagian yang redundan dari sistem keselamatan harus independen (terpisah secara fisik) satu dengan lainnya sedemikian sehingga fungsi keselamatan terpenuhi selama dan setelah DBE.
   - Peralatan sistem keselamatan yang dibutuhkan untuk memitigasi konsekuensi DBA (*Design Basis Accidents*) tertentu harus independen terhadap efek dari DBE.
   - Desain sistem keselamatan harus independen terhadap sistem keselamatan yang lain, sehingga kegagalan atau akibat dari sistem keselamatan lainnya tersebut tidak mengganggu pemenuhan fungsi keselamatan.

7. Kemampuan untuk pengetesan dan kalibrasi

   Kemampuan untuk pengetesan dan kalibrasi dari peralatan sistem keselamatan harus tersedia, tanpa mengganggu kemampuan sistem untuk menjalankan fungsi keselamatan. Pengetesan dan kalibrasi dapat dilakukan pada saat operasi daya reaktor.

8. Tampilan Informasi
   - Instrumentasi tampilan untuk tindakan yang hanya dikendalikan secara manual, dan untuk menjalankan fungsi keselamatan, harus menjadi bagian sistem keselamatan, dan harus memenuhi standar IEEE 497-2002.
   - Instrumentasi tampilan harus memberikan informasi penting keadaan sistem keselamatan secara akurat, lengkap dan pada waktu yang tepat.
   - Apabila bagian dari sistem keselamatan untuk tindakan protektif dilakukan *bypass*, maka informasi tersebut harus ditampilkan di ruang kendali secara kontinyu.
   - Tampilan informasi harus berada di tempat yang dapat diakses oleh operator. Informasi yang diperlukan oleh operator untuk melakukan tindakan secara manual harus dapat dilihat dari lokasi operator malakukan tindakan manual tersebut.

9. Kendali akses

   Desain sistem keselamatan harus memungkinkan kendali akses administratif ke peralatan sistem keselamatan.

10. Perbaikan

    Sistem keselamatan harus didesain untuk memudahkan pendeteksian, penggantian dan perbaikan peralatan yang malfungsi.

 ISSN: 0854 - 2910

11. Identifikasi

    Untuk memberikan jaminan bahwa persyaratan yang ada dalam standar dipenuhi dalam tahap desain, konstruksi, operasi dan perawatan PLTN, maka identifikasi harus mudah dilakukan untuk peralatan sistem keselamatan, komponen, modul, *hardware* dan *software* komputer serta dokumen-dokumen yang berkaitan.

12. Fitur tambahan

    Fitur tambahan adalah fitur-fitur yang tidak menjalankan langsung tindakan protektif seperti sistem *trip*, tetapi mendukung agar fungsi keselamatan dapat dijalankan dengan baik. Contoh dari fitur tambahan ini misalnya sistem HVAC, generator, transformator dll. Desain fitur pendukung tambahan ini harus memenuhi persyaratan dalam standar.

13. *Multi-unit stations*

    Struktur, sistem, komponen yang digunakan bersama (*sharing*) antara unit-unit pada PLTN multi-unit diperbolehkan selama tidak mengganggu fungsi keselamatan di semua unit. Pedoman untuk penggunaan bersama sistem daya listrik seperti tercantum pada standard IEEE 308-2001.

14. Pertimbangan *human factor*

    Faktor manusia harus dipertimbangkan selama proses desain untuk menjamin operator dan pekerja perawatan dapat menjalankan tugasnya dengan baik.

15. Keandalan

    Analisis keandalan dari desain sistem keselamatan perlu dilakukan untuk dapat mengkonfirmasi bahwa jaminan pemenuhan fungsi keselamatan terpenuhi. Analisis keandalan dapat menggunakan metoda kuntitatif dan kualitatif.

16. Kriteria sebab bersama (*common cause*)

    Evaluasi *common cause* perlu dilakukan untuk komponen dan sistem, baik *hardware* maupun *software*. *Common cause* sangat diperlukan dalam perhitungan keandalan sistem.

1.2. Aplikasi Sistem Instrumentasi Digital Pada Sistem Keselamatan

Sejak tahun 1980an banyak operator PLTN menggunakan teknologi digital untuk mengatasi masalah penuaan pada peralatan instrumentasi dan kontrol analog. Kemudian teknologi digital diterapkan pada reaktor-reaktor generasi berikutnya memerlukan fungsi yang lebih kompleks untuk kontrol, sistem proteksi dan sistem pendukung operator[2].

Teknologi modern yang berbasiskan *hardware* digital dan *software* yang canggih berkembang secara cepat dan digunakan secara luas. Seiring dengan kemajuan teknologi dalam sistem Instrumentasi dan Kendali (I&K) seperti teknologi komputer, sistem kendali, transfer data, pemrosesan data dan teknologi *software*, teknologi digital diharapkan dapat meningkatkan kinerja dan keselamatan PLTN.

Banyak PLTN di Perancis seri 900MWe dan 1300MWe mengadopsi sistem I&K digital. Di Korea, reaktor Ulchin unit 5 & 6 sudah menggunakan sistem I&K digital, demikian juga Korean Next Generation Reactor (KNGR) didesain dengan sistem I&K digital untuk sistem keselamatan, yaitu sistem proteksi reaktor (RPS) digital dan *Digital Engineered safety Feature Actuation System* (DESFAS). Di Jepang, RPS digital digunakan pertama kali di PLTN *Kashiwazaki Kariwa* Unit 6 yang mulai beroperasi secara komersial di tahun 1997[2].

Perubahan perangkat dalam pemanfatan teknologi digital untuk sistem I&K, disamping penggunaan komputer (modul prosesor) yang menggantikan rangkaian analog, juga transfer data yang tadinya kabel tembaga, diganti fiber optik yang lebih baik terhadap gangguan sinyal elektromagnetik dan kecepatan transfer dan kapasitas *bandwidth* yang lebih tinggi. Sistem monitoring parameter proses dapat tersaji dalam satu layar *display* sehingga memudahkan dalam pembacaan informasi yang ditampilkan.

Penggunaan *software* untuk menggantikan rangkaian elektronik tentu membuat sederhana rangkaian keseluruhan, dan mempermudah dalam melakukan perawatan. Dari sisi kualitas dan keandalan, penggunaan software dalam teknologi digital tidak hanya mempunyai kelebihan, tetapi juga mempunyai kekurangan[3].

Kelebihan penggunaan software dalam teknologi digital :

- Jumlah *hardware/device* dalam rangkaian berkurang.
- Jumlah tipe *device* lebih sedikit
- Lebih mudah dalam mendukung beragam model/versi.
- Lebih sederhana untuk memodifikasi atau rekonfigurasi.

Kekurangannya :

- Sulit untuk memeriksa *software* akan adanya kesalahan.
- Sulit mengharuskan penggunaan pendekatan standar untuk desain *software*
- Sulit mengontrol perubahan dalam *software*
- Kegagalan *software* tidak dapat diprediksi.

2. METODOLOGI

Evaluasi dilakukan dengan dua metode:

1. Membandingkan struktur/konfigurasi sistem instrumentasi digital dan analog untuk mengetahui bagian sistem yang kritis untuk keselamatan.
2. Melakukan pemodelan *fault tree*, untuk perhitungan analisis keandalan sistem. Dari hasil analisis pohon kegagalan dapat diketahui faktor-faktor yang berkontribusi secara signifikan terhadap kegagalan sistem.

3. HASIL DAN PEMBAHASAN

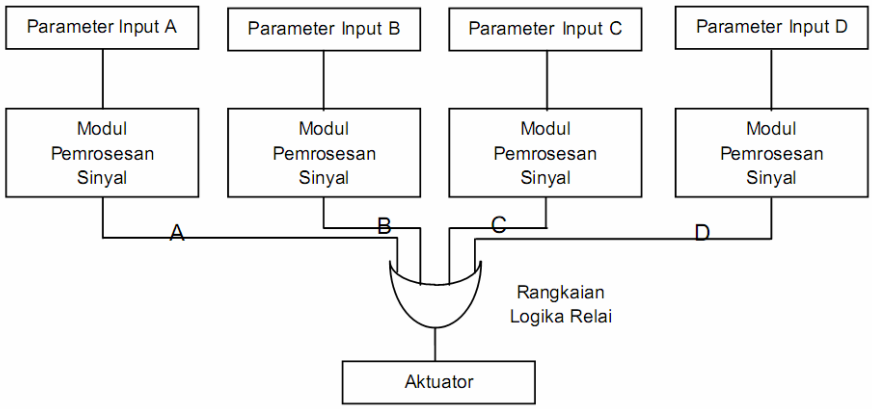
Dalam penelitian ini dibahas dua permasalahan yang muncul dalam penggunaan perangkat instrumentasi digital *programmable*, yaitu pemrosesan *multi-tasking* dan penanganan kejadian kegagalan prosesor.

3.1. Kegagalan modul digital

Satu prosesor digital dapat mengolah banyak data masukan secara simultan. Hal ini akan membuat desain rangkaian elektronika lebih sederhana, karena sebagian rangkaian elektronika yang cukup kompleks, fungsinya dapat digantikan oleh *software*. Tetapi dari segi keandalan, hal ini justru kurang bagus, karena penyatuan komponen-komponen menjadi satu modul dapat menurunkan keandalan sistem.

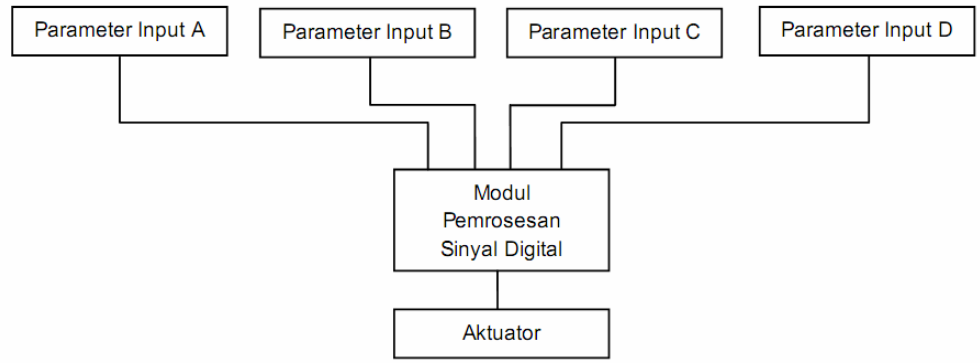
Pada kasus terjadinya kecelakaan pecahnya pipa uap (*Main Steam Line Break* / MSLB) pada *steam generator*, sistem proteksi reaktor akan melakukan trip reaktor dengan adanya masukan sinyal "Tekanan *steam generator* rendah (A)", diikuti sinyal "Tekanan *Pressurizer* rendah (B)", "*Level steam generator* rendah (C)" dan "Daya reaktor berlebih (*over power*) (D)".

Sinyal trip "Tekanan *steam generator* rendah (A)" melakukan inisiasi trip reactor dan *Main Steam Isolation Signal* (MSIS) yang merupakan bagian dari *Engineered Safety Features* (ESF) pada saat tekanan sisi sekunder *steam generator* turun di bawah nilai batas. Jika terjadi kegagalan pada modul pemrosesan sinyal untuk membangkitkan sinyal *trip* untuk input A tersebut, maka modul pemrosesan sinyal B akan mengeluarkan sinyal perintah *trip*. Jika ini gagal, modul pemrosesan sinyal C akan mengeluarkan sinyal *trip*, dan berikutnya jika masih terjadi kegagalan, maka modul sinyal D mengeluarkan sinyal *trip*. Redundansi dan diversifikasi parameter input akan meningkatkan keandalan sistem proteksi reaktor untuk melakukan trip pada saat diminta. Skema rangkaian pemrosesan sinyal trip menggunakan perangkat analog dan digital dapat dilihat pada Gambar 1a dan 1b.



Gambar 1a. Skema rangkaian pemrosesan sinyal trip menggunakan perangkat analog.

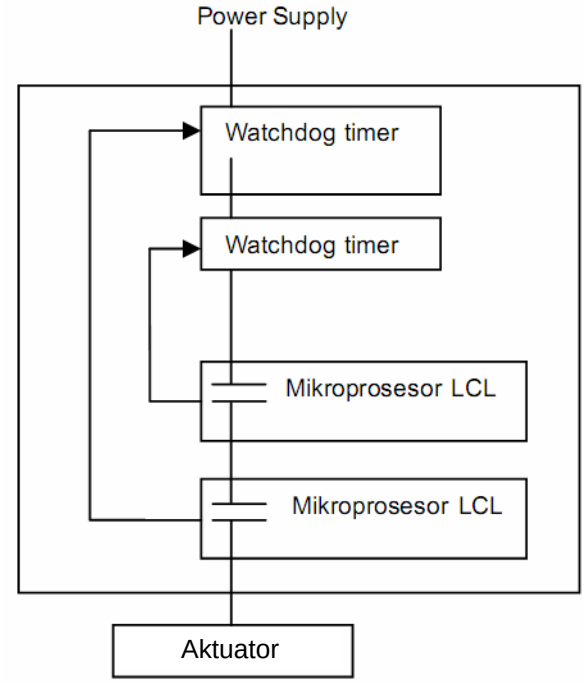
Dari Gambar 1b tampak bahwa modul digital merupakan bagian yang sangat kritis untuk agar fungsi sistem proteksi reaktor terpenuhi. Berbeda dengan rangkaian analog yang menggunakan lebih banyak komponen, kerusakan pada satu komponen (misal Pemrosesan Sinyal untuk input parameter A), tidak langsung mengakibatkan gagalnya fungsi proteksi, karena dibackup oleh komponen/modul yang lain. Dengan demikian, untuk sistem keselamatan yang menggunakan instrumentasi digital diperlukan redundansi kanal. Dalam sistem proteksi reaktor, redundansi empat kanal sudah digunakan sejak teknolog instrumentasi analog, sehingga penggunaan instrumentasi digital tidak mengubah konfigurasi sistem proteksi tersebut.



Gambar 1b. Skema rangkaian pemrosesan sinyal trip menggunakan perangkat digital.

3.2. Penanganan kegagalan prosesor

Sistem instrumentasi digital terdiri dari perangkat keras dan perangkat lunak. Oleh karena itu kegagalannya juga dapat disebabkan oleh kegagalan perangkat keras ataupun kegagalan perangkat lunak. Contoh kegagalan perangkat lunak yaitu prosesor yang menjalankan *loop* pengulangan tanpa henti, sehingga tidak dapat menghasilkan sinyal keluaran.



Gambar 2. Hubungan Watchdog timer dan mikroprosesor dalam unit LCL.

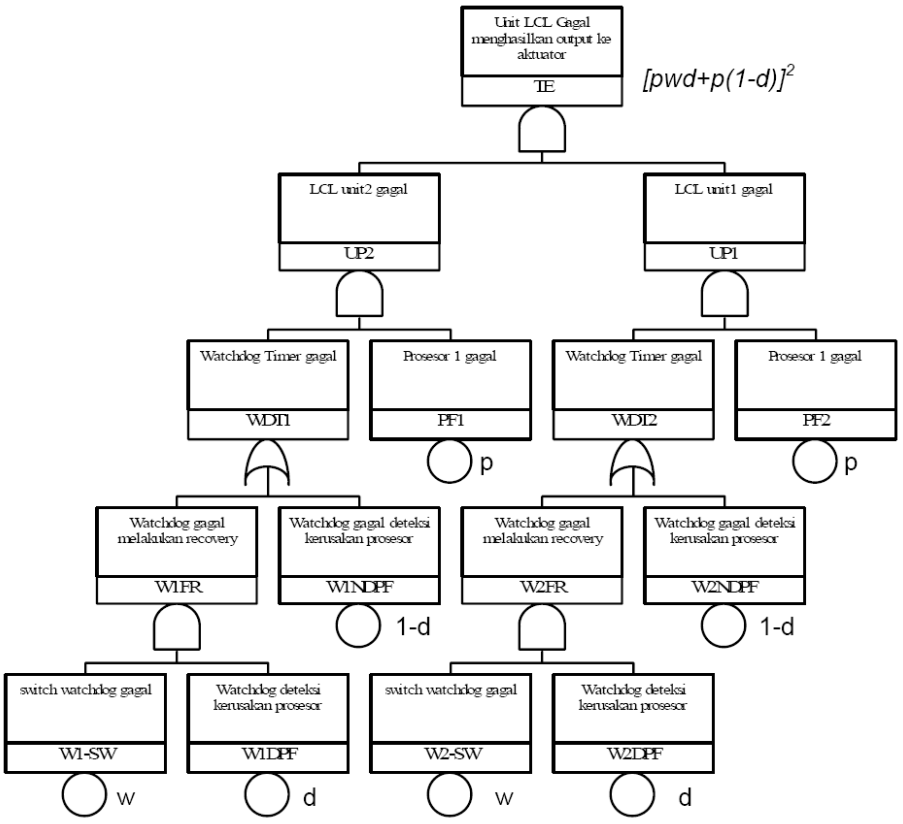
Sistem instrumentasi digital untuk sistem keselamatan didesain secara *fault-tolerant*, artinya sistem tersebut masih bisa berfungsi meskipun terjadi kegagalan di dalam sistem tersebut. Mekanisme *fault-tolerant* adalah dengan melakukan pengecekan integritas sistem, apabila terjadi kegagalan dalam operasi/eksekusi, akan memberikan sinyal pemberitahuan. Metode melakukan penanganan kegagalan prosesor secara *hardware* adalah dengan *watchdog timer*. Perangkat ini akan melakukan pengecekan prosesor secara rutin. Jika terjadi kegagalan prosesor hingga batas *setting*

 ISSN: 0854 - 2910

waktu yang ditentukan telah tercapai, *watchdog timer* akan mengirim sinyal untuk melakukan *reset* sistem. Diagram hubungan *watchdog timer* dengan prosesor ditunjukkan dalam gambar 2[4].

Arsitektur unit *Local Coincidence Logic* (LCL) menggunakan dua prosesor untuk meningkatkan keandalannya. Apabila prosesor pertama gagal beroperasi, fungsi LCL dilakukan oleh prosesor kedua. *Watchdog timer* digunakan untuk memantau bekerja tidaknya kedua prosesor tersebut.

Untuk melihat pengaruh *watchdog timer* terhadap keandalan unit LCL, dilakukan analisis pohon kegagalan (*fault tree*). Untuk keperluan pemodelan, kegagalan *watchdog timer* dibagi dua yaitu karena kegagalan *watchdog timer* mendeteksi kerusakan pada prosesor (kegagalan fungsional) dan kegagalan pada *watchdog timer* itu sendiri. Sedangkan kegagalan LCL dikarenakan kegagalan pada mikroprosesor atau kegagalan *watchdog timer*. Hasil pemodelan pohon kegagalan ditunjukkan pada Gambar 3.



Gambar 3. Model Fault Tree untuk Modul Prosesor LCL.

Dari model pohon kegagalan Gambar 3 dapat diketahui bahwa probabilitas kegagalan modul prosesor LCL adalah $[pwd + p(1-d)]^2$, dimana p adalah probabilitas kegagalan mikroprosesor, w adalah probabilitas kegagalan *switch watchdog timer* untuk membuka, dan d adalah probabilitas keberhasilan *watchdog timer* mendeteksi kegagalan prosesor pada saat beroperasi. Tampak bahwa kegagalan LCL berbanding lurus dengan kegagalan mikroprosesor, karena fungsi LCL memang dijalankan dalam mikroprosesor.

Kemampuan *watchdog timer* untuk melakukan *recovery* sistem dengan cara mendeteksi kegagalan mikroposesor (d) juga sangat berpengaruh pada keandalan LCL. Untuk d = 0 (*Watchdog timer* tidak difungsikan), probabilitas kegagalan LCL sama dengan probabilitas kegagalan mikroprosesor ($F = p^2$, dimana F adalah probabilitas laju kegagalan unit LCL). Untuk d = 1 (*watchdog timer* selalu mendeteksi kegagalan operasi mikroprosesor), probabilitas kegagalan LCL ditentukan oleh keandalan mikroprosesor dan mekanisme *recovery watchdog timer* ($F = (pw)^2$).

4. KESIMPULAN

Dalam makalah ini telah dibahas pengaruh sistem instrumentasi digital untuk sistem keselamatan PLTN, terutama sistem proteksi reaktor. Kemampuan prosesor digital untuk *multi-tasking* menjadi bagian sistem keselamatan yang kritis, sehingga diperlukan redundansi untuk meningkatkan keandalan sistem keselamatan. Untuk mendapatkan sistem yang mampu melakukan penanganan kegagalan prosesor dapat digunakan *watchdog timer*. Keandalan fungsional *watchdog timer* sangat penting untuk meningkatkan keandalan modul prosesor digital LCL.

5. DAFTAR PUSTAKA

[1]. Anonim, “Criteria for Safety Systems for Nuclear Power Generating Stations”, IEEE 603-2009.

[2]. Anonim, “Digital Instrumentation and Control System for Safety System and Main Control Room Design in Japan Nuclear Power Station” JNES, December 2007.

[3]. Smith David J, “Reliability, Maintanability and Risk – Practical Methods for Engineers”, 4th edition, Butterworth – Heinemann, Oxford, 1993.

[4]. Kang H.G., Sung Y.T., Eom H.S., Jeong H.S., Park J.K., Lee K.Y., Park J.K., “The PSA of Safety-Critical Digital I&C System : The Determination of Importan Factors and Sensitivity Analysis” KAERI, 2002.

DISKUSI/TANYA JAWAB:

1. PERTANYAAN: (Sri Sudadiyo, PTRKN-BATAN)

- Untuk meningkatkan keandalan sistem Digital, bagaimana kalau tidak difungsikan secara *multitasking*, tetapi *single tasking* saja?.

JAWABAN: (Sudarno, PTRKN-BATAN)

- *Tentu saja sistem digital dapat difungsikan secara single tasking, tetapi akan menambah banyak perangkat dan kompleksitas sistem. Dengan multitasking, sistem dapat direalisasikan hanya dengan satu prosesor. Redundansi ditujukan untuk meningkatkan keandalan sistem, tapi digunakan untuk multitasking yang sama.*

2. PERTANYAAN: (Pande Made Udiyani, PTRKN-BATAN)

- Apakah sistem Instrumentasi digital juga mempunyai prosedur perawatan seperti pada sistem analog?

ISSN: 0854 - 2910

JAWABAN: (Sudarno, PTRKN-BATAN)

- *Dalam sistem proteksi reactor digital misalnya, sudah dilengkapi dengan MTP (Maintenance and Test Panel), yang mampu melakukan pengetesan sistem proteksi tiap-tiap kanal secara terprogram dari computer. Sehingga prosedur perawatan menjadi lebih mudah.*