

EVALUASI KESELAMATAN TERAS REAKTOR PWR BERDASARKAN KEJADIAN PEMICU DAN ASPEK DESAIN

D. T. Sony Tjahyani

Bidang Pengkajian dan Analisis Keselamatan Reaktor
Pusat Teknologi Reaktor dan Keselamatan Nuklir-BATAN
sonybatan@yahoo.com

ABSTRAK

EVALUASI KESELAMATAN TERAS REAKTOR PWR BERDASARKAN KEJADIAN PEMICU DAN ASPEK DESAIN. Evaluasi keselamatan PLTN yang penting dilakukan adalah menentukan frekuensi dan konsekuensi lepasan produk fisi ke masyarakat dan lingkungan. Kondisi tersebut disebabkan oleh kerusakan teras dan kegagalan sistem pengungkung. Kerusakan teras disebabkan kejadian pemicu dan kegagalan sistem keselamatan yang ada pada desain. Kegagalan sistem keselamatan tergantung dari atas 6 hal yaitu: kriteria gagal tunggal, redundansi, kemandirian, keragaman, konsep gagal-aman, interaksi sistem dan ketergantungan. Tujuan evaluasi ini untuk menentukan item tersebut yang berpengaruh terhadap kegagalan sistem serta kejadian pemicu yang berpengaruh terhadap kerusakan teras. Sebagai obyek kajian dilakukan pada PWR generasi II dan generasi III (III⁺). Analisis dilakukan dengan mengumpulkan data kejadian pemicu dan frekuensi kerusakan teras serta mengkaji konfigurasi desain untuk PWR generasi II dan III (III⁺). Dari hasil evaluasi ini menunjukkan modifikasi sistem terhadap PWR generasi II mempunyai pengaruh yang signifikan terhadap tingkat keselamatan teras PWR generasi III (III⁺), sehingga menurunkan terhadap frekuensi kejadian pemicu dan kerusakan teras.

Kata kunci: PWR, Kerusakan Teras, Kejadian Pemicu, PWR generasi II dan III (III⁺).

ABSTRACT

SAFETY EVALUATION OF REACTOR CORE FOR PWR BASED ON INITIATING EVENT AND DESIGN ASPECT. Safety evaluation for NPP is important to determine frequency and consequence of fission product released to public and environmental. Those condition is caused by core damage and containment system failure. Core damage is caused initiating events and safety system failure. Safety system failure is dependent by 6 items that is single failure criteria, redundancy, independency, diversity, fail-safe concept, system interaction and dependencies. The objective of the evaluation is to determine those items to system failure and initiating events contribution to core damage. PWR for generation II and III (III⁺) are used as object of study for this assessment. The analysis was carried out by collecting initiating event and core damage data also to assess design configuration of PWR for generation II and III (III⁺). The evaluation results showed that system modification of generation II is significant to core safety level for generation III (III⁺) PWR, so it is to reduce initiating events and core damage frequency.

Keywords: PWR, Core Damage, Initiating Event, PWR for Generation II and III (III⁺).

1. PENDAHULUAN

Sebagai salah satu hal penting didalam evaluasi keselamatan PLTN adalah menentukan frekuensi dan konsekuensi lepasan produk fisi ke masyarakat dan lingkungan. Secara analisis deduksi, kedua kondisi tersebut disebabkan oleh 2 hal yang terjadi bersamaan yaitu terjadi kerusakan teras dan sistem pengungkung (*Containment*

System) gagal. Kerusakan teras diakibatkan oleh kecelakaan dasar desain (*design basis accident*). Hal ini dipengaruhi oleh sistem keselamatan, maka dari itu tergantung dari desain untuk setiap jenis PLTN.

Perubahan desain PLTN pada saat ini dilakukan dengan berdasarkan 4 pendekatan yaitu: pengurangan kesalahan manusia dengan memperbaiki antar-muka manusia-mesin serta

kendali dan instrumentasi digital, meningkatkan keandalan sistem keselamatan pasif dan aktif, pengurangan frekuensi kerusakan teras (CDF), serta menjamin lepasan yang sangat rendah pada saat kondisi kecelakaan parah.

Analisis kerusakan teras dapat dilakukan secara deterministik dan probabilitistik. Dalam hubungannya menentukan frekuensi, maka secara probabilitistik dipengaruhi oleh 2 hal yaitu kejadian pemicu (*initiating event*) dan sistem keselamatan yang memitigasi dari kejadian pemicu tersebut [1,2]. Kedua hal tersebut tergantung dari keandalan sistem yang dipengaruhi oleh 6 item yaitu: kriteria gagal tunggal (*single failure criterion*), redundansi, kemandirian (*independence*), keragaman (*diversity*), konsep gagal-aman (*fail-safe*), interaksi sistem dan ketergantungan [3].

Dalam PSA (*Probabilistic Safety Assessment*), frekuensi kerusakan teras ditentukan berdasarkan jumlah dari frekuensi setiap sekuensi kecelakaan yaitu perkalian frekuensi setiap kejadian pemicu dengan kombinasi probabilitas gagal atau sukses sistem keselamatan/tindakan mitigasi. Kegagalan sistem keselamatan merupakan kombinasi kegagalan komponen (*minimal cutset*), sehingga dapat dilakukan pendekatan bahwa kerusakan teras merupakan kombinasi terkecil kegagalan komponen setiap sistem keselamatan/tindakan mitigasi.

Dalam penelitian sebelumnya telah dilakukan analisis desain ECCS terhadap kerusakan teras [4]. Pada makalah ini bertujuan menganalisis desain terhadap kegagalan sistem serta kejadian pemicu yang berpengaruh terhadap kerusakan teras berdasarkan kriteria gagal tunggal, redundansi, kemandirian, keragaman, konsep gagal-aman serta interaksi sistem dan ketergantungan. Sebagai obyek analisis dilakukan pada PWR generasi II dan generasi III (III⁺). Untuk PWR generasi III (III⁺) dipilih jenis PWR berdasarkan sistem aktif dan pasif.

2. KEJADIAN PEMICU DAN ANALISIS SISTEM

Target keselamatan dalam pelaksanaan PSA level 1 adalah menentukan frekuensi kerusakan teras (CDF), maka untuk mendapatkan hal tersebut perlu dilakukan identifikasi rentetan (*sequences*) kejadian yang menimbulkan kerusakan teras. Sebagai nilai frekuensi ditentukan berdasarkan jumlah dari frekuensi setiap rentetan kecelakaan, dimana rentetan kecelakaan merupakan perkalian dari kejadian pemicu dan kombinasi gagal/sukses dari sistem keselamatan, sistem pendukung dan kesalahan manusia. Karena dalam proses analisis tersebut melibatkan tingkat keandalan sistem,

maka hasil analisis tersebut dapat dipergunakan sebagai evaluasi untuk menentukan kekuatan dan kelemahan sistem keselamatan serta prosedur untuk mencegah kerusakan teras.

Berdasarkan frekuensi terjadinya, kejadian pemicu dapat berupa internal dan eksternal dikategorikan sebagai kejadian operasional terantisipasi (*Anticipated Operational Occurrences*) yang sering disebut sebagai transien dan kecelakaan [5]. Sedangkan kecelakaan terbagi atas kecelakaan dasar desain (DBA, *Design Basis Accident*), kecelakaan melampaui dasar desain (BDBA, *Beyond Design Basis Accident*) dan kecelakaan parah. Namun secara prinsip, kejadian pemicu merupakan gangguan pada sistem yang menimbulkan kerusakan teras disebabkan atas: kecelakaan reaktivitas, pengurangan aliran pendingin, bertambah/berkurangnya inventori pada pendingin reaktor, bertambah/berkurangnya pemindah panas pada sisi sekunder, dan transien terantisipasi tanpa scram (ATWS). Frekuensi timbulnya kejadian pemicu serta sukses/gagal sistem keselamatan dipengaruhi oleh keandalan sistem. Keandalan sistem dipengaruhi oleh kriteria gagal tunggal, redundansi, kemandirian (*independence*), keragaman, dan konsep gagal-aman.

Berdasarkan kriteria yang ditetapkan NRC sistem yang bersifat sebagai proteksi harus di desain dengan mempunyai keandalan fungsi yang tinggi dan dapat diuji dengan tetap berfungsi. Redundansi dan kemandirian didesain pada sistem proteksi untuk cukup menjamin bahwa tidak ada kegagalan tunggal yang mengakibatkan hilangnya fungsi sebagai proteksi. Selanjutnya pengalihan fungsi/layanan setiap komponen atau kanal tidak menyebabkan hilangnya redundansi minimum yang dipersyaratkan. Demikian juga sistem yang bersifat sebagai proteksi harus didesain untuk dapat diuji secara periodik ketika reaktor beroperasi, termasuk kemampuan untuk menguji kanal secara mandiri dalam menentukan kegagalan dan hilangnya redundansi yang mungkin terjadi.

Sistem redundansi pada semua komponen kritis ditujukan untuk memenuhi kriteria gagal tunggal, sehingga dapat menurunkan probabilitas kegagalan sistem yang berdampak terhadap perbaikan keandalan. Sebagai redundansi memerlukan jalur tersendiri yang kapasitasnya cukup untuk memenuhi persyaratan fungsi sistem tersebut. Ketentuan yang diperlukan dalam redundansi adalah pengujian periodik secara *on-line* dan dapat memindahkan kanal dari layanan, sehingga untuk memenuhi kriteria tersebut menggunakan minimum 3 jalur (*train*) atau kanal redundan. Untuk mencegah sinyal palsu dalam pengoperasian sistem keselamatan pada umumnya digunakan logika 2/3. Sistem proteksi reaktor pada umumnya digunakan logika 2/3 atau 2/4.

Penerapan kriteria gagal tunggal untuk sistem redundan diimplikasikan pada redundan jalur atau kanal secara fisik mandiri terhadap satu sama lain. Selain itu tidak ada ketergantungan bersama untuk daya listrik dan lingkungan. Hubungan silang (*cross connection*) harus diisolasi untuk mencegah kesalahan di suatu jalur yang dapat menyebabkan kegagalan pada jalur redundan. Hubungan silang dapat menggunakan peralatan isolasi elektrik terkualifikasi, isolator *optical* jenis resistor "NOT". Untuk hubungan silang sistem fluida dapat diisolasi melalui katup cek.

Keandalan redundan dan kemandirian sistem keselamatan dibatasi oleh kegagalan berpenyebab sama (*common cause failure*), maka salah satu metoda untuk menghindari hal tersebut adalah dilakukan dengan menerapkan keragaman (*diversity*). Penambahan redundansi tidak dapat untuk mengatasi kegagalan berpenyebab sama. Kegagalan berpenyebab sama disebabkan antara lain: kesalahan desain atau margin desain yang tidak cukup, cacat dalam manufaktur, kesalahan pengujian, penurunan fungsi akibat lingkungan (misalnya kelembaban, kotor, dan lain-lainnya). Keragaman dapat dicapai melalui penggunaan prinsip pengoperasian yang berbeda secara fisika, penggunaan manufaktur komponen yang berbeda, penggunaan teknik yang berbeda dalam pengujian, perawatan atau pengoperasian peralatan. Maka dari itu dalam desain, redundansi tidak hanya sekedar memberi cadangan tetapi juga harus dipertimbangkan keragamannya. Penerapan dalam desain kendali tidak hanya berdasarkan logika 2/3 atau 2/4, tetapi juga menerapkan jenis sensor yang mengaktuasi, misalnya tekanan dan temperatur.

Konsep gagal-aman memerlukan identifikasi secara sistematis untuk mendapatkan keluaran yang aman dari kegagalan sistem. Substansi dari konsep gagal-aman adalah identifikasi dari kondisi *de-energized* dari sistem atau komponen.

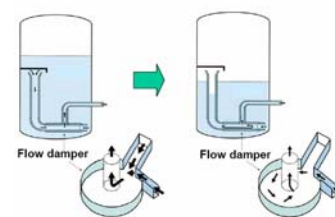
Dalam desain PLTN mempunyai sistem proteksi secara redundansi yang ditunjang dengan sistem pendukung (*support system*) yang redundansi pula. Kegagalan satu jalur dari sistem pendukung akan menimbulkan kejadian transien yang sangat kompleks. Interaksi sistem yang disebabkan gagal tunggal dapat menyebabkan komponen yang signifikan menimbulkan kegagalan secara bersamaan (*simultaneously*). Maka dari itu kesalahan yang dipicu oleh kegagalan sistem pendukung dan interaksi sistem harus dipertimbangkan dalam kajian gagal tunggal, salah satu metoda yang digunakan adalah FMEA (*Failure Mode and Effect Analysis*).

Selain dari aspek ekonomi, perkembangan desain PWR dari generasi II ke generasi III (III⁺) pada umumnya untuk memperbaiki keandalan sistem ECCS serta pertimbangan dalam

memitigasi kecelakaan parah. Sehubungan dengan perkembangan teknologi, ECCS ditujukan untuk implementasi dari konsep *defence in depth* level-3 yaitu mencegah terjadinya kecelakaan dasar desain, antara lain kecelakaan kehilangan pendingin (LOCA) yang sebelumnya diprediksi mempunyai probabilitas yang kecil untuk menimbulkan kerusakan teras (1×10^{-4} /reaktor-tahun). Probabilitas tersebut termasuk kecil, tetapi dapat terjadi seperti pada peristiwa TMI-2 (*Three Miles Islands-2*).

Konsep ECCS pada PWR generasi II terdiri atas 3 subsistem yaitu: akumulator, injeksi tekanan tinggi dan injeksi tekanan rendah. Akumulator merupakan suatu tangki berisi air borat dan ditekan oleh gas nitrogen serta terhubung dengan sistem primer melalui sebuah katup yang beroperasi secara pasif. Bila terjadi kecelakaan yang termasuk klasifikasi kecelakaan dasar desain, maka tekanan akan turun (sekitar 40 bar), sehingga katup akan membuka secara otomatis dan air diinjeksikan ke dalam teras (sistem primer). Injeksi tekanan tinggi mempunyai fungsi yang hampir sama, tetapi bekerja pada saat tekanan di dalam reaktor masih tinggi (sekitar 100 bar) dan membutuhkan pompa. Demikian juga dengan injeksi tekanan rendah mempunyai fungsi yang hampir sama, tetapi bekerja pada saat tekanan rendah (sekitar 30 bar). Sumber pendingin dari injeksi tekanan tinggi dan rendah berasal dari RWST (*Refueling Water Storage Tank*) yang berada di luar pengungkung.

Desain ECCS untuk generasi III (III⁺) seperti AP-1000 (*Advanced Passive-1000*), US-APWR (*US-Advanced Pressurized Water Reactor*) dan US-EPR (*US-Evolutionary Pressurized Reactor*) mengembangkan teknologi ECCS tersebut, baik secara prinsip kerja, konfigurasi maupun sistem kendali. Ke-3 tipe tersebut saat ini sedang dalam tahap konstruksi pada beberapa negara.



Gambar 1. Proses akumulator dan injeksi tekanan rendah pada US-APWR [6]

Pada AP-1000 juga terdiri atas 3 subsistem yaitu akumulator, CMT (*core make-up tank*) dan IRWST (*in-containment refueling water storage tank*) yang mempunyai fungsi seperti halnya ECCS pada generasi II, tetapi menggunakan sistem pasif.

ECCS untuk US-APWR dan US-EPR tetap didominasi berdasarkan sistem aktif tetapi mengalami penggabungan fungsi. Pada US-APWR fungsi injeksi tekanan rendah digabung dengan akumulator. Sedangkan injeksi tekanan tinggi pada US-EPR dihilangkan, serta diganti dengan injeksi tekanan menengah.

Pada US-APWR akumulator dapat digabung dengan injeksi tekanan rendah karena menggunakan prinsip pada saat berfungsi sebagai akumulator dapat menginjeksikan dari 2 lokasi, sehingga mempunyai kecepatan yang sangat tinggi, karena semakin lama level air dalam tangki turun, maka injeksi hanya berasal dari satu lokasi dan berfungsi sebagai injeksi tekanan rendah seperti ditunjukkan dalam Gambar 1. Perbedaan lain yang menyolok dibandingkan dengan generasi II adalah RWST pada semua generasi III (III⁺) terletak di dalam pengungkuh. Perbedaan lainnya, walaupun sebenarnya sistem ECCS pada US-APWR dan US-EPR merupakan kombinasi dari sistem pasif dan aktif, namun yang lebih dominan adalah sistem aktif.

Dalam sistem suplai daya untuk US-EPR bila dibandingkan dengan PWR generasi II, setiap jalur ECCS disuplai daya normal dan 1 buah disel darurat. Apabila sumber daya tersebut juga gagal (untuk 4 jalur), maka masih tersedia 2 buah disel darurat. Sedangkan pada US-APWR suplai daya darurat berdasarkan prinsip 2 out of 4, dengan menggunakan *gas turbine generator*.

3. METODE

Analisis dilakukan dengan pengumpulan data kejadian pemicu dan CDF untuk PWR generasi II dan III (III⁺) serta rekayasa teknik keandalan yang diterapkan dalam masing-masing desain. Untuk mengkaji besarnya kontribusi setiap item terhadap keselamatan dilakukan dengan membuat analisis pohon kegagalan generik dan diagram blok keandalan, dengan menggunakan program SAPHIRE ver. 6.76 [7]. Demikian juga karena tujuan utama adalah kontribusinya terhadap frekuensi kerusakan teras, maka item yang ditinjau adalah hal yang berhubungan dengan ECCS dan sistem kendali yang berfungsi sebagai aktuasi sistem.

4. HASIL DAN PEMBAHASAN

Untuk mengevaluasi keandalan secara menyeluruh sangat sulit dilakukan karena harus memerlukan data yang lengkap untuk setiap tipe PWR, yang hal ini sulit didapatkan. Namun beberapa item dapat dilakukan untuk mewakili kondisi desain. Berdasarkan perkembangan desain

karena menggunakan sistem pasif pada AP-1000 maka dilakukan pengurangan beberapa komponen antara lain: 50% katup keselamatan, pompa 35%, pipa keselamatan 80 %, jumlah kabel berkurang sampai dengan 70% [8]. Maka jika dihitung ulang secara diagram blok keandalan, desain tersebut jika dibandingkan dengan PWR generasi ke II secara rata-rata akan mengurangi kejadian pemicu kecelakaan kehilangan pendingin sehingga frekuensi kerusakan teras menjadi sekitar $2,75 \times 10^{-6}$ per tahun, demikian juga yang disebabkan oleh transien menjadi $5,25 \times 10^{-5}$ per tahun.

Dari perhitungan secara keandalan berdasarkan konfigurasi untuk redundansi sistem, antara PWR generasi II dan generasi III (III⁺) telah mengalami perubahan yang signifikan. Bila dibandingkan dengan PWR generasi II berdasarkan aspek redundansi, maka AP-1000 mempunyai tingkatan yang sama, tetapi dengan berdasarkan prinsip sistem pasif maka perhitungan keandalannya menjadi tinggi (probabilitas gagal menurun). Bila dibandingkan dengan tipe US-APWR, maka mempunyai probabilitas gagal 0,33 dari probabilitas gagal generasi II, sedangkan untuk US-EPR mempunyai probabilitas 0,5 kalinya. Namun bila diasumsikan 1 jalur (*train*) kehilangan fungsi, maka US-APWR menjadi 3 kombinasi sistem sukses sehingga probabilitas gagalnya menjadi 0,66 kalinya terhadap probabilitas gagal generasi II, dan hal ini sama dengan US-EPR apabila kehilangan fungsi untuk 1 jalur. Namun bila diasumsikan 2 jalur gagal, maka pada US-APWR akan mempunyai probabilitas gagal yang lebih besar dari generasi II, walaupun hal ini kecil kemungkinannya terjadi untuk 2 jalur gagal. Sebaliknya pada US-EPR bila 2 jalur tidak berfungsi, masih mempunyai 2 kombinasi sukses, sehingga bila dibandingkan dengan PWR generasi II mempunyai probabilitas gagal yang sama. Maka dari itu bila disusun atas dasar kelonggaran dilakukan uji atau perawatan pada saat reaktor beroperasi, US-EPR mempunyai rentang yang lebih lebar, diikuti dengan US-APWR.

Untuk desain sistem listrik yang mensuplai sistem keselamatan dalam mencegah kerusakan teras mempunyai tingkat keandalan yang sama antara US-EPR dan US-APWR, berdasarkan perhitungan diagram blok didapatkan probabilitas gagal 0,17. Tetapi pada US-APWR mempunyai tingkat keragaman yang lebih yaitu digunakannya *gas turbine generator*, hal ini mempunyai keunggulan dalam menghadapi kegagalan berpenyebab sama.

Di antara tipe PWR yang dikaji, maka US-EPR mempunyai tingkatan kriteria gagal tunggal yang lebih tinggi, karena konfigurasi sistemnya menggunakan *1 out of 4* atau N+2, sehingga cukup mempunyai redundansi untuk perawatan dan uji.

Prinsip gagal-aman sudah diterapkan pada pengaturan batang kendali untuk semua tipe PWR. Namun untuk pengaturan katup keselamatan, pada AP-1000 banyak menggunakan prinsip ini, misalnya: katup dengan prinsip *Normal Closed* dengan daya aktuasi menggunakan baterai, *spring* atau gas terkompresi.

Sistem ECCS pada PWR generasi II dan AP-1000 berdasarkan *1 out of 2*, sedangkan pada US-APWR berdasarkan *2 out of 4* dan US-EPR berdasarkan *1 out of 4*.

Hal yang juga sangat signifikan dipertimbangkan dalam desain dibandingkan dengan PWR generasi II adalah mengenai kecelakaan parah. Pada seluruh tipe PWR generasi III (III⁺) memberikan suatu ruangan untuk mengantisipasi terjadinya kecelakaan parah (bejana reaktor gagal), dimana hal ini tidak dilakukan pada PWR generasi II.

Dari pengumpulan data mengenai kejadian pemicu dan frekuensi kerusakan teras[9-13], selanjutnya dihitung ulang untuk dilakukan pengelompokkan data agar dapat dibandingkan maka didapatkan kontribusi kejadian pemicu untuk PWR generasi II dan generasi III (III⁺) seperti ditunjukkan dalam Tabel 1, pengelompokkan dilakukan karena setiap tipe mempunyai beberapa kejadian pemicu yang khusus. Dari tabel terlihat bahwa frekuensi kerusakan teras mengalami penurunan yang signifikan pada PWR generasi III (III⁺) karena terjadinya perubahan desain, baik secara redundansi, keragaman maupun kemandirian.

Dari tabel terlihat bahwa kejadian pemicu SBO (*Station Black Out*) baik untuk PWR generasi II maupun generasi III (III⁺) tipe aktif merupakan

kontribusi terbesar menyebabkan kerusakan teras, namun pada generasi III (III⁺) semakin mengecil, hal ini disebabkan penggunaan redundansi dan keragaman. SBO pada AP-1000 terlihat kecil, hal ini disebabkan penggunaan sistem dari 2 subsistem ECCS berdasarkan sistem pasif. Berdasarkan kajian juga terlihat kenaikan keandalan tidak hanya pada sistem utama, tetapi juga pada sistem pendukung, hal ini terlihat pada kejadian pemicu transien yang semakin menurun kontribusinya terhadap kerusakan teras.

Dalam analisis/kajian keandalan desain tidak hanya berdasarkan redundansi, tetapi harus dilihat keragamannya dan kemandiriannya karena ke-3 hal tersebut saling berpengaruh hal ini terlihat dalam desain yang ada di AP-1000, US-APWR dan US-EPR.

Dalam tabel tersebut juga menunjukkan bahwa PWR kejadian pemicu yang menimbulkan kerusakan teras semakin kecil probabilitasnya, namun tetap dipersiapkan tindakan atau sistem mitigasi yang mengarah terjadinya kecelakaan parah. Hal ini berbeda sekali dengan desain yang ada pada PWR generasi II.

Berdasarkan analisis tersebut terlihat bahwa kejadian pemicu dan frekuensi kerusakan teras generasi III (III⁺) menunjukkan tingkat keselamatan yang semakin tinggi (angka probabilitas terjadi yang kecil) dibandingkan generasi II. Maka dalam persiapan untuk pembangunan PLTN pertama jenis PWR di Indonesia, kajian keselamatan ataupun persyaratan keselamatan yang diminta oleh pengguna (*owner*) sebanyak mungkin parameternya harus mengacu pada PWR generasi III (III⁺).

Tabel 1. Kontribusi Kejadian Pemicu Terhadap Frekuensi Kerusakan Teras

Kejadian Pemicu	Frekuensi Kerusakan Teras, per tahun						
	Surry	Sequoyah	NUREG-1560 (Rata-rata)	Daya Bay	AP-1000	US-EPR	US-APWR
SBO	$2,7 \times 10^{-5}$	$1,46 \times 10^{-5}$	$3,50 \times 10^{-5}$	$4,84 \times 10^{-6}$	$1,00 \times 10^{-9}$	$1,5 \times 10^{-7}$	$5,80 \times 10^{-7}$
ATWS	$1,6 \times 10^{-6}$	$1,90 \times 10^{-6}$	$2,00 \times 10^{-5}$	$9,74 \times 10^{-7}$	$5,00 \times 10^{-9}$	1×10^{-8}	$1,40 \times 10^{-8}$
Transient	$2,0 \times 10^{-6}$	$2,60 \times 10^{-6}$	$1,50 \times 10^{-4}$	$2,67 \times 10^{-6}$	$8,00 \times 10^{-9}$	$5,98 \times 10^{-8}$	$3,61 \times 10^{-7}$
LOCA	$6,0 \times 10^{-6}$	$3,60 \times 10^{-5}$	$4,05 \times 10^{-5}$	$7,03 \times 10^{-6}$	$2,11 \times 10^{-7}$	$5,1 \times 10^{-8}$	$9,53 \times 10^{-8}$
Interfacing LOCA	$1,6 \times 10^{-6}$	$6,50 \times 10^{-7}$	$4,00 \times 10^{-6}$	$2,78 \times 10^{-6}$	$5,00 \times 10^{-11}$	$1,69 \times 10^{-8}$	$1,94 \times 10^{-8}$
SGTR	$1,8 \times 10^{-6}$	$1,70 \times 10^{-6}$	$1,50 \times 10^{-5}$	$2,81 \times 10^{-6}$	$7,00 \times 10^{-9}$	$1,3 \times 10^{-8}$	$6,70 \times 10^{-9}$
Vessel Rupture	-	-	$1,00 \times 10^{-7}$	$2,4 \times 10^{-7}$	$1,00 \times 10^{-8}$	-	$1,00 \times 10^{-7}$
Total	$4,0 \times 10^{-5}$	$5,75 \times 10^{-5}$	$2,65 \times 10^{-4}$	$2,13 \times 10^{-5}$	$2,42 \times 10^{-7}$	$3,01 \times 10^{-7}$	$1,18 \times 10^{-6}$

Sedikit kendala yang dihadapi adalah ketentuan dalam pasal 4 PP no. 43 tahun 2006 [14] bahwa PLTN yang dibangun di Indonesia adalah harus teknologi teruji (pengalaman operasi 3 tahun dan faktor kapasitas rerata 75%). Memang pada saat ini belum ada reaktor generasi III (III⁺) yang mempunyai pengalaman operasi 3 tahun. Tetapi dengan mengacu pada negara lain yang sudah mulai konstruksi untuk PWR generasi III (III⁺) pada saat ini, serta lamanya konstruksi sekitar 5 tahun. Dihubungkan juga dengan proses perizinan pada badan regulasi (izin tapak 1 tahun dan izin konstruksi 2 tahun), maka seharusnya pada saat Indonesia mengoperasikan PLTN pertamanya, pengalaman operasi dari PWR generasi III (III⁺) sudah mencapai 3 tahun sehingga sudah memenuhi kriteria yang tertuang dalam PP no. 43 tahun 2006. Maka dari itu harus sudah dipertimbangkan mulai saat ini untuk mempersiapkan mengenai hal-hal yang berhubungan dengan spesifikasi teknis PWR generasi III (III⁺), misalnya laporan analisis keselamatan dan URD (*User Requirement Document*).

5. KESIMPULAN

Dalam evaluasi ini disimpulkan bahwa perubahan rekayasa teknik keandalan atau modifikasi sistem terhadap PWR generasi II mempunyai pengaruh yang signifikan terhadap tingkat keselamatan teras PWR generasi III (III⁺), sehingga menurunkan frekuensi kejadian pemicu dan kerusakan teras.

6. DAFTAR PUSTAKA

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Applications of Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, TECDOC 1200, IAEA, 2001.
2. INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plant, DS-394, IAEA, 2007.
3. UNITED STATE NUCLEAR REGULATORY COMMISSION, General Design Criteria for Nuclear Power Plants, 10CFR50: Appendix A.
4. D. T. Sony Tjahyani, Analisis Desain ECCS Terhadap Frekuensi Kerusakan Teras Pada PWR, Laporan Teknis PTRKN-BATAN, 2009.
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants with Pressurized Water Reactors, SS-30, IAEA, 2003.
6. -----, US-APWR Overview, Mitsubishi, 2007.
7. -----, Sapphire Technical Reference Manual, Idaho National Engineering Laboratory, 2002.
8. SHIGENORI SHIGA, AP1000 and Other Reactors Dveloped By Toshiba and Westinghouse, Toshiba, 2007.
9. UNITED STATE NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, NUREG 1150, 1990.
10. UNITED STATE NUCLEAR REGULATORY COMMISSION, Individual Plant Examination Program: Perspective On Reactor Safety and Performance, NUREG 1560, 1996.
11. -----, The Westinghouse AP1000 Advanced Nuclear Power Plant: Plant Description, Westinghouse, 2003.
12. -----, Chapter 19: PRA and Severe Accident, US EPR Final Safety Analysis Report,
13. -----, Chapter 19: Probabilistic Risk Assessment and Severe Accident Evaluation, Design Control Document for the US-APWR, MHI, 2007.
14. -----, Perizinan Reaktor Nuklir, Peraturan Pemerintah No.43 Tahun 2006.

TANYA JAWAB