

EVALUASI KESELAMATAN TERHADAP BAHAYA EKSTERNAL PADA KONDISI PADAM UNTUK AP1000 DAN VVER 1200

D. T. Sony Tjahyani

Pusat Teknologi Reaktor dan Keselamatan Nuklir – BATAN
Kawasan Puspptek Gd. 80, Serpong, Tangerang 15310
Telp/Fax: 021-7560912/021-7560913
e-mail: dtsony@batan.go.id

ABSTRAK

EVALUASI KESELAMATAN TERHADAP BAHAYA EKSTERNAL PADA KONDISI PADAM UNTUK AP1000 DAN VVER1200. Analisis keselamatan dilakukan berdasarkan kejadian awal internal, bahaya internal maupun eksternal baik pada kondisi daya penuh dan padam. Berdasarkan *expert mission* IAEA setelah kejadian Fukushima dihasilkan beberapa kesimpulan dan pembelajaran. Salah satu kesimpulan tersebut adalah ketidakcukupan konsep pertahanan berlapis dalam mengatasi bahaya tsunami serta diperlukan suatu tindakan/sistem untuk menjamin keselamatan terhadap bahaya eksternal. Jenis reaktor yang sedang dibangun saat ini adalah AP1000 (*Advanced Passive Pressurized Water Reactor 1000*) dan VVER 1200 (*Vodo Vodyanoi Energetichesky Reactor ≈ Water-Water Energetic Reactor*). Pada saat ini, Indonesia belum memastikan jenis reaktor daya yang akan dibangun. Maka sangatlah penting menganalisis keselamatan teknologi reaktor yang berkembang saat ini. Tujuan dari makalah ini adalah mengevaluasi keselamatan AP1000 dan VVER1200 pada kondisi padam terhadap bahaya eksternal. Analisis dilakukan dengan mengidentifikasi kegiatan pada kondisi padam selanjutnya dilakukan perhitungan kemungkinan ketersediaan dari sistem dalam mengatasi bahaya eksternal dengan memperhitungkan faktor redundansi dan keragaman sumber pendingin dari luar. Hasil analisis didapatkan bahwa probabilitas sistem berfungsi dalam mengatasi bahaya eksternal bervariasi antara 0,0001 – 0,3673 untuk AP1000 dan 0 – 0,3213 untuk VVER1200. Dari evaluasi ini disimpulkan bahwa AP1000 dan VVER1200 secara probabilistik mempunyai tingkat keselamatan yang cukup tinggi, meskipun demikian perlu ditunjang analisis secara deterministik.

Kata kunci: bahaya eksternal, kondisi padam, AP1000, VVER1200, probabilistik.

ABSTRACT

SAFETY EVALUATION AGAINST EXTERNAL HAZARD ON SHUTDOWN CONDITION FOR AP1000 AND VVER1200. The safety analysis is carried out based on internal initiating events, internal and external hazards both at full power and shutdown condition. Based on IAEA expert mission after Fukushima event is recommended several conclusions and learning. One of the conclusions, there was insufficient defense in depth provisions for tsunami hazard and required an action or system to ensure safety against external hazards. Type of reactor which is being built in current is AP1000 (*Advanced Passive Pressurized Water Reactor 1000*) and VVER 1200 (*Vodo Vodyanoi Energetichesky Reactor ≈ Water-Water Energetic Reactor*). At this time, Indonesia does not decide yet the type of power reactor to be built. So, It is important to analyze the safety of the reactor technology developed at present. The purpose of this paper is to evaluate the safety of AP1000 and VVER1200 on shutdown condition against external hazards. The analysis was done by identifying the activities on shutdown condition, hereinafter it is carried out probability calculation of system availability to mitigate external hazards based on redundancy and diversity of cooling sources from the outside. The analysis result is obtained that the probability of the system to mitigate external hazards between 0.0001 to 0.3673 for the AP1000 and 0 to 0.3213 for VVER1200. Based on evaluation, it is concluded that AP1000 and VVER1200 by probabilistic method have a highly safety level, however it should be supported by deterministic analysis.

Keywords: external hazard, shutdown condition, AP1000, VVER1200, probabilistic.

PENDAHULUAN

Dalam analisis keselamatan, sebagai tahapan awal adalah menentukan kejadian awal (*initiating event*) yaitu kejadian yang dipertimbangkan pada desain sehingga menimbulkan kejadian operasional terantisipasi atau kecelakaan dan ancaman terhadap fungsi keselamatan. Kejadian awal terdiri atas kejadian internal dan bahaya. Kejadian internal disebabkan oleh 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 dari luar tapak. Beberapa jenis bahaya eksternal yang dipertimbangkan adalah gempa, tsunami, banjir, kebakaran, kejadian ulah manusia (*human induced*), dan lain-lainya.

Berdasarkan *expert mission* IAEA terhadap kejadian Fukushima telah dihasilkan 15 item kesimpulan dan 16 item pembelajaran^[1]. Salah satu kesimpulan tersebut adalah ketidakcukupan konsep pertahanan berlapis (*defence in depth*) dalam mengatasi bahaya tsunami. Selain itu harus melakukan revisi terhadap pedoman dan persyaratan keselamatan secara komprehensif sehubungan dengan gempa bumi, tsunami, banjir eksternal serta semua kejadian eksternal. Beberapa item pembelajaran yang dapat diambil dalam kejadian tersebut adalah diperlukan suatu tindakan/sistem untuk menjamin keselamatan terhadap bahaya eksternal. Dalam hal terjadi kondisi parah, misalnya hilangnya suplai daya listrik luar kawasan (*off-site*), hilangnya buangan panas (*heat sink*) atau hilangnya sistem keselamatan terekayasa (*engineering safety system*) harus disediakan sumber alternatif yang sederhana untuk peralatan yang signifikan (misalnya suplai daya yang bergerak, suplai air dan udara bertekanan) dalam proses manajemen kecelakaan parah.

Berdasarkan pedoman IAEA NS-G-2.15^[2] disebutkan bahwa dalam menentukan manajemen kecelakaan parah harus memperhitungkan pada semua modus operasi termasuk pada kondisi padam (*shutdown*) serta mempertimbangkan kejadian eksternal seperti kebakaran, banjir, gempa dan kondisi cuaca yang ekstrim. Hal ini juga ditunjang dengan kejadian di Fukushima Dai-ichi unit 4 yang mengalami kehilangan pendingin pada kolam penyimpanan bahan bakar bekas setelah terjadi gempa dan tsunami. Dari analisis probabilistik juga menunjukkan bahwa frekuensi kerusakan teras pada kondisi operasi dan padam mempunyai orde yang hampir sama.

Pada saat ini jenis reaktor yang sedang dibangun/konstruksi adalah jenis PWR generasi III⁺ berdasarkan sistem aktif dan pasif. AP1000 (*Advanced Passive Pressurized Water Reactor 1000*) dan VVER 1200 (*Vodo Vodyanoi Energetichesky Reactor ≈ Water-Water Energetic Reactor*) termasuk jenis PWR generasi III⁺ berdasarkan sistem pasif, yang sedang atau segera dibangun di China, Rusia, India, Amerika dan Vietnam.

Pada saat ini di Indonesia belum memastikan jenis reaktor daya yang akan dibangun, maka sangatlah penting menganalisis keselamatan teknologi reaktor yang berkembang saat ini dari berbagai faktor serta berdasarkan implementasi konsep keselamatan setelah kejadian Fukushima.

Tujuan dari makalah ini adalah mengevaluasi keselamatan reaktor daya AP1000 dan VVER1200 yang merupakan PWR generasi III⁺ pada kondisi padam terhadap bahaya eksternal. Analisis dilakukan dengan mengidentifikasi kegiatan reaktor daya pada kondisi padam selanjutnya

dilakukan perhitungan kemungkinan ketersediaan dari sistem dalam mengatasi bahaya eksternal dengan memperhitungkan faktor redundansi dan keragaman sumber pendingin dari luar.

KONSEP KESELAMATAN DAN ANALISIS PROBABILISTIK SETELAH KEJADIAN FUKUSHIMA

Berdasarkan *expert mission*, pelajaran yang harus diimplementasikan pada desain reaktor daya saat ini terhadap bahaya eksternal adalah:

- Pemilihan tapak desain reaktor daya hendaknya memberikan proteksi yang cukup terhadap bahaya eksternal yang jarang terjadi serta dapat menimbulkan kejadian kombinasi yang kompleks, khususnya kejadian yang dapat menyebabkan banjir pada tapak dan mempunyai pengaruh jangka panjang.
- Tata letak instalasi hendaknya mempertahankan “konsep tapak kering” (*dry site concept*) yang merupakan tindakan pertahanan berlapis terhadap banjir pada tapak seperti halnya pemisahan secara fisik dan keragaman dari sistem keselamatan yang kritis.
- Kegagalan berpenyebab sama (*common cause failure*) hendaknya dipertimbangkan secara khusus untuk tapak yang terdiri atas beberapa unit serta tapak yang berdekatan. Serta disediakan pula pilihan pemulihan (*recovery*) yang tidak saling tergantung dan dapat menggunakan semua sumber yang ada pada tapak.
- Setiap perubahan bahaya eksternal atau fenomenanya hendaknya secara periodik ditinjau ulang dampaknya pada konfigurasi instalasi.
- Sistem alarm tsunami hendaknya ditetapkan untuk tindakan operator sesegera mungkin.

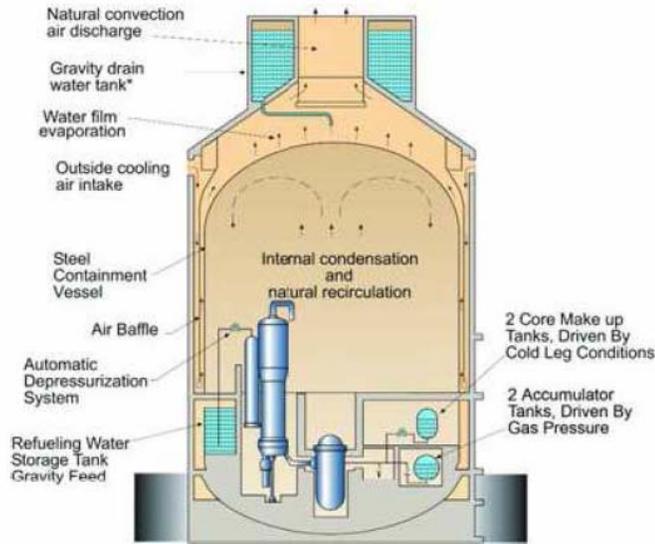
Berdasarkan dokumen IAEA terutama setelah terjadinya peristiwa Fukushima, analisis probabilistik harus selalu dipadukan dengan analisis deterministik. Karena walaupun peluang terjadinya kecelakaan sangat kecil, tetap harus dianalisis dengan analisis deterministik bagaimana hasilnya bila yang diskenariokan terjadi. Sebagai contoh dapat dilihat pada peristiwa Fukushima. Walaupun target frekuensi kerusakan teras (*core damage frequency, CDF*) sangat kecil dan apabila dihubungkan dengan waktu hidup reaktor, maka kecelakaan parah tersebut tidak akan terjadi selama hidup reaktor, namun perhitungan akan berubah dengan drastis bila kejadian tersebut terjadi pada tahun terakhir dari periode hidup reaktor tersebut. Berdasarkan kejadian tersebut, bukan berarti analisis probabilistik tidak diperlukan. Analisis probabilistik dilakukan untuk menunjukkan bahwa sesuatu kejadian tersebut terjadi setelah melalui tahapan-tahapan mitigasi yang gagal serta menunjukkan titik terlemah mengapa tahapan mitigasi tersebut gagal. Tahapan mitigasi serta titik terlemah tersebut berhubungan dengan tingkat teknologi keselamatan reaktor daya.

AP1000 dan VVER1200 merupakan reaktor PWR generasi III⁺ yang merupakan versi Amerika dan Rusia. Ke-2 tipe reaktor daya tersebut berdasarkan sistem pasif dalam mengatasi kecelakaan dasar desain maupun kecelakaan parah, walaupun terdapat perbedaan. Pada AP1000 mengandalkan mutlak sistem pasif, sedangkan VVER1200 perpaduan antara sistem aktif dan pasif.

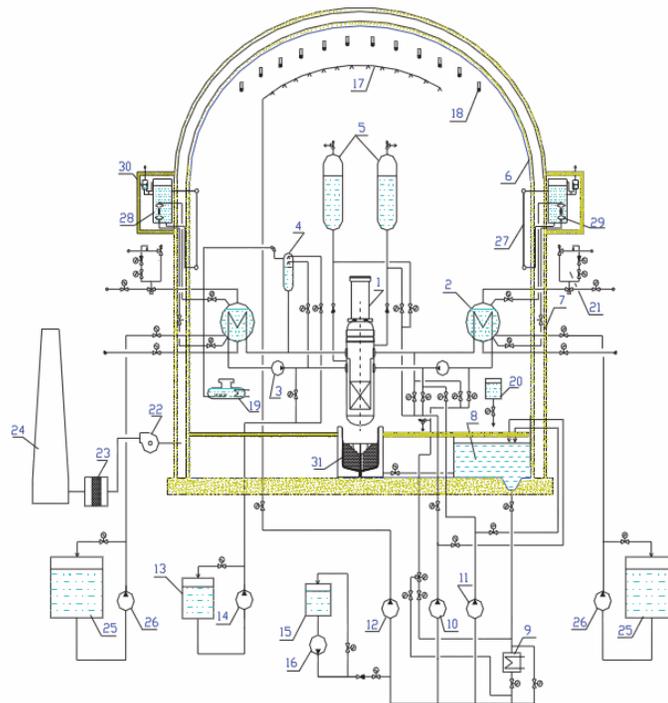
Perbedaan sistem keselamatan yang penting antara AP1000 dan VVER1200 seperti ditunjukkan dalam Tabel 1, serta diagram sistemnya seperti ditunjukkan dalam Gambar 1 dan 2.

Tabel 1. Perbedaan Sistem Keselamatan Antara AP1000 dan VVER1200^[3,4]

| No. | Fungsi Keselamatan | AP1000 | | VVER1200 | |
|-----|--|---|---------------|--|---------------|
| | | Sistem | Prinsip Kerja | Sistem | Prinsip Kerja |
| 1. | Menyiram teras pada tekanan rendah (<i>Large LOCA</i>) | Akumulator | Pasif | HA-2 (<i>Hydro Accumulator-2</i>) | Pasif |
| | | | | LPEI (<i>Low Pressure Emergency Injection</i>) | Aktif |
| 2. | Menyiram teras pada tekanan tinggi (<i>Small LOCA</i>) | CMT (<i>Core Make-up Tank</i>) | Pasif | HA-1 (<i>Hydro Accumulator-1</i>) | Pasif |
| | | | | HPEI (<i>High Pressure Emergency Injection</i>) | Aktif |
| 3. | Menyiram teras pada jangka panjang (<i>Long term</i>) | PRHR-HX (<i>Passive Residual Heat Removal Heat Exchanger</i>) | Pasif | PSHR SG (<i>Passive System of Heat Removal from Steam Generator</i>) | Pasif |
| | | IRWST (<i>In-Containment Refueling Water storage Tank</i>) | Pasif | | |
| 4. | Mendinginkan Pengungkung (<i>Containment</i>) | PCS (<i>Passive Containment Cooling System</i>) | Pasif | PSHR C (<i>Passive System of Heat Removal from Containment</i>) | Pasif |
| | | | | Core spray | Aktif |



Gambar 1. Diagram Sistem Keselamatan AP1000^[5].



- | | | | |
|----------------------|---|---|--------------------------------------|
| 1. Reactor | 9. Heat exchangers | 17. Spray collector | 25. Desalted water storage tank |
| 2. Steam generator | 10. Low pressure emergency injection pump | 18. Passive hydrogen recombiner | 26. Emergency injection pump |
| 3. RCPS | 11. High pressure emergency injection pump | 19. Bubbler | 27. PSHR C condenser heat exchanger |
| 4. Pressurizer | 12. Spray pump | 20. Emergency alkali storage tank | 28. PSHR emergency heat removal tank |
| 5. ECCS tanks | 13. High concentration boric water storage tank | 21. Main steam valve block | 29. PSHR SG heat exchanger |
| 6. Containment | 14. Emergency Boron Injection Pump | 22. Ventilation for emergency depression in the annular gap | 30. Hydraulic lock |
| 7. Outer containment | 15. Chemicals supply tank | 23. Filter | 31. Core melt localizing facility |
| 8. Sump tank | 16. Chemicals injection pump | 24. Ventilation stack | |

Gambar 2. Diagram Sistem VVER1200^[4]

METODOLOGI

Melakukan evaluasi ketahanan AP1000 dan VVER 1200 pada kondisi padam dalam mengatasi bahaya eksternal. Analisis dilakukan dengan menentukan aktivitas reaktor pada kondisi padam dan selanjutnya dilakukan skenario adanya bahaya eksternal berupa gempa dan tsunami, karena ke-2 bahaya eksternal tersebut yang mempunyai dampak yang lebih luas dan kompleks. Aktivitas pada kondisi padam dipilih berdasarkan SSG-3^[6]. Selanjutnya dilakukan perhitungan yaitu membandingkan jumlah terjadinya kegiatan tersebut dengan kejadian pada daya rendah dan padam pada PWR sistem pasif dalam hal ini AP1000 dan VVER 1200. Sebagai batasan analisis, sistem keselamatan dan tindakan operator dalam mengantisipasi kejadian eksternal tersebut adalah tingkat redundansi dan keragaman (*diversity*) sumber pendingin yaitu untuk menentukan jumlah sumber pendingin.

Untuk menunjang hasil evaluasi juga dilakukan perhitungan probabilitas gagal AP1000 dan VVER1200 dalam menghadapi bahaya eksternal pada kondisi operasi menggunakan metoda binomial dengan mengasumsikan kriteria sukses beberapa sistem yaitu menentukan probabilitas ketersediaan sistem dalam memitigasi kondisi bahaya eksternal. Selanjutnya untuk menunjukkan perubahan target keselamatan setelah terjadi peristiwa Fukushima, maka dilakukan perhitungan CDF yaitu terjadinya kecelakaan parah dibandingkan dengan periode operasi reaktor. Dari perhitungan dan jenis keselamatan tersebut ditentukan tingkat keselamatan pada AP1000 dan VVER1200.

HASIL DAN PEMBAHASAN

Sistem keselamatan setelah terjadinya Fukushima mengalami perubahan yang sangat menyeluruh yaitu harus terdapat sistem yang dapat mengantisipasi terhadap bahaya eksternal, karena pada umumnya teknologi reaktor daya hanya menekankan kejadian internal yaitu kegagalan komponen dan kesalahan operator sudah diantisipasi dari sistem yang ada baik secara aktif maupun pasif. Apalagi setelah terjadinya peristiwa Chernobyl dan TMI. Dalam konsep keselamatan selain reaktor dapat dikendalikan harus mampu memindahkan panas yang terjadi, karena lepasan produk fisi terjadi dikarenakan pendinginan yang tidak cukup. Maka salah satu implementasi dalam reaktor daya generasi III⁺ adanya kecukupan sumber pendingin yang bila memungkinkan beroperasi secara pasif.

Hal ini terlihat dari hasil analisis sistem antara AP1000 dan VVER1200, sistem pasif mampu mengatasi pada kecelakaan dasar desain dan kecelakaan parah, namun pada saat kondisi daya penuh (*full power operating*). Pada kondisi ini, keragaman sistem keselamatan baik secara pasif maupun aktif akan menurunkan probabilitas gagal dalam menghadapi kecelakaan tersebut bila dibandingkan dengan PWR yang banyak beroperasi saat ini, seperti terlihat dari hasil perhitungan ditunjukkan dalam Tabel 2.

Tabel 2. Probabilitas gagal AP1000 dan VVER1200 Dibandingkan PWR acuan dalam menghadapi bahaya eksternal

| | AP1000 | VVER1200 |
|---|--------|----------|
| Penurunan probabilitas gagal sistem jika dibandingkan dengan PWR yang beroperasi saat ini | 0,200 | 0,143 |

Perhitungan tersebut hanya berdasarkan keragaman (*diversity*) sistem keselamatan dengan tanpa memperhitungkan redundansi, yang apabila dipertimbangkan probabilitas gagalnya akan semakin kecil. Hal ini dikarenakan walaupun bahaya eksternal terjadi, maka pendinginan akan tetap berlangsung walaupun tidak ada sumber listrik dengan syarat sistem tersebut tidak rusak dikarenakan bahaya eksternal. Untuk VVER1200 probabilitas gagalnya lebih kecil karena sistem injeksi pendingin ke teras selain berdasarkan sistem pasif juga dipadukan dengan sistem aktif. Walaupun pada kondisi kehilangan suplai daya listrik, sistem aktif tidak banyak berperan. Pada kecelakaan parah akibat bahaya eksternal, AP1000 lebih unggul karena mempunyai tangki PCS (*passive containment cooling system*) dengan volume pendingin yang cukup memadai dan bekerja secara pasif.

Pada kondisi reaktor padam, sistem keselamatan pasif tersebut tidak bekerja, karena sistem kerja pasif tersebut berdasarkan tekanan dan *driving force* yang tidak dapat berfungsi atau kinerjanya menurun pada saat tekanan dan temperatur yang rendah. Dalam analisis keselamatan, kondisi padam dan daya rendah dianalisis dalam satu kelompok. Berdasarkan pedoman dari SSG-3 untuk kelompok pada kondisi padam dan daya rendah, maka dapat dihitung kegiatan pada kondisi padam sekitar 65,57% dengan rincian sebagai berikut: transien 10,81%, LOCA 35,14%, kebakaran dan banjir internal 8,11%, kekritisasi 8,11 % dan jatuhnya beban berat 5,41%. Maka kejadian yang signifikan pada kondisi padam adalah kelompok LOCA yang terdiri atas kebocoran pada bejana tekan, RHR (*residual heat removal*), kavitas reaktor, sistem penghubung dan kolam penyimpanan bahan bakar bekas. Sehingga dalam desain harus dipertimbangkan keragaman dan redundansi sumber pendingin lainnya untuk mengatasi kebocoran tersebut. Pada kondisi padam, umumnya fungsi keselamatan hanya untuk mencukupi pendingin dalam menjaga panas peluruhan dengan temperatur yang relatif rendah. Yang perlu dianalisis lebih seksama adalah bahaya eksternal terjadi sesaat setelah reaktor padam, yaitu temperatur masih relatif tinggi, tetapi sistem pasif tidak bekerja.

Pada kondisi padam dengan diikuti bahaya eksternal, maka harus dianalisis jumlah sumber pendingin yang ada di sekitar fasilitas. Dengan asumsi sumber pendingin terdiri atas pompa dan sistem pemipaan yang dapat di masukkan ke dalam fasilitas dengan probabilitas gagal sebesar $9,64 \cdot 10^{-2(7)}$, maka dapat dihitung probabilitas sumber-sumber pendingin berfungsi untuk AP1000 dan VVER1200, seperti ditunjukkan dalam Tabel 3. Dalam perhitungan itu digunakan asumsi beberapa kriteria sukses sumber pendingin, karena dalam memitigasi bahaya eksternal tidak diketahui dengan pasti berapa jumlah pendingin yang diperlukan, tergantung dari tingkat keparahan. Dimana tingkat keparahannya sangat random. Hal ini berbeda dengan kejadian/bahaya internal yang dapat ditentukan lebih pasti jumlah pendingin yang diperlukan untuk memitigasi atau mendinginkan.

Tabel 3. Probabilitas Sistem Berfungsi Untuk Memitigasi Kondisi Bahaya Eksternal

| No. | Jenis Reaktor | Jumlah Sumber Pendingin | Probabilitas Sistem berfungsi | | | | |
|-----|---------------|-------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|------------------------------------|
| | | | Kriteria Sukses 1 Sumber Pendingin | Kriteria Sukses 2 Sumber Pendingin | Kriteria Sukses 3 Sumber Pendingin | Kriteria Sukses 4 Sumber Pendingin | Kriteria Sukses 5 Sumber Pendingin |
| 1. | AP1000 | 7 | 0,3673 | 0,1776 | 0,0209 | 0,0022 | 0,0001 |
| | | 10 | 0,3871 | 0,1859 | 0,0529 | 0,0099 | 0,0013 |
| 2. | VVER1200 | 5 | 0,3213 | 0,0686 | 0,0073 | 0,0004 | ≈ 0 |
| | | 10 | 0,3871 | 0,1859 | 0,0529 | 0,0099 | 0,0013 |

Dari Tabel 3 tersebut terlihat bahwa semakin tinggi kriteria sukses pendingin yang artinya semakin banyak sumber pendingin yang diperlukan, maka akan semakin kecil probabilitas ketersediaannya untuk memitigasi bahaya eksternal. Hal ini berlaku baik untuk AP1000 maupun VVER1200. Untuk tingkat kriteria sukses yang sama, AP1000 mempunyai probabilitas ketersediaan yang lebih tinggi bila dibandingkan dengan VVER1200. Kondisi ini terjadi karena pada AP1000 mempunyai sumber pendingin lebih banyak jika dibandingkan dengan VVER1200. Sejumlah 5 (lima) sumber pendingin antara AP1000 dan VVER1200 mempunyai sumber pendingin yang identik, sedangkan 2 lainnya pada AP1000 mempunyai sumber pendingin yang spesifik dengan mempunyai kapasitas pendingin yang cukup besar yaitu PCWST (*passive containment cooling water storage tank*) dan PCAWST (*passive containment cooling ancillary water storage tank*). Walaupun dalam kondisi padam diperlukan tindakan operator untuk membuka katup pada PCWST, sedangkan untuk PCAWST diperlukan pompa untuk mengalirkan dari PCAWST ke PCWST. Dari Tabel 3 tersebut juga ditunjukkan bila semakin banyaknya sumber pendingin (misalnya 10 jenis), maka probabilitas ketersediaan sistem juga semakin besar pula. Untuk implementasi lebih lanjut, sumber-sumber pendingin tersebut harus terletak pada tapak yang sesuai dengan “*Dry Site Concept*”.

Sebenarnya bahaya (baik internal maupun eksternal) sudah terdapat dalam beberapa pedoman IAEA baik pada saat pemilihan tapak maupun implementasi pada desain yaitu kejadian ulah manusia (*human induced*), gempa, meteorologi yang ekstrim, banjir, kebakaran dan ledakan [8-15] sejak dulu, namun karena diasumsikan peluang terjadinya kecil serta tidak mengasumsikan kejadian yang beruntun serta menimbulkan pengaruh jangka panjang maka kurang mendapat perhatian secara lebih seksama dalam analisis keselamatan sebelum terjadinya peristiwa Fukushima.

Berdasarkan kejadian Fukushima ini maka telah terjadi perubahan fenomena keselamatan yang sangat signifikan karena diakibatkan pengaruh bahaya eksternal. Perubahan tersebut yaitu target keselamatan dimana ditentukan kerusakan teras $< 10^{-4}$ reaktor tahun⁻¹ atau lepasan produk fisi $< 10^{-5}$ reaktor tahun⁻¹ untuk reaktor yang sudah ada atau beroperasi saat ini telah terlampaui, hal ini terlihat dalam perhitungan yang dilakukan seperti ditunjukkan dalam Tabel 4, yaitu dalam waktu yang singkat target keselamatan terlampaui sangat signifikan pada reaktor daya yang sedang operasi (unit 1, 2 dan 3) serta padam (unit 4) semuanya disebabkan oleh bahaya eksternal.

Tabel 4. Perhitungan CDF/probabilitas kecelakaan parah setelah terjadinya bahaya eksternal

| No. | Fukushima Dai-ichi | Tahun Operasi Komersil | Perhitungan CDF/probabilitas kecelakaan parah setelah terjadinya bahaya eksternal, reaktor-tahun ¹ |
|-----|--------------------|------------------------|---|
| 1. | Unit 1 | 1971 | $2,44.10^{-2}$ |
| 2. | Unit 2 | 1974 | $2,63.10^{-2}$ |
| 3. | Unit 3 | 1976 | $2,78.10^{-2}$ |
| 4. | Unit 4 | 1978 | $2,94.10^{-2}$ |

Dari tabel tersebut terlihat dengan adanya bahaya eksternal seolah-olah analisis probabilistik mempunyai penyimpangan yang sangat besar. Sebenarnya tidak demikian, analisis probabilistik menunjukkan bahwa sesuatu yang mempunyai probabilitas kecil disebabkan oleh beberapa tahapan kegagalan sistem yang masing-masing mempunyai probabilitas gagal yang kecil pula, sehingga peluang terjadinya secara keseluruhan juga kecil. Maka dengan kejadian Fukushima ini analisis secara deterministik sebaiknya memadukan kejadian internal dan bahaya eksternal secara bersamaan.

Dari hasil evaluasi ini menunjukkan tingkat keselamatan AP1000 dan VVER1200 pada kondisi operasi menunjukkan tingkat keselamatan yang tinggi, karena adanya beberapa ragam keselamatan yang bekerja secara pasif. Pada kondisi padam secara probabilistik juga menunjukkan tingkat keandalan yang tinggi karena adanya beberapa sumber pendingin. Meskipun demikian harus dilakukan perhitungan secara deterministik untuk beberapa skenario yang menggambarkan variasi jumlah air pendingin yang diperlukan.

KESIMPULAN

Berdasarkan evaluasi ini menunjukkan bahwa AP1000 dan VVER1200 secara probabilistik mempunyai tingkat keselamatan yang cukup tinggi, meskipun demikian perlu ditunjang analisis secara deterministik. Probabilitas sistem berfungsi dalam mengatasi bahaya eksternal bervariasi antara 0,0001 – 0,3673 untuk AP1000 dan 0 – 0,3213 untuk VVER1200.

DAFTAR PUSTAKA

- [1]. INTERNATIONAL ATOMIC ENERGY AGENCY, Mission Report: IAEA International Fact Finding Expert Mission of the Fukushima Dai-ichi NPP Accident Following the Great East Japan Earthquake and Tsunami, Department of Nuclear Safety and Security, Vienna, 2011.
- [2]. INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear power Plants, IAEA-NS-G-2.15, Vienna, 2009.
- [3]. WESTINGHOUSE, “AP1000 Technology Seminar”, Jakarta, 2011.
- [4]. ATOMENERGOPROEKT, Design AES2006: Concept Solutions by the Examples of Leningrad NPP-2, ROSATOM Company, Saint Petersburg, 2011.
- [5]. Martin T., Generation III of Nuclear Reactor, AREVA, 2008.
- [6]. INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA-SSG-3, Vienna, 2010.

- [7]. INTERNATIONAL ATOMIC ENERGY AGENCY, Component Reliability Data for Use in Probabilistic Safety Assessment, IAEA-TECDOC-478, Vienna, 2010.
- [8]. INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA-NS-G-3.1, Vienna, 2002.
- [9]. INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Hazards for Nuclear Power Plants, IAEA-NS-G-3.3, Vienna, 2002.
- [10]. INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological Events in Site Evaluation for Nuclear Power Plants, IAEA-NS-G-3.4, Vienna, 2003.
- [11]. INTERNATIONAL ATOMIC ENERGY AGENCY, Flood Hazard for Nuclear Power Plants on Coastal and River Sites, IAEA-NS-G-3.5, Vienna, 2003.
- [12]. INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA-NS-G-1.5, Vienna, 2003.
- [13]. INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA-NS-G-1.6, Vienna, 2003.
- [14]. INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the design of Nuclear Power Plants, IAEA-NS-G-1.7, Vienna, 2004.
- [15]. INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the design of Nuclear Power Plants, IAEA-NS-G-1.11, Vienna, 2004.

DISKUSI/TANYA JAWAB:

1. PERTANYAAN: (Amir Hamzah, PTRKN – BATAN)

- Bagaimana akurasi analisis tersebut bila dibandingkan dengan analisis deterministik, dan bagaimana hasil tersebut dibandingkan dengan SAR?
- Berdasarkan hasil, apakah reaktor dalam kondisi aman?

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

- *Akurasi hasil analisis probabilistik tidak dapat dibandingkan dengan analisis deterministik, tetapi kedua metoda tersebut saling melengkapi. Selain itu hasil yang kami lakukan tidak dapat dibandingkan dengan SAR, karena analisis ini dilakukan setelah terjadinya Fukushima.*
- *Hasil analisis menunjukkan kondisi cukup aman, karena secara probabilitas menunjukkan ketersediaan pendingin selalu mencukupi baik pada API1000 maupun VVER1200. Permasalahannya akan jadi lain, bila sistem pendingin yang mensuplai ke dalam reaktor menjadi tidak berfungsi/tidak tersedia (unavailability).*

2. PERTANYAAN: (Ikhsan Khairu R., Mahasiswa UPI - Bandung)

- Apa bahaya eksternal dapat dihilangkan?.

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

- Bahaya eksternal tidak dapat dihilangkan karena sudah melekat pada suatu tapak. Yang dapat dilakukan adalah meminimalkan bahaya eksternal tersebut dengan memilih tapak raktor yang tepat, serta sudah dipertimbangkan dalam desain. Selain itu juga harus sudah dimasukkan dalam manajemen kecelakaan kondisi-kondisi tersebut, terutama dalam menerapkan pertahanan berlapis (defence in depth) level 4.*