EVALUASI DESAIN REAKTOR DAYA GENERASI III$^+$ BERDASARKAN KEJADIAN FUKUSHIMA

D. T. Sony Tjahyani
Pusat Teknologi Reaktor dan Keselamatan Nuklir (PTRKN) - BATAN
Kawasan PUSPIPTEK Gd. No. 80 Serpong, Tangerang Selatan 15310
e-mail: sonybatan@yahoo.com

ABSTRAK

EVALUASI DESAIN REAKTOR DAYA GENERASI III$^+$ BERDASARKAN KEJADIAN FUKUSHIMA. Peristiwa Fukushima merupakan kecelakaan parah yang diawali dengan kejadian eksternal secara berturut-turut yaitu gempa dan tsunami sehingga menimbulkan kehilangan daya listrik eksternal dan dilanjutkan dengan Station Blackout (SBO). Reaktor daya yang mengalami kecelakaan di Fukushima merupakan reaktor daya generasi II. Saat ini yang sedang dibangun di dunia adalah termasuk generasi III$^+$, maka sangat penting untuk mengevaluasi kejadian yang sama terhadap reaktor daya generasi III$^+$. Makalah ini menentukan beberapa titik lemah fungsi sistem yang terjadi pada peristiwa di Fukushima, selanjutnya dibandingkan hal tersebut pada desain reaktor daya generasi III$^+$, terutama sebelum terjadinya kerusakan teras. Evaluasi dilakukan dengan analisis pohon kejadian pada peristiwa Fukushima, selanjutnya dibandingkan pada desain reaktor daya generasi III$^+$ serta data kontribusi SBO terhadap frekuensi kerusakan teras. Dari evaluasi menunjukkan terdapat 4 (empat) faktor penyebab kecelakaan yaitu: kehilangan suplai daya listrik offsite, tidak berfungsinya genset karena tsunami, tidak berfungsinya pemindah panas sisa (RHR), dan hilangnya buangan panas akhir (UHS). Hasil evaluasi juga menunjukkan bahwa terjadinya kehilangan suplai daya listrik offsite yang memicu terjadinya kecelakaan parah seperti halnya peristiwa Fukushima sangat kecil probabilitasnya, hal ini karena pada desain sudah mengalami perbaikan dan peningkata sistem keselamatan bila dibandingkan dengan reaktor daya generasi II. Selain itu juga dilakukan penerapan secara ketat terhadap redundansi, keragaman, kemandirian, pemisahan secara fisik serta pemilihan tata letak.

Kata kunci: Reaktor daya generasi III$^+$, Fukushima, SBO.

ABSTRACT

DESIGN EVALUATION FOR GENERATION III$^+$ POWER REACTOR BASED ON FUKUSHIMA INCIDENT. *Fukushima incident is severe accident which is initiated external event respectively. It is earthquake and tsunami, so loss of external power supply is occurred and be continued with Station Black out (SBO). Power reactor which has been accident at Fukushima is generation II power reactor. In the present, reactors are being built in the world are generation III$^+$ power reactor, so it is important to evaluate similar event against generation III$^+$ power reactor. This paper is to determine some weak points of function system at fukushima incident, and further it is compared with design of generation III$^+$, especially before core damage occcured. Evaluation has been done by event tree analysis (ETA) for fukushima incident, and then it is compared on generation III power reactor design and SBO contribution data to core damage frequency. The evaluation results showed that there are 4 weaks point cause of the accident. That is loss of power offsite, no function diesel generator caused by tsunami, no function residual heat removal (RHR) and loss of ultimate heat sink (UHS). And further, evaluation results showed that loss of power offsite and it initiate severe accident as Fukushima incident is small probability because of design improvement and enhancement for safety system if compared with generation II power reactor. Moreover, It done the application of redundancy, diversity, independent, physical separation and layout selection with robustness.*

Keywords: *Generation III$^+$ power reactor, Fukushima, SBO.*

1. PENDAHULUAN

Reaktor daya (Pembangkit Listrik Tenaga Nuklir, PLTN) didesain dengan berdasarkan 3 (tiga) prinsip yaitu mampu dipadamkan dengan aman (*safe shutdown*), didinginkan serta mengungkung produk fisi apabila terjadi lepasan dari teras reaktor. Dalam kaitannya dengan mendinginkan, reaktor didesain mampu memindahkan panas dari teras baik hasil fisi secara langsung maupun dari panas peluruhan (*decay heat*). Sehubungan dengan hal tersebut maka pada reaktor daya perlu disediakan beberapa sistem pendingin baik pendingin pada saat beroperasi, transien, kecelakaan maupun kondisi padam (*shutdown*). Desain dari sistem tersebut beroperasi berdasarkan secara pasif maupun aktif yaitu secara sirkulasi alam atau memerlukan gaya penggerak (*driving force*) dari luar (listrik).

Berdasarkan fenomena yang terjadi dalam teras reaktor, walaupun reaktor sudah padam namun panas peluruhan masih mempunyai panas sekitar ≈ 6–7% dari daya nominal (termal), sehingga apabila panas tersebut tidak mampu dipindahkan atau sistem pendingin yang mempunyai fungsi untuk memindahkan mengalami kegagalan, maka akan menimbulkan kecelakaan dasar desain bahkan sampai kecelakaan parah (*severe accident*).

Reaktor daya didesain dengan mempertimbangkan kejadian awal terpostulasi (*Postulated Initiating Event*, PIE) yaitu baik kejadian internal maupun bahaya yang diterapkan pada desain yang menimbulkan kejadian operasional terantisipasi atau kecelakaan dan ancaman terhadap fungsi keselamatan[1,2]. Kejadian internal disebabkan kegagalan komponen dan kesalahan operator, sedangkan bahaya terdiri atas bahaya internal dan eksternal. Bahaya internal berasal dari dalam tapak reaktor, baik di dalam maupun di luar instalasi, sedangkan bahaya eksternal berasal luar tapak[3]. Beberapa jenis bahaya eksternal yang dipertimbangkan adalah gempa, banjir, kebakaran, kejadian ulah manusia (*human induced*), dan lain-lainya. Masing-masing PIE tersebut maupun kombinasinya apabila tidak dilakukan mitigasi oleh sistem keselamatan dan tindakan operator akan menimbulkan kecelakaan dasar desain bahkan sampai kecelakaan parah. Hal ini seperti yang terjadi pada peristiwa di Fukushima.

Pada makalah ini bertujuan menentukan beberapa titik lemah fungsi sistem yang terjadi pada peristiwa di Fukushima, selanjutnya dibandingkan hal tersebut pada desain reaktor daya generasi III$^+$. Analisis dibatasi hanya sampai pada kecelakaan dasar desain (teras meleleh). Reaktor daya generasi III$^+$ yang digunakan sebagai obyek analisis adalah PWR jenis pasif dan aktif, BWR serta PHWR. Metoda yang dilakukan dengan menganalisis rentetan kejadian (*event sequence*) peristiwa Fukushima sebelum teras meleleh untuk menentukan titik lemahnya, selanjutnya dibandingkan dengan sistem yang ada di reaktor daya generasi III$^+$.

2. PERSYARATAN KESELAMATAN, PERISTIWA FUKUSHIMA DAN REAKTOR DAYA GENERASI III$^+$

2.1. Persyaratan Keselamatan Desain

Tujuan utama desain sistem pendingin reaktor dan penunjangnya adalah menjamin kecukupan aliran dan kualitas pendingin untuk memindahkan panas dari teras berdasarkan semua

kondisi operasi serta saat dan sesudah kecelakaan dasar desain[4]. Selanjutnya sistem tersebut juga digunakan untuk memitigasi konsekuensi kecelakaan dasar desain dan kecelakaan parah.

Untuk mencapai tujuan tersebut, maka sistem pendingin mempunyai kegunaan atau tujuan sebagai berikut:

- Memberikan dan mempertahankan inventori pendingin reaktor yang memadai untuk pendinginan teras pada semua kondisi operasi dan kecelakaan dasar desain dan untuk memindahkan panas yang dibangkitkan buangan panas akhir (*ultimate heat sink*);
- Mempertahankan aliran pendingin yang memadai untuk menjamin kriteria batas desain bahan bakar;
- Mencegah hilangnya inventori yang tak terkendali pada batas tekanan pendingin reaktor (*reactor coolant pressure boundary*).

Sistem pendingin dan pendukungnya terdiri atas sistem pendingin utama, sistem penghubung (*connected*) dan *associated system*. Sistem pendingin utama meliputi komponen yang diperlukan untuk menjamin kesempurnaan aliran pendingin reaktor, tetapi diluar elemen bahan bakar dan elemen kendali reaktivitas. Sistem penghubung adalah sistem yang dihubungkan secara langsung ke sistem pendingin utama atau untuk tipe reaktor jenis PWR ke sisi sekunder pembangkit uap. Bersama dengan komponen dan sistem lainnya, berfungsi untuk menjamin integritas pendingin utama pada kondisi normal, mengantisipasi transien atau kecelakaan dasar desain. Termasuk kelompok sistem ini antara lain: sistem fluida kendali reaktivitas, sistem pendingin teras darurat (*Emergency Core Cooling System,* ECCS), sistem pemindah panas sisa (*Residual Heat Removal System,* RHR), dan lain-lainnya. *Associated system* adalah sistem yang diperlukan sistem pendingin utama dan sistem penghubung yang terutama memindahkan panas ke pembuang panas terakhir (*Ultimate Heat Sink,* UHS). UHS pada umumnya berupa air atau udara yang sebagian besar atau seluruh panas sisa dipindahkan pada saat kondisi normal, kejadian operasional terantisipasi dan kecelakaan. Bila air digunakan sebagai media pembuangan panas terakhir, maka yang perlu dipertimbangkan adalah: kapasitas suplai air, jenis suplai air pendingin (misalnya laut, danau, sungai atau penampungan buatan manusia/alami), sumber *make-up* menuju UHS, kemampuan buangan panas untuk menampung aliran air pendingin pada temperatur kondisi reaktor padam, operasi, dan kecelakaan.

Desain sistem pendingin reaktor dan pendukungnya yang berfungsi sebagai sistem keselamatan harus mempunyai kriteria sebagai berikut: kapasitas cukup, tidak ada gagal tunggal, suplai listrik pada kondisi normal dan darurat, proteksi terhadap bahaya eksternal dan internal, klasifikasi keselamatan desain mekanik, kualifikasi lingkungan, pemantauan status dan karakteristik sistem, diuji secara periodik, diinspeksi dan dirawat pada saat operasi, dapat diaktuasi secara manual.

Berdasarkan kriteria desain dari NRC[4,5] ditentukan untuk mencapai tingkat keandalan yang tinggi maka pada desain perlu menerapkan 7 hal yaitu: kriteria gagal tunggal (*single failure criterion*), redundansi, kemandirian (*independence*), keragaman (*diversity*), konsep gagal-aman (*fail-*

safe), interaksi sistem dan ketergantungan serta pemisahan fisik (*physical separation*). Dalam hubungannya dengan desain sistem pendingin yang bersifat sebagai sistem proteksi yaitu mencegah teras meleleh akibat panas peluruhan maka didesain dengan tingkat redundansi dan kemandirian untuk cukup menjamin bahwa tidak ada kegagalan tunggal yang mengakibatkan kehilangan fungsi. Demikian juga setiap komponen atau kanal yang merangkap fungsi/layanannya tidak menyebabkan redundansi minimum yang dipersyaratkan. Penerapan kriteria gagal tunggal untuk sistem redundan diimplikasikan pada redundan jalur atau kanal secara fisik mandiri terhadap satu sama lain. Selain itu setiap sistem yang mempunyai fungsi yang sama, tidak bergantung pada suplai daya listrik yang sama dan tidak menyebabkan kegagalan apabila terjadi perubahan lingkungan.

Kenaikan probabilitas gagal sistem atau komponen yang menerapkan prinsip redundan dan kemandirian adalah disebabkan kegagalan berpenyebab sama (*Common Cause Failure*, CCF), maka salah satu metoda untuk menghindari hal tersebut adalah dilakukan dengan menerapkan keragaman (*diversity*) dan pemisahan secara fisik. Walaupun dalam pengalaman teknis, beberapa hal rekayasa keragaman juga akan tidak berarti disebabkan oleh kegagalan berpenyebab sama. Kegagalan berpenyebab sama disebabkan antara lain: kesalahan desain atau marjin desain yang tidak cukup, cacat dalam manufaktur, kesalahan pengujian, penurunan fungsi akibat lingkungan (misalnya kelembaban, kotor, dan lain-lainnya) dan kejadian eksternal baik secara alam maupun ulah manusia (*human induced*). Beberapa hal yang perlu diterapkan dalam penentuan keragaman adalah penggunaan prinsip pengoperasian yang berbeda secara fisika, penggunaan manufaktur komponen yang berbeda, penggunaan teknik yang berbeda dalam pengujian, perawatan atau pengoperasian peralatan serta penempatan posisi yang berbeda secara fisik dan lokasi. Maka dari itu dalam desain, redundansi tidak hanya sekedar memberi cadangan tetapi juga harus dipertimbangkan keragamannya. Dalam reaktor daya setiap sistem keselamatan atau yang berfungsi untuk proteksi didesain secara redundansi ditunjang dengan sistem pendukung (*support system*) yang redundansi pula. Secara umum tujuan dari tindakan rekayasa dalam desain tersebut adalah untuk mempertahankan reaktor dapat padam dengan aman (*safe shutdown*) serta pendinginan yang cukup setelah padam.

2.2. Rentetan Kejadian Fukushima

Pada peristiwa Fukushima jenis reaktor daya adalah BWR dengan berbeda tipe (BWR 3 dan 4), sehingga rentetan kejadian (*event sequence*) setiap unit juga berbeda [6-8]. Dengan sistem yang digunakan untuk memitigasi kondisi darurat adalah sistem pemindah panas sisa, penyemprot teras tekanan rendah, injeksi teras tekanan tinggi, pendingin isolasi teras reaktor/kondensor isolasi (*Reactor Core Isolation Cooling/Isolation Condenser*, RCIC/IC), dan sistem pemboratan. Secara umum rentetan kejadian yang terjadi adalah diawali dengan kejadian pemicu gempa sehingga reaktor secara otomatis *scram* dan diikuti dengan hilangnya suplai daya *offsite* dari jaringan eksternal, serta sistem bekerja secara normal termasuk genset (*diesel generator*) beroperasi, sehingga reaktor dalam kondisi stabil. Setelah beberapa saat (55 menit) terjadi tsunami sehingga membanjiri beberapa gedung/fasilitas termasuk genset karena tinggi tsunami yang melebihi desain yang dipertimbangkan.

Peristiwa ini menimbulkan kegagalan pada genset. Kondisi ini diklasifikasikan sebagai *station blackout* (SBO), walaupun baterai masih berfungsi namun sistem pendingin teras darurat lainnya tidak berfungsi kecuali RCIC/IC. Kondisi pendinginan ini kurang efektif, karena tidak ada buangan panas sehingga memicu kenaikan temperatur dan tekanan di dalam teras. Setelah baterai habis, maka praktis temperatur akan naik, walaupun dilakukan usaha pengurangan tekanan dengan venting. Hal ini menimbulkan terjadinya kerusakan teras (pelelehan teras) serta dihasilkan hidrogen dari hasil reaksi Zr dan uap air, sehingga memicu terjadinya kecelakaan parah (*severe accident*).

2.3. Reaktor Daya Generasi III$^+$

Jenis reaktor daya yang mengalami kecelakaan pada peristiwa Fukushima merupakan reaktor generasi II. Sedangkan reaktor daya yang sekarang banyak dibangun adalah jenis desain generasi III$^+$ baik dari jenis PWR, BWR maupun air berat. Yang termasuk PWR generasi III$^+$ antara lain *Advanced Passive* 1000 (AP1000), *US-Advanced Pressurized Water Reactor* (US-APWR), *Evolutionary Pressurized Water Reactor* (EPR) dan lain-lainnya, sedangkan yang termasuk BWR adalah *Advanced Boiling Water Reactor* (ABWR) dan *Economic Simplified Boiling Water Reactor* (ESBWR). *Advanced* CANDU *Reactor* (ACR1000) merupakan jenis berpendingin air berat yang termasuk generasi III$^+$. Ciri khusus dari generasi III$^+$ adalah mempunyai daya yang besar, tingkat keekonomisan yang kompetitif serta tingkat keselamatan yang tinggi dengan frekuensi kerusakan teras yang semakin kecil, yaitu lebih kecil dari kriteria *International Nuclear Safety Advisory Group* (INSAG) sebesar 10^{-5} reaktor-tahun^{-1}, seperti ditunjukkan dalam Tabel 1. Setiap jenis reaktor daya generasi III$^+$ mempunyai keunggulan fitur desain yang berbeda.

Tabel 1. Frekuensi Kerusakan Teras Pada Reaktor Daya Generasi III$^+$[9]

	AP1000	US-APWR	EPR	ABWR	ESBWR	ACR1000
Frekuensi Kerusakan Teras (CDF), reaktor-tahun^{-1}	2,5 x 10^{-7}	1,2 x 10^{-6}	3,0 x 10^{-7}	1,6 x 10^{-7}	2,92 x 10^{-8}	9,5 x 10^{-8}

AP1000 berdaya 1154 MWe dengan 2 loop, serta menggunakan sistem pasif untuk meningkatkan keselamatannya. Sistem pasif tersebut digunakan pada sistem pendingin teras darurat (*Accumulator*, CMT dan PRHR) serta pendinginan pengungkung (*Passive Containment System*, PCS).

US-APWR berdaya 1700 MWe dengan 4 loop. Sistem keselamatan ditingkatkan dengan redundansi, menggunakan 4 jalur dengan masing-masing mempunyai kemampuan 50%, meningkatkan reaktivitas dan menghemat bahan bakar, meningkatkan sistem pasif pada sistem injeksi keselamatan (*Advanced Accumulator*).

EPR mempunyai kapasitas daya sebesar 1600 MWe dengan 4 loop, 4 jalur masing-masing 100% untuk ESF, pengungkung rangkap (*double-walled*) serta dilengkapi perlindungan terhadap tumbukan pesawat, dilengkapi *core catcher* untuk mendinginkan material teras setelah kecelakaan

parah yang menimbulkan kegagalan bejana reaktor, desain tidak hanya mengandalkan keselamatan pasif, setiap kasus kecelakaan tidak memerlukan evakuasi penduduk di sekitar reaktor daya.

ABWR mempunyai daya 1350 MWe, meningkatkan keselamatan dan kinerja pompa internal reaktor dengan mengeliminasi sistem resirkulasi eksternal, memberikan tingkat keandalan yang tinggi dalam pengendalian, gedung reaktor dan sungkup yang terintegrasi sehingga memperbaiki respon seismik.

ESBWR dengan daya 1550 MWe mempunyai 4 pipa uap dan 2 jalur untuk air umpan tanpa pompa. Selama kondisi normal menggunakan sirkulasi alam serta menghilangkan pompa resirkulasi, sistem kondensasi mempunyai 4 loop tekanan tinggi yang mandiri dengan berdasarkan sistem pasif. Sistem keselamatan berdasarkan sistem pasif yaitu sistem pendinginan secara gravitasi dengan 72 jam tanpa tindakan operator serta menggunakan sistem pendinginan pengungkung secara pasif.

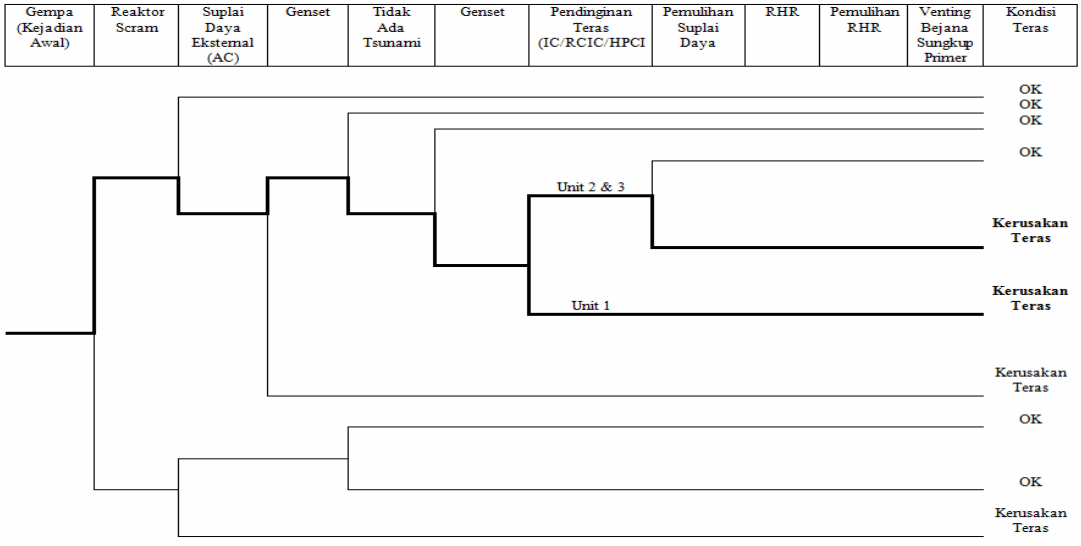
ACR1000 mempunyai daya 1200 MWe dengan 4 loop dan merupakan evolusioner pada kelas reaktor tabung bertekanan, berpendingin air ringan dengan menggunakan moderasi air berat. Keunggulan fitur desain adalah pengurangan inventori air berat, kemampuan penggunaan campuran bahan bakar MOX dan Thorium serta meningkatkan pengaturan daya.

3. METODE

Analisis dilakukan dengan mengkaji rentetan kejadian peristiwa Fukhushima, selanjutnya dilakukan penyusunan analisis pohon kejadian untuk menentukan faktor penting yang merupakan titik lemah, sehingga menyebabkan terjadi peristiwa tersebut. Dari faktor tersebut selanjutnya dibandingkan dengan fitur secara umum yang ada pada reaktor daya generasi III^+ apabila peristiwa serupa terjadi.

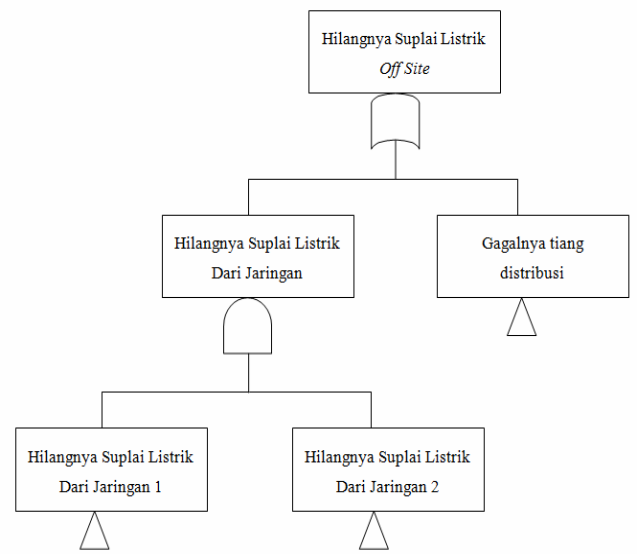
4. HASIL DAN PEMBAHASAN

Dari hasil kajian maka pada peristiwa Fukushima dapat disusun analisis pohon kejadian terjadinya teras meleleh seperti ditunjukkan dalam Gambar 1.



Gambar 1. Analisis Pohon Kejadian peristiwa Fukushima

Berdasarkan hasil analisis pohon kejadian tersebut sebenarnya banyak sekali faktor yang dapat dipelajari berdasarkan kejadian di Fukushima, namun untuk membatasi permasalahan, hanya ditinjau berdasarkan 4 hal yang mengakibatkan teras meleleh yaitu kehilangan suplai daya listrik *offsite*, tidak berfungsinya genset karena tsunami, tidak berfungsinya RHR, dan hilangnya buangan panas akhir (UHS). Maka 4 hal tersebut yang akan dibahas lebih lanjut.



Gambar 2. Analisis pohon kegagalan hilangnya suplai listrik *offsite*

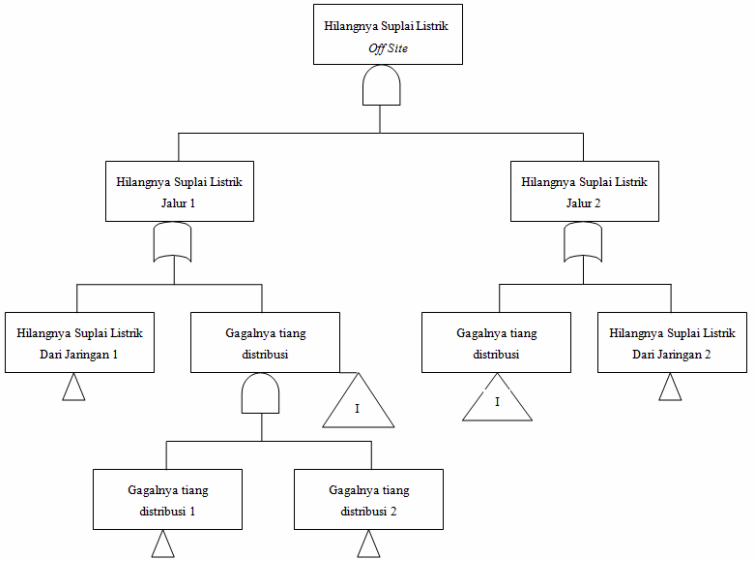
Menurut pedoman keselamatan, hilangnya suplai daya listrik *offsite* sudah dipertimbangkan dalam desain sebagai kejadian awal, sehingga harus dianalisis pada Laporan Analisis Keselamatan. Salah satu cara untuk mengantisipasi kejadian ini, didesain dengan adanya redundansi beberapa sumber listrik, secara sederhana dapat diasumsikan seperti ditunjukkan dalam Gambar 2. Maka dengan menggunakan analisis aljabar Boolean dapat ditentukan bahwa:

$$P(G) = P(A).P(B) + P(C) \quad (1)$$

bila P (A) dan P (B) menunjukkan probabilitas hilangnya suplai listrik dari jaringan 1 dan jaringan 2, sedangkan P (C) adalah gagalnya tiang distribusi. Dari persamaan tersebut terlihat bahwa tanpa memperhitungkan kegagalan berpenyebab sama (CCF) serta harga probabilitas gagal antara 0 dan 1, maka probabilitas gagal total P (G) kecil. Namun karena adanya CCF berupa gempa, maka penerapan redundansi (jaringan 1 dan 2) menjadi tidak ada artinya. Untuk mencegah pengaruh CCF tersebut sebenarnya kejadian "C" harus dibuat redundansi dan keragaman, dengan salah satunya misalnya membuat jaringan distribusi bawah tanah, sehingga tingkat probabilitas gagalnya menjadi kecil yaitu:

$$P(G) = P(A).P(B) + P(C_1).P(C_2) \quad (2)$$

dengan P (C_1) dan P (C_2) adalah probabilitas gagal tiang distribusi 1 dan 2, dengan model logika ditunjukkan seperti dalam Gambar 3.



Gambar 3. Analisis pohon kegagalan hilangnya suplai listrik *offsite* dengan keragaman tiang distribusi

Untuk mendapatkan harga probabilitas gagal yang konservatif pada desain, maka pada masing-masing jaringan listrik ditunjang dengan tiang distribusi yang berbeda secara ragam dan pemisahan fisik, maka probabilitas terjadinya *offsite* semakin kecil yaitu:

$$P(G)= P(A)P(B)+P(A)P(C_2)P(C_3)+P(B)P(C_1)P(C_2)+P(C_1)P(C_2)P(C_3)P(C_4) \quad (3)$$

dengan C_1, C_2, C_3 dan C_4 adalah tiang distribusi yang terpisah secara fisik, sehingga dari persamaan tersebut terlihat bahwa probabilitas gagal tiang distribusi karena CCF (gempa atau banjir/tsunami), menjadi sangat kecil. Tingkat keandalan sistem secara keseluruhan juga semakin tinggi, karena setiap minimal cutset terdiri atas lebih dari 1 kejadian dasar (*basic event).*

Kondisi kehilangan daya listrik *offsite* ini, dapat terjadi baik pada semua generasi dan tipe reaktor daya, yang berbeda adalah cara mitigasinya serta cara memperkecil frekuensi kejadian awal tersebut terjadi, antara lain dengan memperkecil kejadian dasar berupa CCF yaitu dengan pemilihan tapak yang tepat, serta menerapkan redundansi dan keragaman. Kecuali pada PWR dan BWR generasi III$^+$ yang fitur keselamatan teknisnya (ESF) mutlak menggunakan sistem pasif seperti halnya AP1000[10] dan ESBWR.

Frekuensi kerusakan teras merupakan salah satu parameter yang digunakan untuk indikator tingkat keselamatan reaktor daya. Kontribusi kehilangan suplai daya listrik (SBO) terhadap frekuensi kerusakan teras total seperti ditunjukkan dalam Tabel 2.

Dalam tabel tersebut menunjukkan bahwa SBO mempunyai kontribusi yang besar dalam frekuensi kerusakan teras baik pada reaktor daya generasi II maupun generasi III$^+$, namun terlihat bahwa frekuensi kontribusi terhadap CDF pada generasi III$^+$ semakin kecil yaitu turun sampai lebih dari 2 orde. Hal ini menunjukkan bahwa pada desain reaktor daya generasi III$^+$ kecil pengaruhnya menimbulkan kecelakaan parah, seperti halnya yang terjadi di Fukushima.

Tabel 2. Hasil Evaluasi Kontribusi SBO terhadap Frekuensi Kerusakan Teras (CDF) Pada Reaktor Daya Generasi II dan III^{+}[11-16]

	Generasi II		AP1000	US-APWR	EPR	ABWR	ESBWR	ACR-1000
	PWR	BWR						
Kontribusi SBO terhadap CDF, reaktor-tahun^{-1}	2,1 x 10^{-5}	3,1 x 10^{-6}	9,6 x 10^{-10}	5,8 x 10^{-7}	1,5 x 10^{-7}	9,1 x 10^{-8}	1,67 x 10^{-8}	2,03 x 10^{-8}
Prosentase kontribusi Terhadap Kerusakan Teras	43,3 %	72,9 %	0,4 %	49,3 %	49,3 %	56,8 %	57,19 %	21,0 %

Bahkan bila dibandingkan dengan AP1000 kontribusinya dapat diabaikan, demikian juga untuk jenis ESBWR dan ACR-1000 walaupun tidak dapat diabaikan, namun frekuensi nominalnya sangat kecil (berorde 10^{-8}). Dari tabel tersebut terlihat juga bahwa faktor sistem pasif sangat besar pengaruhnya terhadap penurunan kontribusi kerusakan teras dalam desain reaktor daya generasi III^{+}, karena sistem masih dapat melakukan fungsi keselamatannya walaupun kehilangan suplai daya listrik. Seperti *accumulator*, *Core MakeupTank* (CMT), *Passive Residual Heat Removal* (PRHR) dan *Passive Containment Cooling System* (PCCS) pada AP1000, sedangkan pada ESBWR adalah *Gravity Driven Cooling System* (GDCS), *Isolation Condenser System* (ICS) dan PCCS.

Tidak berfungsinya genset secara umum disebabkan keandalan genset yang rendah atau posisi genset yang tidak mempertimbangkan level banjir/tsunami serta posisi yang tidak terpisah secara fisik. Sehubungan dengan peristiwa di Fukushima, maka posisi mempunyai kontribusi terbesar terjadinya kegagalan genset. Dalam desain reaktor daya generasi III^{+} kondisi ini dilakukan dengan mengatur tata letak yaitu pada arah (kuadran) yang berbeda, pemisahan fisik yang sangat ketat, redundansi atau posisi level pada tempat yang tinggi. Dari hasil evaluasi terhadap reaktor daya generasi II dan III^{+} seperti ditunjukkan dalam Tabel 3.

Tabel 3. Hasil evaluasi Desain Posisi Genset, Prinsip RHR dan UHS Pada Reaktor Daya Generasi II dan III^{+}

Posisi Genset	Generasi II		AP1000	US-APWR	EPR	ABWR	ESBWR	ACR1000
	PWR	BWR						
Level/posisi	Rendah	Rendah	Rendah	Rendah	Rendah	Tinggi	Rendah	Rendah
Pemisahan Fisik	2 divisi, 1 kuadran	2 divisi, 1 kuadran	2 divisi, 1 kuadran (Genset bukan klas keselamatan)	4 divisi terpisah pada 2 kuadran	4 divisi terpisah pada 2 kuadran	3 divisi, 1 kuadran	2 divisi, 1 kuadran (Genset bukan klas keselamatan)	4 divisi terpisah pada 2 kuadran
RHR	Sistem aktif	Sistem aktif	Sistem pasif	Sistem aktif	Sistem aktif	Sistem aktif	Sistem pasif	Sistem aktif dan pasif
UHS	Air	Air	Udara	Air	Air	Air	Udara	Air dan Udara

Dari Tabel 3 tersebut terlihat bahwa level genset pada setiap tipe reaktor daya berbeda (pada tempat yang rendah atau tinggi), yang pada umumnya dikombinasikan dengan pemisahan fisik dan kuadran yang berbeda. Pada generasi reaktor daya generasi II pada umumnya terletak pada 1 kuadran (arah) yang sama, sehingga walaupun sudah diterapkan adanya redundansi (2 divisi) tetapi apabila terkena bahaya eksternal (misalnya banjir atau tsunami, maka kedua-duanya akan gagal). Hal ini tidak akan menjadi masalah untuk reaktor daya generasi III$^+$ yang mempunyai sistem keselamatan pasif, karena memang tidak tergantung suplai daya listrik, bahkan gensetnya tidak termasuk kelas keselamatan, misalnya pada AP1000 dan ESBWR. Sedangkan untuk reator daya generasi III$^+$ yang mengandalkan sistem keselamatannya dengan sistem aktif atau kombinasi dengan sistem pasif dilakukan dengan jumlah redundansi genset yang banyak antara 3 sampai 4 dengan diletakkan pada 2 kuadran yang berbeda, sehingga apabila 1 kuadran terkena bahaya eksternal, redundansi pada kuadran yang lain masih ada kemungkinan sukses, seperti misalnya pada US-APWR, EPR dan ACR1000. Untuk desain reaktor daya generasi III$^+$ yang meletakkan genset pada 1 kuadran, maka untuk mengantisipasi bahaya eksternal dilakukan dengan meletakkan genset pada posisi yang tinggi, seperti halnya pada ABWR.

Dengan melihat hasil pengaruh SBO cukup kecil terhadap CDF pada desain reaktor daya generasi III$^+$ maka menunjukkan bahwa permasalahan RHR dan UHS sudah mengalami perubahan desain juga dibandingkan reaktor daya pada peristiwa Fukushima. Desain RHR pada reaktor daya generasi III$^+$ pada umumnya masih berprinsip dengan sistem aktif yang artinya masih tergantung dengan suplai daya listrik, kecuali untuk beberapa tipe reaktor daya seperti AP1000 dan ESBWR, seperti ditunjukkan dalam Tabel 3. Maka untuk tipe yang masih berdasarkan sistem aktif meningkatkan keandalannya dilakukan dengan menerapkan prinsip redundansi yang ketat. Seperti pada US-APWR dengan berdasarkan prinsip 2 *out of* 4, demikian juga EPR terdiri atas 4 *train* yang terpisah secara fisik dan mandiri.

Beberapa tipe reaktor daya generasi III$^+$, RHR sudah bukan merupakan sistem utama dalam sistem keselamatan, karena sistem keselamatan yang bekerja sebelum RHR bekerja setelah terjadi kondisi abnormal, sudah mempunyai tingkat keandalan yang tinggi. Pada umumnya RHR pada reaktor tipe PWR di desain bersama dengan sistem injeksi tekanan rendah (*Low Pressure Injection System*, LPIS), setelah sistem ini berhenti maka fungsinya menjadi RHR. Pada US-APWR digabung dengan sistem penyemprot pengungkung (*Containment Spray System*, *CSS*).

Sehubungan dengan RHR, terutama yang berdasarkan sistem aktif perlu analisis lebih lanjut, karena pada perhitungan probabilistik maupun deterministik, pada peristiwa kehilangan daya listrik yang diasumsikan pada umumnya tidak berfungsinya pompa, sehingga menyebabkan kehilangan aliran pendingin. Seperti diketahui bahwa pada peristiwa di Fukushima terjadinya kecelakaan yang parah dikarenakan terjadinya kegagalan infrastruktur. Demikian juga seperti terlihat pada Gambar 1, dalam analisis pohon kejadian juga mempertimbangkan usaha pemulihan (*recovery*) pada RHR (maupun genset), maka perlu analisis lebih lanjut baik secara deterministik maupun probabilistik sampai berapa lama usaha pemulihan tersebut dapat dikatakan aman sehingga tidak menyebabkan teras meleleh.

Desain UHS yang diterapkan, salah satu faktornya tergantung dari sistem aktif atau pasif pada RHR, seperti ditunjukkan dalam Tabel 3. Apabila berdasarkan sistem pasif, maka sebagai UHS adalah udara. Pada kecelakaan parah yang disertai dengan kerusakan infrastruktur atau sistem, UHS yang mengandalkan udara lebih menguntungkan.

APR1400, ABWR dan ACR-1000 termasuk reaktor daya generasi III^+ yang desainnya berdasarkan konsep *twin*, perlu dianalisis lebih lanjut. Dalam manajemen kecelakaan yang dipertimbangkan pada analisis keselamatan probabilistik, kondisi tersebut menguntungkan yaitu apabila terjadi kehilangan suplai daya listrik *offsite* dan gagalnya genset dapat dilakukan usaha pemulihan dari instalasi sebelahnya, namun demikian apabila kecelakaan dasar desain menjadi kecelakaan parah, maka kondisi unit yang bersebelahan akan menjadi terpengaruh bahkan apabila sudah sampai terjadi kecelakaan parah dapat mengakibatkan terlepasnya hidrogen pada unit sebelahnya.

Dari kasus Fukushima ini dapat ditarik suatu pembelajaran bahwa kejadian tersebut bukan hanya dapat terjadi/didominasi pada salah satu tipe reaktor daya tertentu (BWR atau PWR), tetapi lebih tergantung pada desain sistem keselamatan yang dapat berfungsi secara optimal tanpa dipengaruhi perubahan lingkungan yang ekstrim. Selain itu, walaupun desain reaktor daya yang berdasarkan sistem pasif lebih tahan/rentan terhadap perubahan eksternal yang sangat ekstrim, namun perlu analisis lebih lanjut tentang ketahanan desain secara seismik. Karena apabila kekuatan gempa yang terjadi melebihi desainnya, maka infrastruktur dari sistem pasif dapat terganggu. Dalam hal ini perlu diterapkan *fail-safe* yang lebih ketat.

5. KESIMPULAN

Dari analisis desain reaktor daya generasi III^+ menunjukkan bahwa terjadinya kehilangan suplai daya listrik *offsite* yang memicu terjadinya kecelakaan parah seperti halnya peristiwa Fukushima adalah sangat kecil probabilitasnya. Hal ini karena desainnya sudah mengalami perubahan bila dibandingkan dengan reaktor daya generasi II. Perubahan yang terjadi adalah meningkatkan dan memperbaiki sistem keselamatannya maupun penerapan redundansi, keragaman, kemandirian dan pemisahan secara fisik serta tata letak secara ketat.

6. DAFTAR PUSTAKA

[1]. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA-GSR-Part 4, 2009.

[2]. INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plant: Design, IAEA-NS-R-1, 2001.

[3]. INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assesment for Nuclear Power Plants, IAEA-SSG-3, 2010.

[4]. BADAN PENGAWAS TENAGA NUKLIR, Ketentuan Keselamatan Desain Reaktor Daya, PERKA BAPETEN No. 3 Tahun 2011.

[5]. UNITED STATE NUCLEAR REGULATORY COMMISSION, General Design Criteria for Nuclear Power Plants, 10CFR50: Appendix A.

[6]. INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA International Fact Finding Expert Mission of the Nuclear Accident Following the Great East Japan Earthquake and Tsunami, Chapter 4, IAEA, 2011.

[7]. FUCHS, M., Ereignisse in Fukushima Daiichi, EFZN, 2011.

[8]. BRAUN, M., The Fukushima Daiichi Incident, AREVA, 2011.

[9]. TITKA, M., Generation III of Nuclear Reactor, AREVA, 2008.

[10]. SONY TJAHYANI, D. T., Analisis Probabilistik Banjir Eksternal Terhadap Desain PWR Generasi III^{+}, Prosiding Seminar Nasional Pengembangan Energi Nuklir, Bangka-Belitung, 2011.

[11]. U. S. NUCLEAR REGULATORY COMMISSION, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plant, Nureg-1150, 1990.

[12]. STERDIS, A., AP1000 Regulatory Overview, Westinghouse.

[13]. MHI, Design Control Document for the US-APWR: Chapter 19 Probabilistic Risk Assessment and Severe Accident Evaluation, 2007.

[14]. AREVA, U.S. EPR FINAL SAFETY ANALYSIS REPORT, 2006.

[15]. BHATT, S. C., ESBWR Certification Probabilistic Risk Assessment, NEDO-33201, 2006.

[16]. Leach, G., ACR-1000 Level 2 Probabilistic Safety Assessment and the ACR Accident Source Term, AECL, 2008.

DISKUSI/TANYA JAWAB:

1. PERTANYAAN: (Purwadi, S.Si., Guru SMAN 1 Kasihan BANTUL)

- Dalam latarbelakang, Indonesia berada dalam daerah sabuk gempa aktif. Seberapa besar kemampuan reaktor generasi ini kuat menahan gempa?.

JAWABAN: (D.T. Sony Tjahyani, PTRKN-BATAN)

- *Pada desain reaktor sebenarnya, parameter yang diterapkan bukan kekuatan menahan gempa, tetapi percepatan gempa yang mampu ditahan biasanya diberi satuan "g", dimana "g" menunjukkan percepatan gravitasi (9,8 m/dt^2), misalnya 0,3g. Yang menentukan parameter ini adalah badan regulasi setiap negara dan permintaan* ***owner*** *(User Requirement Document, URD). Patut diketahui semakin besar parameter "g" akan semakin mahal pula harga reaktor tersebut.*