ANALISIS DESAIN SISTEM PROTEKSI REAKTOR PWR

Djen Djen Djainal
Pusat Teknologi Reaktor dan Keselamatan Nuklir (PTRKN) - BATAN
Kawasan PUSPIPTEK Gd. No. 80 Serpong, Tangerang Selatan 15310
e-mail: djenbptkn@gmail.com

ABSTRAK

ANALISIS DESAIN SISTEM PROTEKSI REAKTOR PWR. Sistem proteksi reaktor adalah sistem yang penting pada instalasi pembangkit listrik tenaga nuklir, karena sistem ini yang men" shutdown" reaktor untuk menjaga keutuhan teras dan menjaga tekanan normal sistem pendingin reaktor ketika kondisi parameter proses mencapai batas keselamatan tertentu. Untuk menjamin pengoperasian reaktor yang aman, sistem proteksi reaktor didesain dengan kriteria redundansi. Sistem proteksi reaktor dalam menghindari terjadinya kegagalan tunggal didesain mengambil arsitektur 2 keluaran dari 3 selain ada juga 2 keluaran dari 4. Sistem proteksi reaktor arsitektur 2 keluaran dari 3 berisikan 3, yang masing-masing jalurnya memiliki arsitektur yang sama. Makalah ini menerangkan kajian keselamatan sistem proteksi reaktor PWR yang mengambil arsitektur sistem proteksi 2 keluaran dari 3 dengan menggunakan teknik analisis probabilitas pohon kegagalan. Tujuannya untuk melihat sejauh mana desain redundansi yang menggunakan arsitektur 2 keluaran dari 3 bermanfaat dalam keselamatan. Hasil yang diperoleh dari analisis membuktikan secara kuantitatif bahwa desain redundansi ini berkontribusi pada keselamatan secara signifikan.
Kata kunci: Sistem proteksi reaktor, desain, analisis, keselamatan

ABSTRACT

REACTOR PROTECTION SYSTEM OF PWR DESIGN ANALYSIS. *The Reactor Protection System (RPS) is a very important system in a nuclear power plant because the system shuts down the reactor to maintain the reactor core integrity and the reactor coolant system pressure boundary if the plant conditions approach the specified safety limits. To assure the safe operation of a reactor, the RPS is designed according to the redundancy criteria. The RPS usually adopts the 2-out- of-3 or in other hand the 2-out-of-4 architecture to prevent a single failure. The 2-out-of-3 RPS system consists of three channels, and each channel is implemented with the same architecture. This paper describes the safety assessment of a PWR reactor protection system adopts the architecture 2 out of 3 using the fault tree analysis technique. The goal is to see the safety benefit the extent of redundancy design that adopts the architecture 2 out of 3. Results obtained from quantitative analysis to prove that the design of this redundancy is significantly contribute to safety.*
Keywords: *Reactor protection system, design, analisys, safety*

1. PENDAHULUAN

Sumber bahaya suatu reaktor nuklir terletak pada terakumulasinya produk fisi radioaktif dalam kelongsong bahan bakar. Jika terjadi kerusakan pada kelongsong maka produk fisi tersebut akan keluar melalui uap atau terlarut dalam pendingin dan menyebar. Oleh karenanya usaha keselamatan selama ini yang dilakukan ialah mempertimbangkan agar kelongsong tidak rusak dalam kondisi apapun, oleh karena itu, PLTN dilengkapi dengan sistem Instrumentasi dan pengendali (*I&C*). guna menjaga semua parameter proses tetap pada kondisi yang telah ditetapkan sehingga mencegah tersebarnya produk fisi.

Tiga kelompok fungsi utama sistem instrumentasi dan pengendalian *(I&C*) suatu PLTN[1] adalah melakukan

- Sistem pengamatan(*monitoring*) dan tampilan (*display*),
- sistem pengendalian(*control*)

 ISSN: 0854 - 2910

- sistem perlindungan (*protection*) dan mitigasi.

Sistem proteksi reaktor*(RPS)* yang dibahas dalam paper ini berada dalam sistem proteksi (*Plant Protection System*) bersama dengan *ESFAS (Engineered Safety Feature Actuation System).* Sistem proteksi reaktor melakukan *shutdown* darurat sebagai tindakan untuk menjaga keutuhan teras dan menjaga tekanan normal pada seluruh sistem pendingin reaktor. Sistem proteksi reaktor dirancang harus memenuhi persyaratan *Fail safe*, yaitu jika terjadi kegagalan dalam *RPS* sendiri maka reaktor akan *trip*, dengan kata lain jika dalam sistem *RPS* ada ketidak andalan sistem reaktor masih aman[2]. Untuk menjamin keselamatan operasi reaktor perlu diusahakan dengan meningkatkan keandalan *RPS*, yaitu dengan cara redudansi. Sistem proteksi reaktor biasanya mengadopsi arsitektur 2 keluaran dari 3 atau 2 keluaran dari 4 untuk mencegah terjadi kegagalan tunggal. Sistem proteksi reaktor 2 keluaran dari 4 terdiri atas 4 saluran yang masing masing salurannya mempunyai arsitektur yang sama.

Sistem instrumentasi dan pengendalian *(I&C)* dilain hal dikelompokan dalam dua kategori keselamatan yaitu kelompok *safety* dan *nonsafety. Nonsafety* sistem digunakan operator untuk memonitor dan mengendalikan operasi normal seperti men *starup* dan *shutdown* instalasi. Evaluasi dan analisis keselamatan biasa ditekankan pada sistem instrumentasi dan pengendalian *(I&C)* kelompok *safety*, yaitu sistem proteksi dan mitigasi, namun demikian tidak berarti kelompok *nonsafety* diabaikan, sebab kemunculan kegagalan pada sistem monitoring dan control akan merupakan *initiating events* pada sistem proteksi dan mitigasi.

Metode yang tepat yang dimiliki untuk dapat dipakai evaluasi keselamatan dan keandalan komponen/peralatan merupakan *tools* yang menjadi dasar mengambil keputusan apakah suatu sistem dapat dipakai atau tidak. Dalam lingkup PLTN teknik deterministik dan probabilistik dan/atau kombinasinya sudah dipakai untuk kajian keselamatan dan keandalan PLTN[1]. sebagai contoh *Design basis accident analysis* merupakan kajian deterministik, demikian juga analisis respon *thermal* dari kecelakaan yang dipostulasikan semisal pipa pendingin primer pecah.

Tujuan penelitian pada makalah ini melakukan analisis desain sistem proteksi dan kajian keselamatan kuantitatif (*quantitative safety*) desain redundansi sistem proteksi reaktor yang memiliki arsitektur 2 keluaran dari 3 dengan teknik probabilistik, untuk memberikan gambaran dan membuktikan bahwa persyaratan persyaratan yang diterapkan pada desain sistem proteksi PWR harus betul betul dipenuhi.

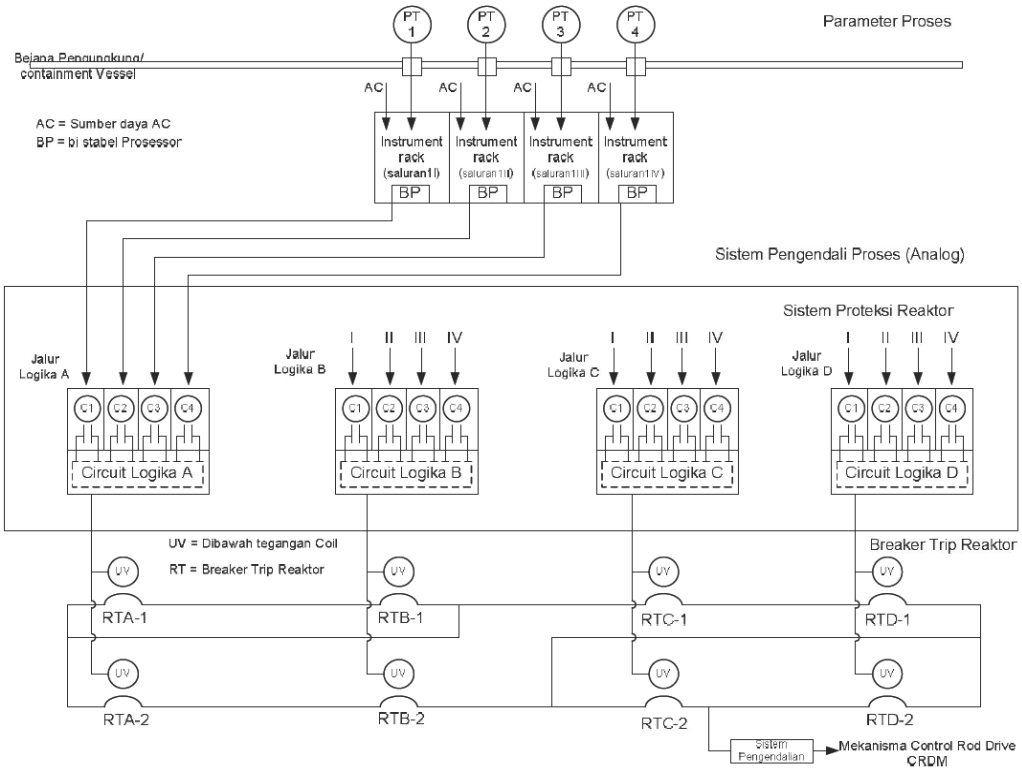
2. SISTEM PROTEKSI PWR

Reactor Protection System (RPS) adalah sistem yang penting dalam instalasi rektor. Sistem ini yang men *shutdown* reaktor ketika terjadi anomali pada parameter proses dalam reaktor, sehingga keutuhan bahan bakar terjaga dan tekanan pada lingkup pendingin reaktor terpelihara. RPS terdiri atas sensor, bagian proses aritmatik, bagian logika dan perlengkapan lain yang diperlukan (seperti untuk memonitor kondisi komponen parameter proses tertentu, perlengkapan untuk keandalan dan perlengkapan reaktor trip)[4].

Instrumentasi utama Sistem Proteksi Reaktor terdiri atas:

1. Bagian sirkuit analog terdiri atas 3 saluran (atau 4 saluran).
2. Bagian sirkuit logika berisikan 3 jalur (atau 4 jalur)
3. Bagian *breaker trip* reaktor menggunakan sistem redundansi dan dirancang independent.

Sebagaimana disajikan pada gambar 1 RPS terdiri atas bagian sirkuit analog berisikan atas 4 saluran (ada juga yang hanya 3 saluran), bagian sirkuit logika berisikan 4 jalur (ada juga yang 3 jalur) dan trip breaker yang masing masing independen dan dirancang secara redudansi. Bagian sirkuit analog menerima sinyal dari masing masing 2 detektor dan selanjutnya melakukan proses aritmatik jika hasil proses mencapai nilai spesifik yang telah ditentukan, sinyal trip akan dikeluarkan. Bagian sirkuit logika menerima sinyal trip dari bagian saluran analog dan melakukan proses aritmatik pada arsitektur 2 keluaran dari 4 jalur (atau 2 keluaran dari 3 jalur) jika lebih dari 2 saluran sirkuit analog mengirimkan trip sinyal, dia akan mengirimkan sinyal trip reaktor pada trip breaker reaktor. Langkah berikutnya meneruskan sinyal pada bagian *mechanism control rod drive (CDRM*). Selanjutnya akan mentrip reaktor[5].



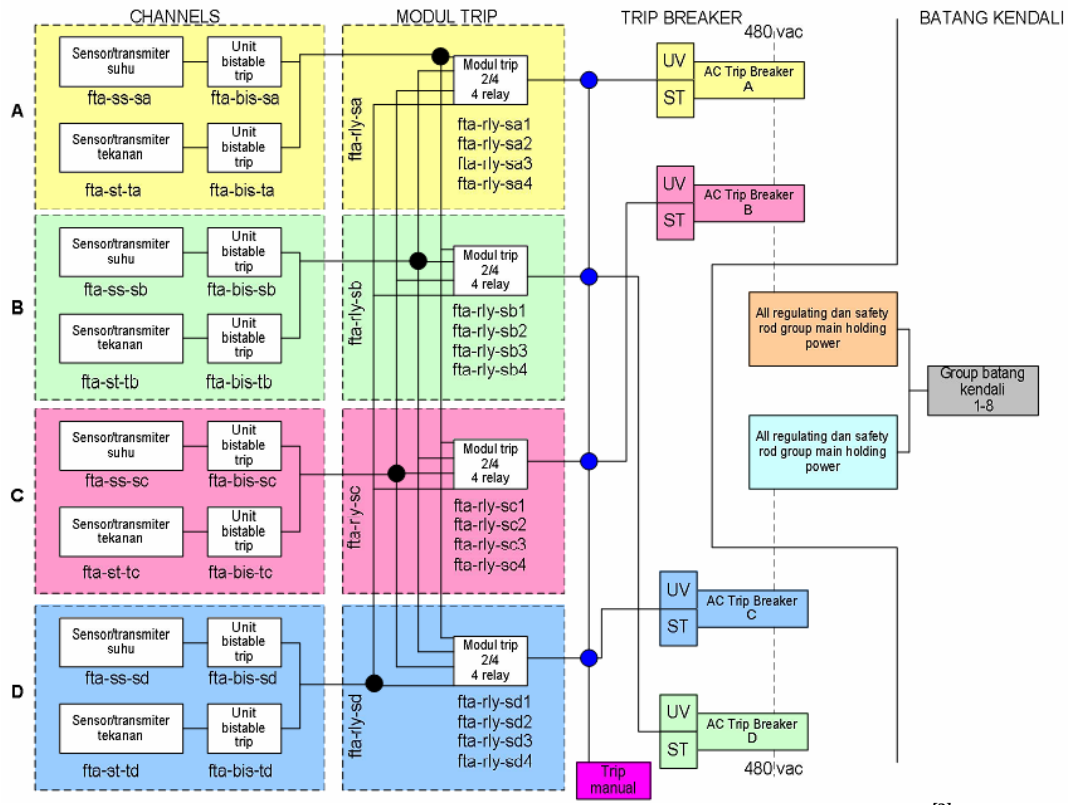
Gambar 1. Sistem Proteksi PWR

3. METODE ANALISIS KESELAMATAN SISTEM PROTEKSI REAKTOR

Metode yang tepat untuk mengkaji keselamatan dan keandalan sistem proteksi reaktor adalah kunci dalam memutuskan apakah desain sistem instrumentasi dan kontrol sistem proteksi reaktor yang dikaji layak dipasang atau tidak pada PLTN. Metode yang digunakan untuk mengkaji keselamatan dan keandalan sistem proteksi reaktor harus efektif dan efesien, harus jelas mampu mendukung dalam menetapkan keandalan sistem proteksi reaktor, metode tersebut dapat melakukan kajian batas keselamatan, hasil dari metode dapat dibandingkan dengan persyaratan keselamatan

 ISSN: 0854 - 2910

yang telah ditetapkan, yang secara nyata metode ini dapat membantu untuk menghindari potensi yang tidak aman atau tidak andal, membantu mengidentifikasi keselamatan, keandalan dan sekaligus meningkatkannya.



Gambar 2. Diagram Sistem Proteksi *PWR Babcock & wilcox Davis Besse*[3]

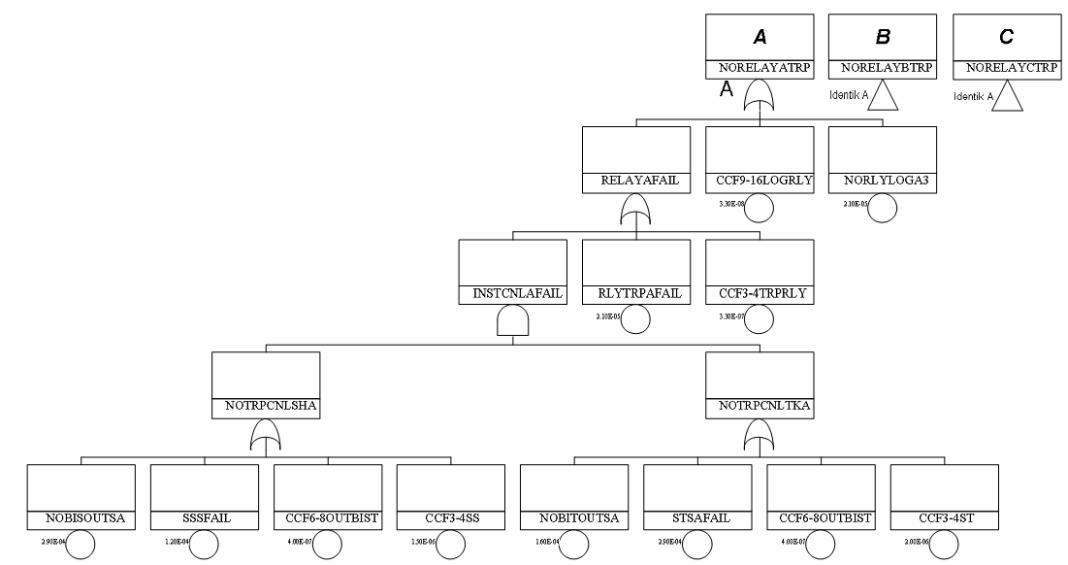
Ada beberapa langkah prosedur dalam pengkajian keselamatan sistem proteksi reaktor, diantaranya yaitu[1]:

- Pemahaman sistem yang akan dikaji
- *Failure Mode and Effect Analysis (FMEA*)
- *quantitative fault tree modeling*
- *failure rate estimation of the hardware components*
- dsb (seperti *analysis critical path, weak point*)

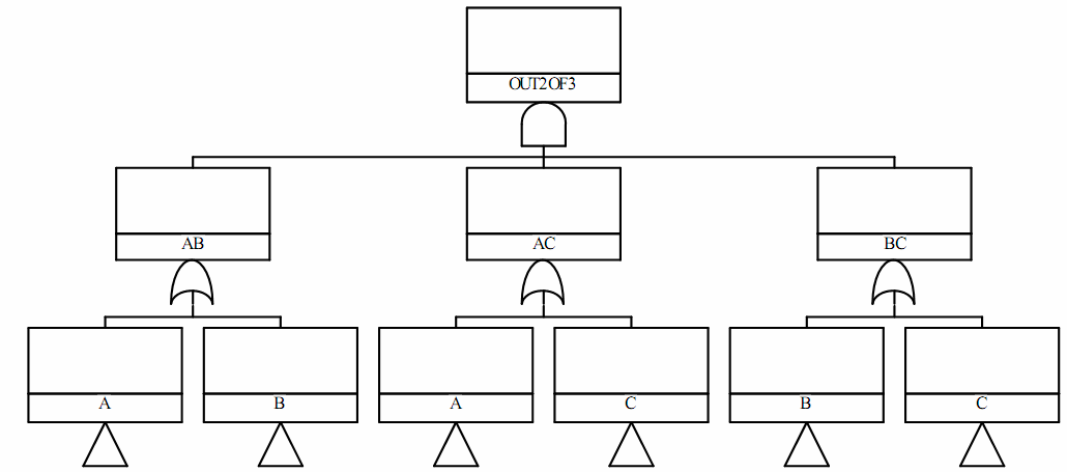
Pada penelitian ini dilakukan analisis kuantitatif pohon kegagalan sistem proteksi PWR *Babcock & Wilcox Davis Besse*[3]. Analisis dimulai dari komponen yang termasuk pada segmen *channel* (saluran) sampai dengan segmen output jalur modul trip (lihat gambar 2), Analisis dilakukan untuk modul trip berjumlah 3 jalur. Analisis keselamatan dan keandalan dengan pemodelan pohon kegagalan yang sesuai dengan sistem dapat memperlihatkan sistem yang benar bagaimana kronologis jika terjadi kecelakaan dan memperlihatkan hasil hitungan probabilitas kejadian akhir merupakan fungsi dari probabilitas kejadian dasar (*basic event*).

4. HASIL ANALISIS DAN PEMBAHASAN

Analisis pohon kegagalan adalah salah satu metode yang banyak dipakai untuk mengkaji keselamatan dan keandalan sistem. Kegagalan suatu sistem keselamatan merupakan kombinasi kegagalan komponen (*basic events*), dalam model analisis pohon kegagalan *basic event* ini dapat terdiri atas *random hardware failures*, *common cause failure (CCF) mechanisms*, kesalahan operator, dll.



Gambar 3. *Cut set* tiap saluran (A, B, C) RPS *Davis Besse* tidak ada sinyal ke bagian trip *breaker*



Gambar 4. Model pohon kegagalan RPS arsitek 2 keluaran dari 3

Basic event merupakan kejadian dalam kajian keselamatan dan keandalan pada analisis pohon kegagalan, kejadian yang jarang terjadi dan dalam penetapan nilainya melibatkan hal hal yang agak rumit dan panjang, yaitu diambil dari data pengalaman kegagalan selama umur operasi dari instalasi yang sama atau dari instalasi yang sejenis lain jika tidak mempunyai data pengalaman operasi (misal diambil dari *handbook* atau generik database standar militer yang berkaitan). Dalam

 ISSN: 0854 - 2910

mendapatkan data komponen beberapa contoh kejadian diambil untuk dipelajari dalam jangka periode yang cukup panjang untuk mendapatkan nilai statistik berarti.

Pada kajian keselamatan disini, digunakan analisis pohon kegagalan yang diterapkan untuk desain bagian depan sistem proteksi reaktor PWR, yaitu dimulai dari segmen saluran (*channel*) sampai dengan inputan untuk segmen *trip breaker (*lihat gambar 2*).* Prosedur analisis pohon kegagalan yang pertama adalah mengidentifikasi komponen kegagalan yang ada pada sistem. Pada segmen saluran (*channel*) terdapat empat *basic event* yaitu CCF sensor/transmiter, CCF keluaran *bistable*, sensor/transmiter gagal dan *output bistable* sensor gagal, masing masing nilai laju kegagalan *basic event* tersebut adalah $1.5e^{-6}$, $4.0e^{-7}$, $1.6e^{-4}$ dan $1.2\ e^{-4}$[3]dengan dua *basic event* relay, yaitu trip relay gagal ($2.1e^{-5}$) dan CCF trip relay($3.3e^{-7}$). Dilain hal pada modul trip terdapat dua *basic event*, logika relay gagal ($2.1e^{-5}$) dan CCF logika relay ($3.3e^{-8}$)[3].

Prosedur analisis pohon kegagalan yang berikutnya adalah merancang pohon kegagalan lihat gambar 3. Untuk merancang sampai Top Event (Tidak ada sinyal/ inputan ke bagian *trip breaker)* perlu dianalisis probabilitas setiap saluran A, B dan C. Dari data laju kegagalan yang diterangkan di atas maka diperoleh *kuantitatif probabilitas cut set* tiap saluran(A, B dan C) adalah $4.295\ e^{-5}$, Selanjutnya untuk memperoleh *kuantitatif porbabilitas top event*, harus dilakukan pemodelan pohon kegagalannya dan analisis probabilitas pohon kegagalan kombinasi arsitek 2 keluaran dari 3. Ada tiga kombinasi jalur yang akan mengagalkan terjadinya *top event* yaitu:

1. jalur A, jalur B, gagal
2. jalur A dan jalur C gagal
3. jalur B, dan jalur C gagal

Ketiga kombinasi digambarkan pada gambar 4. Sesuai desain bahwa tiap saluran independen. Jika dihitung *top event* dari nilai *cut set* yang diperoleh tiap saluran A, B dan C maka diperoleh nilai laju kegagalan untuk RPS arsitektur 2 keluaran dari 3 yaitu sebesar $2.58\ e^{-14}$. Nilai yang signifikan dibandingkan dengan nilai tiap saluran A, B dan C, hal ini membuktikan bahwa begitu berartinya desain redudansi pada RPS.

Pada analisis ini kajian keselamatan dan keandalan sistem proteksi reaktor dengan memanfaatkan analisis probabilitas pohon kegagalan cukup memberikan bukti bahwa sistem proteksi harus dirancang redudansi, mandiri dan bekerja tuntas setelah menerima sinyal perintah.

5. KESIMPULAN

Telah dilakukan analisis keselamatan dan keandalan sistem proteksi reaktor PWR dengan memanfaatkan metode analisis probabilitas pohon kegagalan dan memanfaatkan data pada sistem proteksi reaktor *Babcock & Wilcox Davis Besse.* Hasil analisis menunjukan nilai kuantitatif, yang membuktikan bahwa desain redundansi arsitektur 2 keluaran dari 3 mengurangi probabilitas kegagalan secara signifikan dibandingkan satu jalur.

6. DAFTAR PUSTAKA

[1]. Board on Energy and Environmental System Commision on Engineering and Technical System National Research Counci*l*, "Digital Instrumentation and Control System in Nuclear Power Plants", National Academy Press, Washington, DC 1997.

[2]. Kee Choon Kwon, Myeongsoo Lee, "Technical Review on The Localized Digital Instrumentation and Control Systems", Nuclear Engineering and Technology, vol 41 No 4 May 2009.

[3]. T. E. Wierman, S. T. Beck,M. B. Calley, S. A. Eide,C. D. Gentillon, W. E. Kohn, "Babcock&Wilcox Reactor Protection System 1984-1998", NUREG/CR-5500, Volume 11, November 2001

[4]. Japan Nuclear Energy Safety Organization (JNES), "Outline of Safety Design (case of PWR)", Long-term Training Course on Safety Regulation and Safety Analysis / Inspection2005

[5]. Dong-Young Lee, Jong-Gyun Choi, and Joon Lyou, "A Safety Assessment Methodology for a Digital ReactorProtection System", International Journal of Control, Automation, and Systems, vol. 4, no. 1, pp. 105-112, February 2006

DISKUSI/TANYA-JAWAB:

1. PERTANYAAN: (Masani, FMIPA-UNY)

- Apakah dengan analisa ini pengoperasian reaktor akan aman 100%?

JAWABAN: (Djen Djen Djainal, PTRKN-BATAN)

- *Analisa ini mengevaluasi desain reaktor pada bagian sistem proteksi kendalinya. Membandingkan tingkat keselamatan sistem proteksi reaktor ketika memanfaatkan sistem redudansi dan ketika tidak menggunakan sistem redudansi dan hasilnya sistem proteksi dengan menggunakan sistem redudansi itu tingkat keselamatannya lebih tinggi.*