EVALUASI SISTEM PROTEKSI REAKTOR DIGITAL PADA REAKTOR DAYA TIPE PWR DENGAN METODA FMEA

Deswandri
Pusat Teknologi Reaktor dan Keselamatan Nuklir

ABSTRAK

EVALUASI SISTEM PROTEKSI REAKTOR DIGITAL PADA REAKTOR DAYA TIPE PWR DENGAN METODA FMEA. Dari aspek keselamatan, Sistem Proteksi Reaktor (RPS) adalah sistem paling vital dalam reaktor nuklir. Pada reaktor generasi lama sistem tersusun dalam rangkaian komponen-komponen analog. Namun, mengikuti perkembangan teknologi elektronika yang pesat belakangan ini, teknologi analog telah ditinggalkan dan digantikan dengan teknologi digital yang sangat praktis, akurat, andal dan mempunyai respons cepat. Pada beberapa reaktor nuklir generasi lama, sistem I&K terkait keselamatan (khususnya RPS) analog juga telah dimodifikasi dengan menggunakan teknologi digital. Sebagai sebuah sistem yang sangat penting dan vital, RPS harus dievaluasi secara menyeluruh untuk menjamin dan memastikan keandalannya. Evaluasi RPS analog sudah banyak dilakukan pada dengan menggunakan teknik evaluasi keandalan tradisional. Akan tetapi, karena aplikasi teknologi digital dalam RPS modern relatif baru, evaluasi keandalan sistem ini masih terbatas dan pada umumnya dilakukan oleh para pengembang sistem itu sendiri. Dalam makalah ini dilakukan evaluasi sistem RPS digital pada reaktor daya tipe PWR dengan menggunakan metoda evaluasi keandalan tradisional yang bersifat kualitatif, yaitu metoda *Failure Mode and Effect Analysis* (FMEA). Sebagai objek, diambil Sistem Proteksi Reaktor digital rancangan Korea Selatan. Ada 8 komponen atau modul yang dievaluasi. Evaluasi dilakukan dengan cara mengkaji atau menyelidiki modus kegagalan yang mungkin terjadi pada masing-masing modul. Dari setiap modus kegagalan, diselidiki penyebab potensial kegagalan tersebut. Selanjutnya dipertimbangkan dampak kegagalan (baik secara lokal maupun terhadap sistem), metoda pendeteksian kegagalan dan tindakan mitigasi yang diperlukan. Hasil evaluasi ditabulasikan dalam bentuk format standar FMEA (Tabel 3).

Kata Kunci : Evaluasi Keandalan, FMEA, RPS Digital

ABSTRACT

THE EVALUATION OF THE DIGITAL REACTOR PROTECTION SYSTEM IN THE PWR TYPED NUCLEAR POWER PLANTS USING FMEA METHOD. *From the aspect of safety, Reactor Protection System (RPS) is the most vital systems in a nuclear reactor. In the old generation reactors, the instrumentation and control (I&C) system are composed of the analog circuit components. Following the recent progress of electronics technology, the analog technology has begun to be abandoned and replaced with digital technology that is very practical, accurate, reliable and have fast response. In some old-generation nuclear reactors, safety related analog I & C system (especially RPS) have also been modified by using digital technology. As a system that is very important and vital, the RPS should be evaluated to assure and ensure its reliability. The evaluation of the analog RPS has been done using a traditional reliability evaluation techniques. However, because the applications of modern digital technology are relatively new in the RPS, the reliability evaluations of the system are still limited and are generally done by the developers of the system itself. In this paper, it has been done the evaluation of the digital RPS of PWR typed nuclear power reactors using the traditional qualitative reliability evaluation method, ie the method of Failure Mode and Effect Analysis (FMEA). The object is the digital Reactor Protection System of South Korean NPPs. There are 8 components or modules that were evaluated. The evaluations were done by reviewing or investigating the failure modes that may occur in each module. For each mode of failure, it was investigated the potential causes of such failure. Then, there were considered the effects of failures (both locally and on the system), the method of fault detection and mitigation measures that are required. The evaluation results are tabulated in a standard format of FMEA (Table 3).*

Keywords : *Reliability Evaluation, FMEA, Digital RPS*

PENDAHULUAN

Dari aspek keselamatan, sistem proteksi reaktor (RPS) adalah sistem paling vital dalam reaktor nuklir, baik untuk reaktor riset maupun reaktor daya (PLTN). Sistem ini merupakan salah satu sistem instrumentasi dan kendali (I&K) terkait keselamatan, yang terdiri dari sejumlah sensor yang memonitor variabel keselamatan secara *real-time*, komponen pengkondisi sinyal, prosesor, *voting logic*, relai dan pemutus arus pemegang batang kendali. Sistem bekerja untuk menjatuh batang kendali ke dalam teras agar reaktor *shutdown* secepat nya, ketika sensor-sensor mendeteksi terjadinya penyimpangan pada variabel - variabel keselamatan dalam teras maupun pada tempat tertentu di luar teras reaktor.

Pada awalnya RPS dibangun dengan menggunakan teknologi analog, seperti yang ditemukan pada reaktor-reaktor generasi lama. Dengan perkembangan teknologi elekronika yang begitu pesat pada tahun-tahun belakangan ini, teknologi analog telah ditinggalkan dan digantikan dengan teknologi digital yang sangat praktis, akurat, andal dan mempunyai respons cepat. Pada desain reaktor generasi maju, teknologi digital ini telah diterapkan secara penuh, baik pada sistem instrumentasi dan kendali yang tidak terkait keselamatan maupun yang terkait dengan keselamatan seperti sistem RPS. Pada sejumlah reaktor generasi lama, karena masalah penuaan komponen dan sulit nya dukungan suku-cadang dari pabrikan serta banyaknya kelebihan yang didapat dari sistem digital, sistem I&K terkait keselamatan (khususnya RPS) analog juga telah dimodifikasi dengan menggunakan teknologi digital; seperti pada reaktor daya Kashiwazaki-Kariwa 6 & 7, Hamaoka-5 dan Tomari-3 di Jepang [(1)], Sizewell B di Inggris [(1)], Kalinin-3 di Rusia [(1)] serta Ringhals 1 & 2 di Swedia [(2)] .

Sebagai sebuah sistem yang sangat penting dan vital, keselamatan RPS harus dievaluasi secara menyeluruh untuk menjamin dan memastikan keandalannya. Evaluasi ini sudah banyak dilakukan pada RPS analog dengan menggunakan teknik evaluasi keandalan tradisional. Akan tetapi, karena teknologi digital dalam RPS modern relatif baru, evaluasi keandalan sistem ini masih terbatas dan pada umumnya dilakukan oleh para pengembang sistem itu sendiri.

Evaluasi keandalan secara tradisional dapat dikategorikan ke dalam dua kategori, yaitu metoda kualitatif dan metoda kuantitatif. Kedua metoda ini berbagi peran untuk memastikan dan meninjau tingkat keandalan sebuah sistem yang dievaluasi. Teknik kualitatif memfokuskan perhatian pada pertanyaan " apa yang mesti/ bisa salah, sedemikian sehingga sistem menjadi beresiko". Sedangkan teknik kuantitatif melakukan estimasi probabilitas, laju dan atau tingkat keparahan suatu resiko pada sistem [(3)].

Tujuan makalah ini adalah melakukan evaluasi sistem RPS digital dari reaktor daya tipe PWR dengan menggunakan salah satu metoda evaluasi keandalan tradisional yang bersifat kualitatif, yaitu metoda *Failure Mode and Effect Analysis* (FMEA)[(4)]. Sebagai objek studi, diambil sistem RPS digital di PLTN rancangan Korea Selatan.

DESKRIPSI SISTEM RPS

Dalam sistem keselamatan reaktor daya nuklir (khususnya reaktor tipe PWR desain Korea Selatan), ada dua istilah yang perlu dibedakan, yaitu: Sistem Proteksi Instalasi (*Plant Protection System*) dan Sistem Proteksi Reaktor (RPS). Sistem Proteksi Instalasi adalah sistem yang berjangkauan lebih luas, di mana sistem ini berfungsi tidak saja melindungi teras reaktor akan tetapi juga seluruh sistem yang ada dalam reaktor daya tersebut. Yang termasuk dalam sistem ini antara lain kumpulan sensor-sensor, komponen pengkondisi sinyal, RPS, sistem pemegang batang kendali dan fitur-fitur keselamatan teknis (*Engineering Safety Features*). Sedangkan RPS terbatas pada kumpulan modul-modul yang memproses sinyal trip yang dikirimkan oleh sensor-sensor pengukur variabel keselamatan reaktor, demikian ketika terdeteksi nilai abnormal yang melampaui nilai batas keselamatan, sistem segera memproses dan mengirim sinyal trip ke sistem pemegang batang kendali, sehingga batang kendali segera jatuh bebas ke dalam teras untuk men*scram* reaktor.

Sistem Proteksi Reaktor (RPS) digital desain Korea [5] dirancang dengan arsitektur redundansi *2 out of 4*, dimana setiap kanal diimplementasi kan dalam arsitektur yang sama. Setiap kanal RPS terdiri dari beberapa modul seperti: *Bi-stable Processor* (BP), *Local Coincidence Logic Processor* (LCP), *AutomaticTest & Interface Process* (ATIP), *Cabinet Operator Module* (COM) dan *High Reliable Safety Data Link* (HR-SDL). BP membangkitkan sinyal trip dengan cara membandingkan masukan sinyal dari sensor-sensor keselamatan reaktor terhadap nilai *setting point trip* untuk keselamatan. Sinyal trip yang dibangkitkan oleh BP dikirimkan ke LCP seluruh kanal melalui HR-SDL. LCP memonitor sinyal trip dari setiap kanal BP, jika dua atau lebih kanal memberikan sinyal trip maka BP akan mengaktivasi sinyal *output* untuk men*trip* reaktor. ATIP memonitor status operasi RPS dan melakukan tes pengawasan untuk memastikan keandalan operasi BP dan LCP pada kanal yang sama. Hasil tes dikirim ke COM di Ruang Kendali Utama (RKU). Masing-masing modul BP, LCP dan ATIP dimplementasikan dalam bentuk *Safety Grade Programmable Logic Controller* (PLC), COM dalam bentuk *Industrial PC* dan HR-SDL merupakan *Profibus FDL* (*Fieldbus Data Link*).

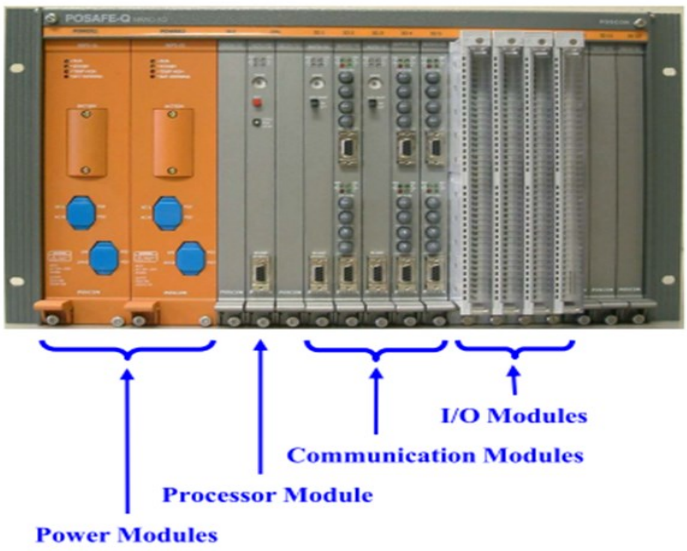
Gambar 1 memperlihatkan *prototype Safety Grade Programmable Logic Controller* yang dirancang untuk sistem instrumentasi dan kendali reaktor daya standar Korea. Gambar 2 memperlihatkan diagram interkoneksi masing-masing PLC dalam satu kanal RPS.

METODOLOGI

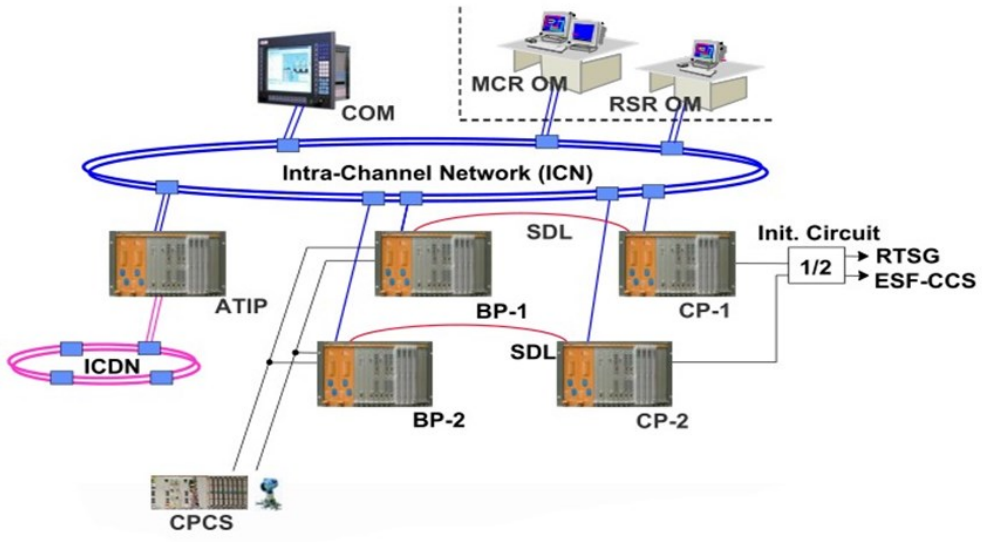
Evaluasi keandalan yang dilakukan terhadap desain RPS dalam makalah ini merupakan evaluasi bersifat kualitatif. Ada beberapa metoda evaluasi kualitatif dalam teknik keandalan (*reliability engineering*), dalam makalah ini metoda yang dipakai adalah metoda *Failure Mode and Effect Analysis* (FMEA). FMEA adalah suatu prosedur sistematis untuk memeriksa setiap komponen atau bagian dalam suatu

sistem, mengidentifikasi bagaimana komponen atau bagian tersebut dapat gagal beserta penyebab kegagalannya, menentukan bagaimana kegagalan *item* tersebut dapat mempengaruhi sistem, serta menetapkan langkah-langkah untuk memitigasi dampak kegagalan tersebut.

FMEA merupakan metoda yang bersifat *bottom-up*, dimana evaluasi dilakukan mulai dari komponen dasar menuju ke sistem keseluruhan. Langkah-langkah yang dilakukan dalam mengevaluasi sistem dengan FMEA adalah sebagai berikut:



Gambar 1. *Safety Grade Programmable Logic Controller* (PLC) Desain Korea[6]



Gambar 2. Diagram Interkoneksi Modul-Modul Penyusun RPS Digital Desain Korea[7]

1. Identifikasi komponen atau bagian penyusun sistem beserta fungsi terkait.
2. Identifikasi dengan cara bagaimana komponen atau bagian sistem bisa gagal (modus kegagalan).
3. Investigasi penyebab kegagalan masing-masing modus kegagalan komponen atau bagian sistem.
4. Pelajari dampak atau efek dari setiap modus kegagalan.
5. Definisikan cara atau metoda untuk mendeteksi modus kegagalan.
6. Tetapkan langkah-langkah untuk memitigasi, mencegah atau mengatasi modus kegagalan tersebut.

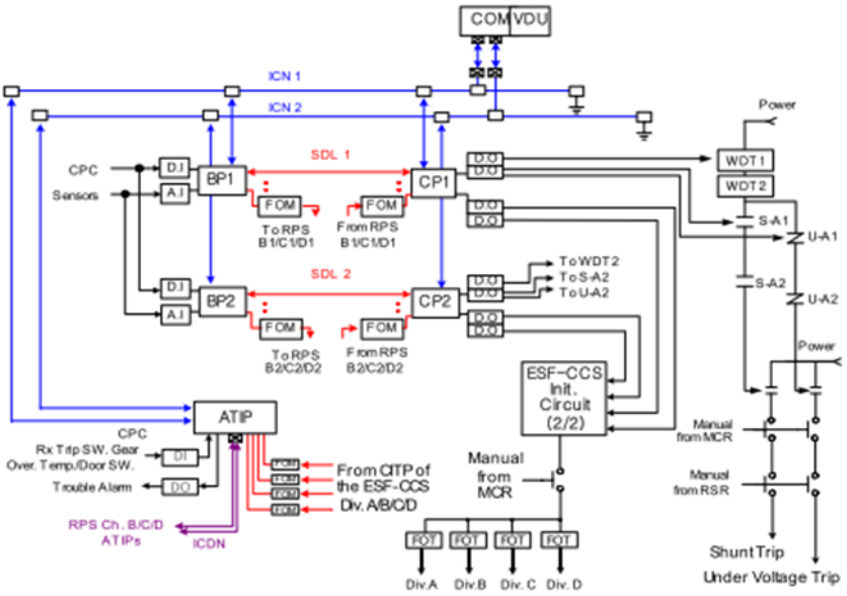
Diagram alir pelaksanaan metoda FMEA diberikan dalam Gambar 3.

Gambar 3. Diagram Alir Pelaksanaan FMEA Dalam Mengevaluasi Sistem [4]

Sebagaimana yang telah dibahas di bagian atas, langkah pertama dalam pelaksanaan metoda FMEA adalah mengidentifikasi komponen atau bagian-bagian penyusun sistem beserta fungsinya. Langkah ini pada dasarnya adalah kegiatan untuk mempelajari sistem secara menyeluruh, serta untuk mengetahui bagaimana interaksi masing-masing komponen atau bagian dalam sistem. Pembuatan blok diagram sistem akan sangat membantu dalam langkah ini. Gambar 4 memperlihatkan blok diagram RPS digital desain Korea.

HASIL EVALUASI dan PEMBAHASAN

Berdasarkan hasil kajian yang diperoleh dari informasi Gambar 4, dapat diuraikan modul-modul penyusun sistem beserta fungsi masing-masing, sebagaimana yang tercantum dalam Tabel 1.



Gambar 4. Blok Diagram RPS Digital Desain Korea [5]

Tabel 1. Komponen Utama Penyusun RPS dan Fungsinya

No	Komponen	Fungsi
1.	*Bi-stable Processor* (BP)	Memonitor variabel proses, membandingkan dengan nilai *Set Point* dan membangkitkan sinyal trip
2.	*Local Coincidence Logic Processor* (LCP)	Membandingkan sinyal trip *bi-stable* dari keempat kanal RPS dan memicu sinyal inisiasi trip berdasarkan *voting logic 2 out of 4*
3.	*Automatic Test & Interface Process* (ATIP),	Memonitor status operasi RPS dan melakukan *surveillance test* untuk menjamin keandalan operasi BP dan LCP. Hasil test dikirimkan ke COM
4.	*Cabinet Operator Module* (COM)	Fasilitas antar-muka operator dengan RPS (diimplementasikan dalam bentuk PC skala industri dan displai panel datar)
5.	*High Reliable Safety Data Link* (HR-SDL)	Modul komunikasi yang menghubungkan BP dengan LCP.
6.	Modul *Input*	Antar-muka antara pemproses sinyal dari sensor-sensor keselamatan dengan BP
7.	Modul *Output*	Antar-muka antara LCP dengan *Trip Logic Initiating Circuit*
6.	*Power Supply*	Memberikan daya pada masing-masing modul

Dari daftar komponen pada Tabel 1 di atas, hasil evaluasi komponen dapat digolongkan dalam tiga kategori umum peralatan elektronika, yaitu: PLC, Catu Daya dan *Board* Komunikasi. Modus kegagalan untuk PLC adalah kegagalan memberikan sinyal atau memberikan sinyal trip yang salah (*spurious trip*). Penyebab kegagalan memberikan sinyal

adalah karena komponen elektronika modul rusak, degradasi komponen, kesalahan perawatan, kerusakan/kesalahan program dan kehilangan catu daya. *Spurious trip* terjadi akibat kesalahan desain CPU atau kesalahan program.

Modus kegagalan dari modul BP adalah kegagalan memberikan sinyal *trip* atau sinyal yang diberikan salah. Akibat lokal dari kegagalan ini adalah tidak adanya input sinyal *trip* pada modul LCP atau input sinyal *trip* yang masuk pada modul LCP merupakan sinyal yang salah. Kegagalan memberikan sinyal pada modul BP mengakibatkan keandalan sistem RPS berkurang karena satu kanal (kanal tempat modul BP yang gagal terpasang) gagal memberikan sinyal *trip*. Sistem masih bisa berfungsi, selama tiga kanal lain dapat berfungsi. Efek dari sinyal output yang salah dari modul BP berpotensi untuk men*trip* reaktor tanpa alasan keselamatan. Hal ini terjadi jika satu kanal lain juga mengalami hal yang sama.

Modus kegagalan dari modul LCP sama dengan modus kegagalan modul BP. Efek lokal dan efek menyeluruh terhadap sistem juga sama dengan efek yang ditimbulkan dari kegagalan modul BP, seperti yang telah dijelaskan pada paragraf di atas.

Modus kegagalan modul ATIP adalah gagal menginisiasi tes atau gagal mengirim sinyal hasil tes ke modul COM. Akibatnya adalah modul BP dan LCP pada kanal yang sama tidak dapat dites secara otomatis atau status operasi modul BP dan LCP tidak tampil di panel ruang kendali. Terhadap sistem, kegagalan modul ATIP menginisiasi tes menyebabkan operator tidak tahu status operasi RPS setiap saat, sehingga harus menunggu jadwal perawatan periodik untuk mengetahuinya. Hal yang sama juga berlaku untuk modus kegagalan modul ATIP yang gagal memberikan sinyal hasil tes ke modul COM. Modus kegagalan modul COM adalah gagal berfungsi. Pengaruh lokal dan pengaruh menyeluruh terhadap sistem sama dengan kegagalan yang terjadi pada modul ATIP, seperti yang telah dijelaskan pada paragraf di atas.

Modus kegagalan untuk modul HR-SDL adalah gagal berfungsi. Akibat lokal dari kegagalan ini adalah terputusnya hubungan antara modul BP dan LCP yang terpasang dalam satu kanal. Akibat yang timbul terhadap sistem adalah keandalan sistem berkurang karena satu kanal gagal berfungsi.

Modus kegagalan untuk *Modul Input* dan *Output* adalah gagal berfungsi. Kegagalan *Modul Input* menyebabkan kegagalan modul prosesor BP menerima sinyal dari sensor-sensor keselamatan, sedangkan kegagalan Modul *Output* menyebabkan kegagalan modul prosesor LCP meneruskan sinyal trip ke modul *Trip Initiation Logic* untuk men*trip* reaktor.

Modus kegagalan pada modul *Power Supply* adalah memberikan voltase terlalu rendah (dan atau mati) atau terlalu tinggi. Voltase terlalu rendah menyebabkan seluruh komponen aktif dalam satu kanal dengan *power supply* tidak dapat berfungsi, sedangkan voltase terlalu tinggi menyebabkan komponen rusak atau terbakar. Akibat terhadap sistem adalah berkurangnya

keandalan karena satu kanal gagal berfugsi.

Tabel 2 memberikan uraian modus kegagalan beserta penyebabnya untuk masing-masing komponen utama penyusun RPS secara lebih terperinci.

Untuk setiap modus kegagalan modul BP dan LCP beserta modul *input-output*nya, metoda pendeteksiannya adalah secara pengujian otomatis melalui modul ATIP, pengujian manual atau perawatan periodik. Modus kegagalan modul ATIP dan COM dideteksi melaui pengujian manual atau perawatan periodik. Untuk langkah mitigasi, setiap kanal yang gagal diisolasi untuk proses perawatan, dan redundansi dirubah menjadi 2 *out of* 3.

Resume dari hasil FMEA ini dicantumkan dalam bentuk format standar FMEA, seperti yang diberikan dalam Tabel 3.

Tabel 2. Modus Kegagalan Komponen Utama RPS dan Penyebabnya

No	Komponen	Modus dan Sebab Kegagalan
1.	*Bi-stable Processor* (BP)	Modus: gagal memberikan sinyal trip Sebab: kerusakan komponen, degradasi komponen, kerusakan *software*, kesalahan *setting point* (nilai terlalu besar) dan kehilangan catu daya. Modus: *spurious trip* Sebab: kesalahan desain cpu dan kesalahan *software*.
2.	*Local Coincidence Logic Processor* (LCP)	Modus: gagal memberikan sinyal inisiasi trip Sebab: kerusakan komponen, degradasi komponen, kerusakan *software*, kesalahan perawatan dan kehilangan catu daya. Modus: *spurious trip* Sebab: kesalahan desain cpu dan kesalahan *software*.
3.	Automatic *Test & Interface Process* (ATIP),	Modus: gagal menginisiasi tes Sebab: kerusakan komponen, degradasi komponen, kerusakan *software* , kesalahan perawatan dan kehilangan catu daya. Modus: gagal mengirim sinyal ke COM Sebab: kerusakan komponen, degradasi komponen, kerusakan *software*, kesalahan perawatan.
4.	*Cabinet Operator Module* (COM)	Modus: gagal berfungsi Sebab: kerusakan komponen/komputer, kegagalan *software*, kerusakan display dan kehilangan catu daya.
5.	*High Reliable Safety Data Link* (HR-SDL)	Modus: gagal menghubungkan BP dengan LCP Sebab: kerusakan komponen, degradasi komponen, kerusakan *software*, kesalahan perawatan dan kehilangan catu daya.
6	*Input Module*	Modus: gagal berfungsi Sebab: kerusakan komponen, degradasi komponen, kerusakan *software*, kesalahan perawatan dan kehilangan catu daya.
7	*Output Module*	Modus: gagal berfungsi Sebab: kerusakan komponen, degradasi komponen, kerusakan *software*, kesalahan perawatan dan kehilangan catu daya.
8.	*Power Supply*	Modus: voltase terlalu rendah Sebab: kerusakan rangkaian dan hubungan singkat (*short-circuit*). Modus: voltase terlalu tinggi Sebab: kerusakan rangkaian dan hubungan singkat (*short-circuit*).

KESIMPULAN

Sudah dilakukan evaluasi desain RPS digital dari reaktor daya tipe PWR rancangan Korea Selatan dengan menggunakan metoda *Failure Mode and Effect Analysis* (FMEA). Berdasarkan hasil kajian dari cara kerja sistem, ada 8 modul utama yang perlu dievaluasi. Evaluasi meliputi identifikasi modus kegagalan yang mungkin terjadi pada masing-masing modul, penyebab potensial modus kegagalan, dampak kegagalan (baik secara lokal maupun terhadap sistem), metoda pendeteksian kegagalan serta tindakan mitigasi yang diperlukan. Hasil evaluasi diberikan dalam bentuk format standar FMEA, seperti pada Tabel 3..

DAFTAR PUSTAKA

1. http://www.iaea.org/About/Policy/GC/GC52/GC52InfDocuments/English/gc52inf-3-att5_en.pdf, diakses tanggal 13 Januari 2011.
2. Authen, Stefan, et. all, *Guidelines for reliability analysis of digital systems in PSA context; Phase 1 Status Report*, NKS-230 Report, NKS, Denmark, 2010.
3. http://en.wikipedia.org/wiki/Safety_engineering, diakses tanggal 13 Januari 2011.
4. Ford Design Institute, *FMEA Handbook Version 4.1*, Ford Motor Company, 2004.
5. Lee, Dong-Young, Choi, Jong-Gyun dan Lyou, Joon, *A Safety Assessment Methodology for a Digital Reactor Protection System*, International Journal of Control, Automation, and Systems, vol. 4, no. 1, pg. 105-112, February 2006.
6. Lee, Cheol-Kwon, *Presentation Material at IAEA Technical Meeting*, Beijing 2008, http://entrac.iaea.org, diakses tanggal 13 Januari 2011.
7. Lee, Seong-Jin, 2008 KEPIC-Week, www.kepic.or.kr/week_2008/down/E1-6.pdf, diakses tanggal 13 Januari 2011.

Tabel 3. Tabel FMEA untuk Sistem Proteksi Reaktor

Item No.	*Component*	*Function*	*Failure Mode*	*Possible Failure Cause*
1	*Bi-stable Processor* (BP)	Memonitor variabel proses, membandingkan dengan nilai *Set Point* dan membangkitkan sinyal *trip*	Gagal Memberikan Sinyal *Output*	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software*, Kesalahan *Setting Point* (nilai terlalu besar) dan kehilangan catu daya
			Sinyal *Output* Salah	Kesalahan Desain CPU dan Kesalahan *Software*.
2	*Local Coincidence Logic Processor* (LCP)	Membandingkan sinyal *trip bi-stable* dari keempat kanal RPS dan memicu sinyal inisiasi *trip* berdasarkan *voting logic 2 out of 4*	Gagal Memberikan Sinyal *Output*	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software*, Kesalahan pengesetan *voting logic* dan kehilangan catu daya
			Sinyal *Output* Salah	Kesalahan Desain CPU dan Kesalahan *Software.*
3	*Automatic Test & Interface Process* (ATIP),	Memonitor status operasi RPS dan melakukan *surveillance test* untuk menjamin ketersediaan operasi BP dan LCP. Hasil test dikirimkan ke COM	Gagal menginisiasi tes	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software* , Kesalahan Perawatan dan kehilangan catu daya
			Gagal mengirim sinyal ke COM	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software*, Kesalahan Perawatan
4	*Cabinet Operator Module* (COM)	Fasilitas antar-muka operator dengan RPS (diimplementasikan dalam bentuk PC skala industri dan displai panel datar)	Gagal berfungsi	Kerusakan Komponen/komputer, Kegagalan *Software*, Kerusakan displai dan kehilangan catu daya.
5	*High Reliable Safety Data Link* (HR-SDL)	Modul komunikasi yang menghubungkan BP dengan LCP.	Gagal berfungsi	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software*, Kesalahan Perawatan dan kehilangan catu daya
6	*Input Module*	Antar-muka antara sinyal dari sensor-sensor keselamatan dengan modul prosesor BP	Gagal berfungsi	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software*, Kesalahan Perawatan dan kehilangan catu daya
7	*Output Module*	Antar-muka antara modul LCP dengan modul *Reactor Trip Initiation Logic*	Gagal berfungsi	Kerusakan Komponen, Degradasi Komponen, Kerusakan *Software*, Kesalahan Perawatan dan kehilangan catu daya
8	*Power Supply*	Memberikan daya pada masing-masing modul	Voltase terlalu rendah	Kerusakan rangkaian dan komponen
			Voltase terlalu tinggi	Kerusakan rangkaian dan hubungan singkat (*short-circuit*)

Tabel 3. Tabel FMEA untuk Sistem Proteksi Reaktor (sambungan)

Item No.	*Component*	*Failure Mode*	*Failure Effect to System*	*Detection Method*	*Mitigation*
1	*Bi-stable Processor* (BP)	Gagal Memberikan Sinyal *Output*	Tidak ada efek yang signifikan terhadap operasionalitas sistem selama dua kanal lain sukses beroperasi. Efek minor yang timbul hanyalah keandalan sistem berkurang karena satu kanal tidak tersedia.	Pengujian otomatis melalui modul ATIP, pengujian manual atau perawatan periodik.	Isolasi kanal yang gagal (untuk perawatan) dan ubah *setting redundancy* menjadi 2 *out of* 3.
		Sinyal *Output* Salah	Memungkinkan reaktor *trip* tanpa alasan keselamatan (apabila 1 kanal lain juga mengalami hal yang sama)	Pengujian manual atau perawatan periodik	Dipulihkan melalui perawatan
2	*Local Coincidence Logic Processor* (LCP)	Gagal Memberikan Sinyal *Output*	Tidak ada efek yang signifikan terhadap operasionalitas sistem selama dua kanal lain sukses beroperasi. Efek minor yang timbul hanyalah keandalan sistem berkurang karena satu kanal tidak tersedia.	Pengujian otomatis melalui modul ATIP, pengujian manual atau perawatan periodik.	Isolasi kanal yang gagal (untuk perawatan) dan ubah *setting redundancy* menjadi 2 *out of* 3.
		Sinyal *Output* Salah	Memungkinkan reaktor *trip* tanpa alasan keselamatan (apabila 1 kanal lain juga mengalami hal yang sama)	Pengujian manual atau perawatan periodik	Dipulihkan melalui perawatan
3	*Automatic Test & Interface Process* (ATIP),	Gagal menginisiasi tes	Tidak ada efek terhadap operasionalitas sistem. Efek minor yang timbul hanyalah status operasi RPS pada kanal ini tidak terpantau secara otomatis	Pengujian manual atau perawatan periodik	Isolasi modul untuk perawatan.
		Gagal mengirim sinyal ke COM	Tidak ada efek terhadap operasionalitas sistem. Efek minor yang timbul hanyalah operator tidak tahu status operasi RPS pada kanal ini secara *real time*	Seketika	Isolasi modul untuk perawatan.
4	*Cabinet Operator Module* (COM)	Gagal berfungsi	Tidak ada efek terhadap operasionalitas sistem. Efek minor yang timbul hanyalah operator tidak tahu status operasi RPS pada kanal ini secara *real time*	Seketika	Isolasi modul untuk perawatan.
5	*High Reliable Safety Data Link* (HR-SDL)	Gagal berfungsi	Tidak ada efek yang signifikan terhadap operasionalitas sistem selama dua kanal lain sukses beroperasi. Efek minor yang timbul hanyalah keandalan sistem berkurang karena satu kanal tidak tersedia.	Pengujian otomatis melalui modul ATIP, pengujian manual atau perawatan periodik.	Isolasi kanal yang gagal (untuk perawatan) dan ubah *setting redundancy* menjadi 2 *out of* 3.
6	*Input Module*	Gagal berfungsi	Tidak ada efek yang signifikan terhadap operasionalitas sistem selama dua kanal lain sukses beroperasi. Efek minor yang timbul hanyalah keandalan sistem berkurang karena satu kanal tidak tersedia.	Pengujian otomatis melalui modul ATIP, pengujian manual atau perawatan periodik.	Isolasi kanal yang gagal (untuk perawatan) dan ubah *setting redundancy* menjadi 2 *out of* 3.
7	*Output Module*	Gagal berfungsi	Tidak ada efek yang signifikan terhadap operasionalitas sistem selama dua kanal lain sukses beroperasi. Efek minor yang timbul hanyalah keandalan sistem berkurang karena satu kanal tidak tersedia.	Pengujian otomatis melalui modul ATIP, pengujian manual atau perawatan periodik.	Isolasi kanal yang gagal (untuk perawatan) dan ubah *setting redundancy* menjadi 2 *out of* 3.
8	Power Supply	Voltase terlalu rendah	Tidak efek yang signifikan selama *power supply* cadangan sukses beroperasi.	Pengujian manual atau perawatan periodik	Isolasi *power supply* yang rusak untuk perawatan.
		Voltase terlalu tinggi	Tidak efek yang signifikan selama *power supply* cadangan sukses beroperasi.	Pengujian manual atau perawatan periodik	Isolasi *power supply* yang rusak untuk perawatan.