View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Badan Tenaga Nuklir Nasional: Jurnal BATAN

J. Tek. Reaktor. Nukl.
Vol. 16 No.3 Oktober 2014, Hal. 134-148
ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012

ANALISIS SKENARIO KEGAGALAN SISTEM UNTUK MENENTUKAN PROBABILITAS KECELAKAAN PARAH AP1000

D. T. Sony Tjahyani, Julwan Hendry Purba
Pusat Teknologi dan Keselamatan Reaktor Nuklir
E-mail: dtsony@batan.go.id; purba-jh@batan.go.id

Diterima editor 27 Agustus 2014
Disetujui untuk publikasi 30 September 2014

ABSTRAK

ANALISIS SKENARIO KEGAGALAN SISTEM UNTUK MENENTUKAN PROBABILITAS KECELAKAAN PARAH AP1000. Kejadian Fukushima telah menunjukkan bahwa kecelakaan parah dapat terjadi, maka dari itu sangatlah penting untuk menganalisis tingkat keselamatan pada reaktor daya. Berdasarkan rekomendasi *expert mission* IAEA setelah kejadian Fukushima, perlu dilakukan upaya untuk meminimalisasi terjadinya kecelakaan parah yaitu dengan melakukan proses pendinginan yang maksimal. Dalam konsep keselamatan fasilitas nuklir, khususnya reaktor daya telah diterapkan konsep keselamatan berlapis (*Defence in Depth, DiD*). Konsep keselamatan tersebut terdiri atas 5 level pertahanan yang bertujuan mencegah dan mengurangi lepasan produk fisi ke masyarakat dan lingkungan pada saat reaktor daya mengalami kecelakaan. Dalam reaktor telah didesain sistem atau tindakan yang mempunyai fungsi untuk mengatasi setiap level tersebut. Tujuan dari analisis ini adalah menentukan probabilitas kecelakaan parah dengan melakukan skenario kegagalan sistem dalam proses pendinginan di reaktor. Sebagai obyek analisis adalah reaktor daya AP1000, karena jenis reaktor ini sedang banyak dibangun saat ini. Skenario dilakukan dengan mengasumsikan beberapa kombinasi kegagalan sistem yang termasuk dalam DiD level 2 dan 3. Kegagalan sistem kemudian dianalisis dengan menggunakan analisis pohon kegagalan berdasarkan perangkat lunak SAPHIRE ver. 6.76. Dari analisis didapatkan probabilitas gagal dari kelompok sistem DiD level 2 dan 3 pada AP1000 masih di bawah batas kriteria dari IAEA yaitu lebih kecil dari 10^{-2}, serta probabilitas kecelakaan parah didapatkan sebesar 6,17 x 10^{-10}. Berdasarkan analisis ini disimpulkan bahwa AP1000 mempunyai tingkat keselamatan yang cukup tinggi, karena melalui skenario kegagalan sistem didapatkan probabilitas kecelakaan parah yang sangat kecil.

Kata kunci: Skenario kegagalan, AP1000, probabilitas, kecelakaan parah

ABSTRACT

ANALYSIS OF SYSTEM FAILURE SCENARIO TO DETERMINE SEVERE ACCIDENT PROBABILITY OF AP1000. *Fukushima accident has shown that severe accident could be occurred, therefore it is important to analyze safety level of nuclear power plants. Based on the recommendations of IAEA expert mission after the Fukushima accident, necessary effort to minimize severe accident by optimizing cooling process. On the safety concept of nuclear facility especially power reactor has been applied defence in depth (DiD) concept. These concept consists of five defense levels which is to prevent and to reduce fission product release to the public and the environment when the power reactor accident happen. On the reactor has been designed system or action that have function to overcome with each those levels. The objective of this paper is to determine severe accident probability by system failure scenario on the cooling process in the reactor. The AP1000 is chosen as the reference plant to be evaluated, because currently this reactor is being built in many countries. The scenario is carried out by combining several system failures included in DiD level 2 and 3. System failure is evaluated by fault tree analysis using SAPHIRE code version 6.76. The analysis results show that the failure probability of system in the DiD level 2 and 3 AP1000 is still below the IAEA criteria limit that is less than 10^{-2}, as well as the probability of severe accident is 6.17 x 10^{-10}. Based on this analysis, it can be concluded that the safety level of AP1000 is high enough, because through system failure scenario is obtained the probability of severe accident is very small.*

Keywords: Failure scenario, AP1000, probability, severe accident

PENDAHULUAN

Didalam filosofi keselamatan instalasi nuklir terutama untuk reaktor, tujuan keselamatan umum yaitu melindungi pekerja, masyarakat dan lingkungan hidup melalui upaya pertahanan yang efektif terhadap bahaya radiasi di fasilitas nuklir. Tujuan keselamatan umum terdiri atas 2 (dua) hal yaitu proteksi radiasi dan keselamatan teknis. Maksud dari tujuan keselamatan teknis adalah mencegah kecelakaan, memastikan dengan kepercayaan tinggi semua kemungkinan kecelakaan telah dipertimbangkan dalam desain serta kecelakaan dengan konsekuensi radiologi yang serius mempunyai probabilitas yang sangat kecil. Untuk mencapai tujuan tersebut, maka diterapkan konsep pertahanan berlapis (*Defence in Depth, DID*) yang terdiri atas 5 (lima) level, yang secara sederhana meliputi pencegahan, mengendalikan operasi abnormal, mengendalikan kecelakaan dasar desain, melakukan manajemen kecelakaan dan tindakan kedaruratan [1, 2]. Maka sesuai dengan tujuan proteksi radiasi diharapkan setiap kejadian sudah dapat diakhiri sampai dengan level ke-3. Apabila tidak berhenti pada level ke-3, maka sesuai dengan tujuan keselamatan teknis dipastikan bahwa kecelakaan yang berpotensi harus mempunyai probabilitas yang kecil.

Kecelakaan parah merupakan suatu kecelakaan yang dihipotesakan dalam desain reaktor dan mempunyai konsekuensi radiologis yang sangat signifikan. Kecelakaan parah disebabkan oleh kejadian awal (*initiating event* level ke-3. Salah satu jenis kejadian awal yang perlu dilakukan analisis adalah kehilangan suplai daya listrik total seperti yang terjadi pada kejadian Fukushima, walaupun penyebab kejadian awal tersebut dipengaruhi oleh) diikuti dengan kegagalan beberapa sistem keselamatan, terutama sistem yang termasuk dalam DiD kejadian eksternal berupa gempa. Dalam analisis keselamatan, kehilangan suplai daya listrik total (*station blackout)* disebabkan kehilangan suplai daya *offsite* diikuti dengan *onsite*.

Dalam teknologi desain reaktor daya, salah satu teknik untuk mengurangi dampak dari kehilangan suplai daya listrik digunakan sistem keselamatan pasif, yaitu sistem yang bekerja tanpa memerlukan masukan atau energi eksternal dan berdasarkan hukum alam, dan/atau energi yang tersimpan dalam sistem. AP1000 (*Advanced Passive Pressurized Water Reactor 1000*) merupakan reaktor jenis PWR (*Pressurized Water Reactor*) yang fitur keselamatan teknis (*Engineered Safety Features, ESFs*) berdasarkan sistem pasif, terutama sistem-sistem yang ditujukan untuk pertahanan berlapis level 3 dan termasuk reaktor daya generasi III^+. Selain itu, saat ini AP1000 merupakan reaktor daya yang mempunyai daya besar (1000 MWe) yang sedang banyak dibangun [3, 4]. Maka dari itu sangatlah penting menganalisis tingkat keselamatan reaktor jenis ini.

Probabilitas kecelakaan parah dapat digunakan sebagai salah satu parameter untuk menentukan tingkat keselamatan atau teknologi suatu reaktor daya. Hal ini dimungkinkan karena secara teori probabilitas, bahwa semakin kecil terjadinya suatu kejadian, menunjukkan semakin banyak tahapan yang dilakukan untuk mencapai kejadian tersebut serta probabilitas gagal setiap tahap juga kecil. Maka dari itu probabilitas gagal suatu kejadian tergantung dari kegagalan setiap tahap atau sistem tersebut. Penentuan probabilitas kecelakaan parah dapat dihitung berdasarkan sistem yang termasuk dalam DiD level 3 tidak berfungsi dalam proses pendinginan. Selain itu pelajaran dari Fukushima menunjukkan bahwa beberapa sistem yang termasuk dalam DiD level 2 atau sistem non-keselamatan pada prinsipnya dapat digunakan untuk mencegah terjadinya kecelakaan parah [5].

Berdasarkan analisis beberapa acuan [6-8], menunjukkan bahwa kontribusi kejadian awal terhadap kerusakan teras sangat bervariasi tergantung dari desain reaktor. Salah satu kejadian awal tersebut adalah kehilangan suplai daya dan kontribusinya termasuk kelompok menengah (10% -15%) dibandingkan dengan kejadian awal lainnya. Namun kejadian Fukushima telah menunjukkan bahwa akibat dari kejadian awal tersebut mempunyai konsekuensi yang besar. Maka dari itu sangat penting menganalisis kehilangan suplai daya listrik terhadap kecelakaan parah pada reaktor daya yang termasuk generasi III^+.

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012

Dalam penelitian sebelumnya telah dilakukan analisis tentang probabilitas gagal sistem yang termasuk dalam DiD level 3 pada AP1000 yaitu sistem yang termasuk dalam kelompok PXS (*Passive Core Cooling System*) [9]. Juga telah dilakukan analisis probabilitas gagal sistem yang termasuk DiD level 2 [10, 11]. Selanjutnya berdasarkan rekomendasi *expert* IAEA dalam pembelajaran kejadian Fukushima disebutkan bahwa dalam kondisi kecelakaan parah, maka semua usaha harus dilakukan untuk melakukan proses pendinginan [5]. Dari hasil tersebut perlu dilakukan analisis lebih lanjut untuk melakukan kemungkinan skenario kegagalan sistem pada proses pendinginan di dalam reaktor.

Tujuan dari penelitian ini adalah menentukan probabilitas kecelakaan parah dengan melakukan skenario kegagalan sistem dalam proses pendinginan di reaktor. Dari hasil ini diharapkan dapat diketahui tingkat keselamatan AP1000. Karena dalam analisis keselamatan sebagai tolok ukur pertama adalah menentukan kejadian awal, maka sebagai kejadian awal yang dipilih dalam analisis ini adalah kehilangan suplai daya listrik. Kejadian awal ini dipilih disebabkan 2 hal yaitu AP1000 merupakan reaktor daya komersial yang menerapkan sistem pasif pada pendingin teras sehingga tidak tergantung adanya suplai daya serta kecelakaan Fukushima disebabkan karena kehilangan suplai daya, walaupun didahului dengan kejadian eksternal adanya gempa bumi. Metoda yang digunakan adalah menentukan probabilitas gagal yang termasuk sistem DiD level 2 dan level 3 dengan analisis pohon kegagalan. Dari hasil probabilitas gagal sistem, selanjutnya dilakukan skenario kegagalan sistem yaitu kombinasi kegagalan dari sistem-sistem tersebut dalam proses pendinginan untuk mencegah kecelakaan parah. Data yang digunakan berdasarkan data kegagalan komponen dari IAEA [12] dan data AP1000 yang sudah dipublikasi [13, 14]. Untuk meningkatkan tingkat keselamatan dalam mencegah atau memperkecil terjadinya kecelakaan parah, juga diusulkan konsep desain untuk cadangan pendingin sebagai buangan panas akhir (*ultimate heat sink*) apabila tangki pendingin internal untuk mengguyur pengungkung tidak berfungsi.

TINJAUAN PUSTAKA

Fungsi Keselamatan Dan Penerapannya Dalam Penentuan Probabilitas Kecelakaan Parah

Setelah terjadinya kecelakaan Fukushima telah dilakukan beberapa penyempurnaan persyaratan keselamatan. Salah satunya adalah penyempurnaan persyaratan dalam fungsi keselamatan dasar. Sesuai dengan persyaratan keselamatan terbaru dalam desain pada PLTN [1], pada semua kondisi *plant* terdapat tiga fungsi keselamatan dasar yang harus dipenuhi. Pertama adalah mengendalikan reaktivitas, kedua memindahkan panas dari reaktor dan penyimpan bahan bakar. Sedangkan ketiga adalah mengungkung bahan radioaktif, menahan radiasi dan mengendalikan lepasan radioaktif yang direncanakan seperti halnya pembatasan lepasan radioaktif yang dihipotesakan (*accidental*). Perubahan yang substansi terlihat pada fungsi keselamatan dasar kedua yaitu pemindahan panas dilakukan untuk gedung reaktor secara umum, sedangkan pada persyaratan keselamatan sebelumnya hanya ditekankan pada teras reaktor.

Sehubungan dengan fungsi keselamatan dasar kedua tersebut, dan berdasarkan pelajaran setelah terjadinya kecelakaan Fukushima yaitu untuk mengefektifkan sistem pendingin yang ada dalam mencegah kecelakaan dasar desain, serta harus juga mengoptimalkan sistem buangan panas akhir, maka perlu dilakukan analisis skenario kegagalan sistem. Salah satu skenario yang digunakan adalah mengefektifkan sistem yang ada.

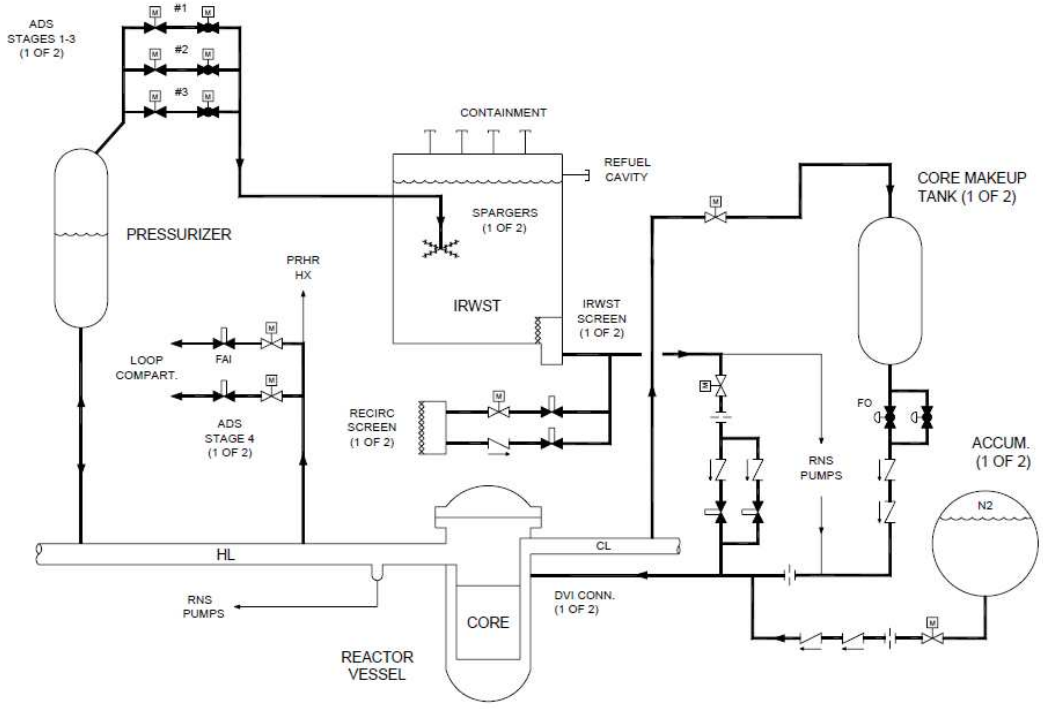
Dalam konsep pertahanan berlapis sudah ditentukan masing-masing sistem yang berfungsi sebagai DiD level 2 dan 3, namun demikian secara probabilistik dapat dilakukan kombinasi fungsi dari sistem-sistem tersebut. Secara teori probabilistik dapat diasumsikan peluang terjadinya kecelakaan disebabkan oleh kejadian awal diikuti dengan kegagalan sistem-sistem/tindakan yang memitigasi dari kejadian awal tersebut. Maka dari itu probabilitas terjadinya suatu kecelakaan dapat diperkecil dengan probabilitas gagal sistem tersebut.

Pada analisis keselamatan, salah satu kejadian awal yang dipertimbangkan adalah kehilangan suplai daya listrik sehingga semua sistem aktif termasuk sistem keselamatan tidak berfungsi. Dalam teknologi reaktor, salah satu strategi dalam mengantisipasi jenis kejadian awal ini adalah dengan menggunakan sistem pasif. Reaktor AP1000, merupakan satu-satunya reaktor daya jenis PWR berdaya besar (3400 MWt) yang semua sistem pendingin terasnya menggunakan sistem pasif termasuk beberapa sistem yang termasuk dalam fitur keselamatan teknis.

Deskripsi Sistem Pendinginan Pada AP1000

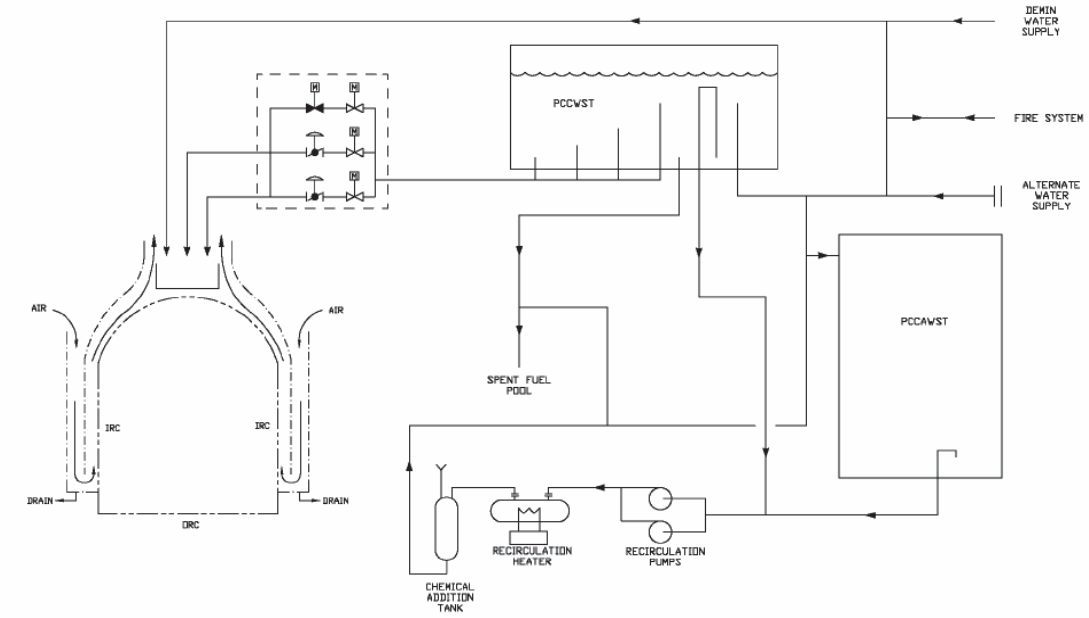
Sistem-sistem pasif pada AP1000 adalah akumulator, tangki *make-up* teras (*Core Make-up Tank*, CMT), sistem pemindah panas sisa secara pasif (*Passive Residual Heat Removal*, PRHR), tangki penyimpan air pengisi dalam pengungkung (*In-containment Refueling Water Storage Tank*, IRWST), sistem depresurisasi otomatik (*Automatic Depressurization System*, ADS), dan sistem pendingin pengungkung secara pasif (*Passive Containment Cooling System*, PCS) [15, 16]. Sistem-sistem tersebut termasuk dalam DiD level 3.

Akumulator digunakan untuk menginjeksi pendingin ke dalam teras pada saat tekanan dalam sistem sudah rendah, sedangkan CMT menginjeksi pada saat tekanan masih tinggi. PRHR mempunyai fungsi memindahkan panas pendingin primer secara sirkulasi alam. IRWST digunakan sebagai buangan panas untuk penukar panas PRHR dan sebagai sumber pendingin untuk injeksi pada saat menggenangi bejana reaktor. ADS berfungsi untuk mengendalikan pengurangan tekanan sistem pendingin primer, sehingga injeksi pendingin ke teras reaktor yang dilakukan oleh sistem yang termasuk dalam kelas keselamatan dan non-keselamatan dapat bekerja secara optimal. PCS berupa bejana besar yang melingkupi sistem suplai uap nuklir ((*nuclear steam supply system*, NSSS) dan semua injeksi keselamatan pasif. Sistem ini berfungsi untuk mengkondensasikan uap sebagai hasil pendidihan dari IRWST pada saat kecelakaan dan juga berfungsi sebagai buangan panas akhir secara pasif dan kontinu karena menggunakan media air dan udara. Sistem keselamatan sistem pasif AP1000 seperti ditunjukkan dalam Gambar 1 dan 2.



Gambar 1. Diagram sistem keselamatan pasif AP1000 [15].

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012



Gambar 2. Diagram alir sistem pendingin pengungkung secara pasif [16].

Konsep sistem pendingin dalam reaktor agar dapat berfungsi secara efektif adalah sistem dapat bekerja pada tekanan tertentu serta berdasarkan persyaratan terbaru dari IAEA, panas peluruhan dan panas sisa yang dipindahkan dari teras reaktor harus juga dikeluarkan dari gedung reaktor. Berdasarkan konsep tersebut, maka beberapa sistem yang termasuk dalam DiD level 2 memungkinkan untuk difungsikan yaitu sistem kendali kimia dan volume (*Chemical and Volume Control System*, CVCS), sistem air umpan *start-up* (*Start-up Feed Water System*, SFWS), sistem pemindah panas sisa secara normal (*Normal Residual Heat Removal System*, RNS).

Pada kondisi kecelakaan, CVCS dapat berfungsi dengan menginjeksi pendingin berupa air boron ke dalam teras reaktor. Sistem ini juga memberikan *spray* bantuan pada *pressurizer*, sehingga dapat berfungsi mengurangi tekanan dalam sistem pendingin reaktor. SFWS berfungsi mensuplai air umpan ke dalam pembangkit uap, apabila sistem air umpan utama tidak berfungsi, sehingga dapat memindahkan panas dari sistem pendingin primer ke sistem pemindah panas. RNS berfungsi memindahkan panas dari teras dan sistem pendingin primer setelah reaktor padam serta memberikan pendinginan pada IRWST. Ketiga sistem tersebut termasuk sistem aktif, sehingga pada saat kehilangan suplai daya listrik memerlukan tindakan operator untuk mengefektifkan kinerja sistem-sistem tersebut.

METODOLOGI

Untuk mendapatkan proses pendinginan yang efektif dalam mencegah terjadinya kecelakaan parah, perlu dilakukan pengaturan tekanan dalam sistem dan kinerja sistem keselamatan untuk menginjeksi pendingin dalam memindahkan panas. Maka dilakukan skenario kombinasi sistem untuk memenuhi fungsi tersebut. Probabilitas kecelakaan parah akibat kehilangan suplai daya listrik diasumsikan karena 5 (lima) tahap rekayasa sistem terjadi dengan asumsi logika "AND" seperti ditunjukkan dalam Gambar 3. Dalam logika ini mengasumsikan bahwa kejadian yang dihipotesakan terjadi apabila semua tahap yang terjadi. Setiap tahap kegagalan disebabkan oleh satu atau lebih dari kombinasi kegagalan sistem sehingga berlaku logika "OR".

Kegagalan tahap pertama mengasumsikan fungsi sistem yang termasuk dalam non-keselamatan gagal dalam menginjeksikan pendingin ke teras reaktor atau ke pembangkit uap. Kegagalan tahap kedua mengasumsikan semua sistem DiD level 3 yang digunakan dalam analisis deterministik

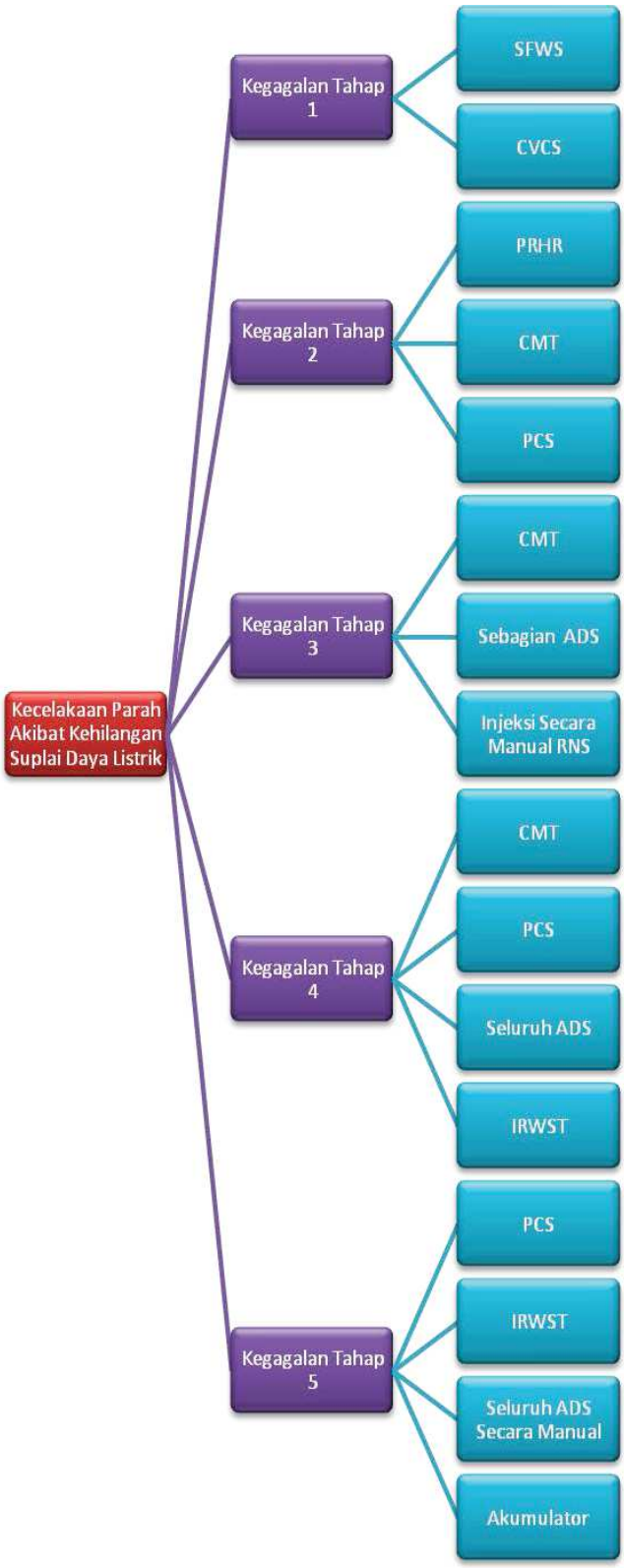
mengalami kegagalan. Kegagalan tahap ketiga mengasumsikan kegagalan yang dipengaruhi oleh 3 sistem yaitu injeksi pendingin ke teras reaktor menggunakan CMT, buangan panas dilakukan secara manual (operator), serta sebagian ADS untuk mengefektifkan kinerja RNS. Kegagalan tahap keempat mengasumsikan kegagalan yang identik dengan kegagalan tahap kedua namun buangan panas menggunakan IRWST sehingga diperlukan juga penggunaan seluruh ADS. Kegagalan kelima mengasumsikan kegagalan seperti kegagalan tahap keempat namun injeksi pendingin ke teras reaktor dilakukan dengan akumulator sehingga perlu penggunaan ADS secara manual (tindakan operator).

Dari asumsi tersebut, selanjutnya dilakukan langkah perhitungan seperti ditunjukkan dalam Gambar 4. Sebagai langkah pertama dilakukan penyusunan analisis pohon kegagalan (*Fault Tree Analysis*) untuk sistem SFWS, CVCS, PRHR, CMT, Akumulator, PCS, sebagian ADS, seluruh ADS, RNS, dan IRWST. Dari analisis pohon kegagalan ini, akan didapatkan probabilitas kejadian puncak (*top event*) dan probabilitas *minimal cutset*. Selanjutnya dilakukan perhitungan probabilitas gagal sistem dengan menggunakan data kegagalan komponen dari IAEA serta beberapa data kegagalan komponen berdasarkan data AP1000 yang sudah dipublikasi [12-14]. Dari hasil probabilitas gagal sistem, selanjutnya dilakukan perhitungan gagal tahap 1, 2, 3, 4 dan 5 sebagai kombinasi probabilitas gagal sistem dan akhirnya ditentukan probabilitas kecelakaan parah sebagai hasil kegagalan kelima tahap tersebut. Sebagai analisis sensitivitas dilakukan pendekatan bahwa setiap kegagalan sistem sebagai kejadian dasar (*basic event*) dari kecelakaan parah, sehingga dapat diketahui sistem yang sangat berpengaruh dalam kecelakaan parah.

Dalam menyusun analisis pohon kegagalan serta menentukan probabilitas gagal digunakan perangkat lunak SAPHIRE Ver. 6.76 (*Systems Analysis Programs for Hands-on Integrated Reliability Evaluations*). Salah satu kegunaan dari perangkat lunak ini adalah dapat menampilkan minimal *cutset* yaitu kombinasi terkecil kejadian dasar yang apabila muncul akan terjadi kejadian puncak (*Top Event*).

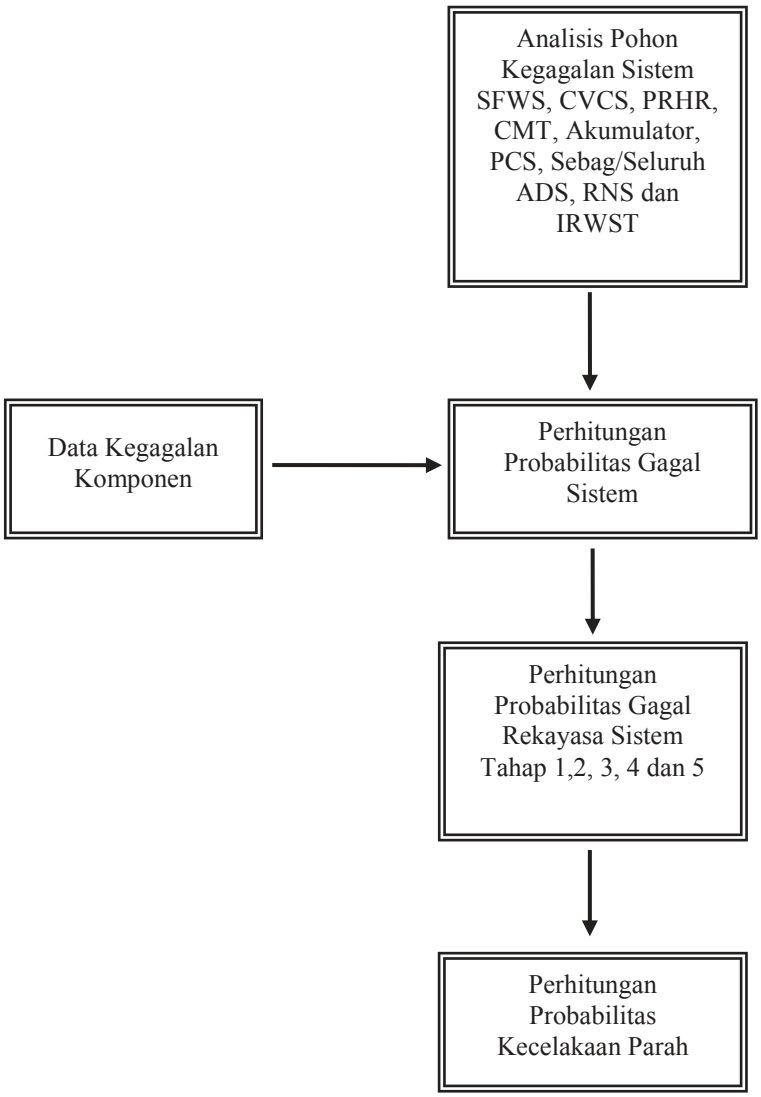
Sebagai usaha memperkecil probabilitas kecelakaan parah juga diusulkan inovasi rekayasa sistem terhadap persediaan pendingin alternatif untuk mengguyur pengungkung (*containment*). Konsep desain yang diusulkan harus berdasarkan prinsip sistem keselamatan antara lain keragaman (*diversity*), redundansi, mandiri dan pasif.

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012



Keterangan:
SFWS = *Start-up Feedwater System*
CVCS = *Chemical and Volume Control System*
PRHR = *Passive Residual Heat Removal*
CMT = *Core Make-up Tank*
PCS = *Passive Containment Cooling System*
ADS = *Automatic Depressurization System*
RNS = *Normal Residual Heat Removal System*
IRWST = *In-Containment Refueling Water Storage Tank*

Gambar 3. Tahapan penentuan probabilitas kecelakaan parah berdasarkan skenario kegagalan sistem.



Gambar 4. Langkah perhitungan probabilitas kecelakaan parah.

HASIL DAN PEMBAHASAN

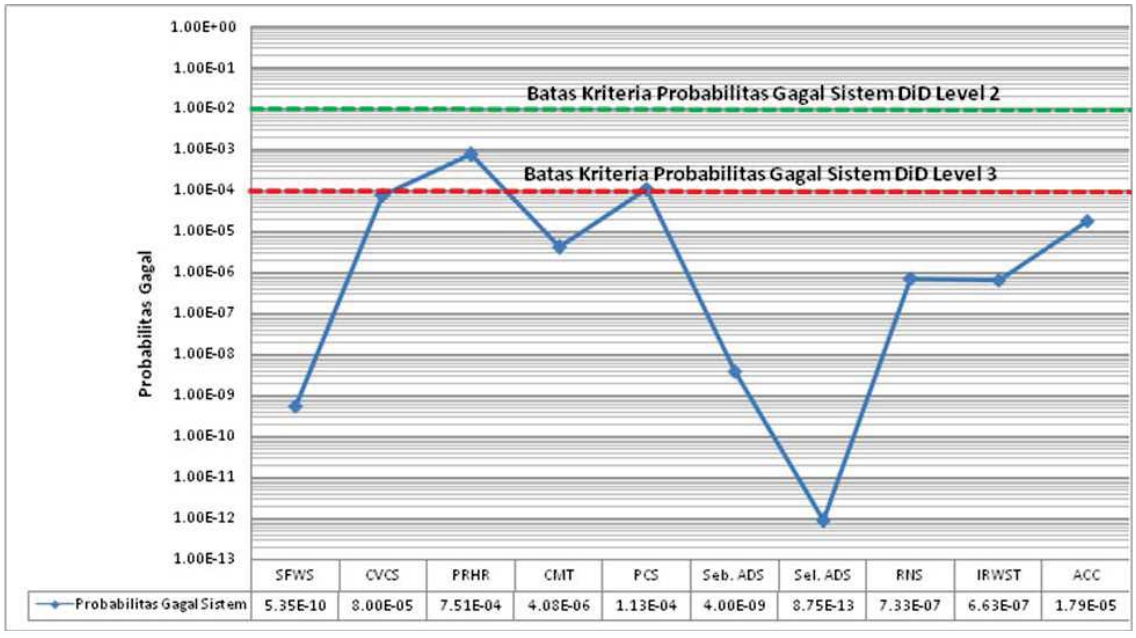
Analisis Kegagalan Sistem

Dari analisis pohon kegagalan didapatkan hasil perhitungan probabilitas gagal untuk setiap sistem yang berkontribusi terhadap kecelakaan parah seperti ditunjukkan dalam Gambar 5. Dari gambar tersebut terlihat bahwa probabilitas gagal untuk sistem yang berfungsi sebagai DiD level 2 (SFWS, CVCS dan RNS) pada AP1000 jauh dari kriteria yang ditentukan oleh pedoman IAEA yaitu lebih besar sama dengan dari 10^{-2}[17]. Kriteria ini mempunyai batas toleransi yang agak longgar dikarenakan sistem-sistem tersebut termasuk klasifikasi non-keselamatan. Berdasarkan perhitungan menunjukkan jauh lebih kecil dari batas minimal tersebut (lebih kecil dari faktor 8 x 10^{-3}). Hal ini menunjukan bahwa pada AP1000, umumnya sistem yang termasuk dalam DiD level 2 mempunyai tingkat keandalan yang cukup tinggi, walaupun sistem-sistem tersebut termasuk dalam kelompok sistem aktif dan termasuk kategori non-keselamatan. Sesuai dengan konsep keselamatan fungsi dari sistem tersebut adalah mengembalikan kondisi abnormal menjadi normal pada saat operasi.

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012

Dari Gambar 5 tersebut juga menunjukkan bahwa dari kelompok DiD level 2 terlihat probabilitas gagal CVCS mempunyai probabilitas yang lebih besar bila dibandingkan dengan SFWS dan RNS. Hal ini disebabkan karena *minimal cut set* terbesar pada CVCS terdiri atas 1 kejadian dasar, sedangkan pada SFWS dan RNS terdiri atas 2 kejadian dasar. Seperti diketahui bahwa *minimal cutset* adalah kombinasi terkecil dari kejadian dasar yang apabila muncul akan menimbulkan kegagalan sistem. Maka dari itu, untuk *minimal cutset* yang terdiri lebih dari 1 kejadian dasar akan membuat probabilitas gagal sistem tersebut menjadi kecil. Apabila dianalisis lebih lanjut, probabilitas gagal CVCS dapat lebih diperkecil lagi, dengan beberapa katup (5 katup) harus dipasang secara redundansi, sehingga probabilitas total CVCS akan mengecil. Namun demikian, tanpa penambahan tersebut sebenarnya probabilitas gagal CVCS sudah jauh dari batas kriteria seperti ditunjukkan dalam Gambar 5.

Bila dibandingkan antara SFWS dan RNS, SFWS lebih andal karena mempunyai probabilitas gagal yang kecil, hal ini disebabkan probabilitas *minimal cutset* pada SFWS mempunyai kontribusi yang lebih merata terhadap kejadian puncak (*top event*), sedangkan pada RNS mempunyai kontribusi probabilitas *minimal cutset* yang tidak merata yaitu *minimal cutset* pertama mempunyai kontribusi yang sangat besar terhadap kejadian puncak, walaupun kontribusi *minimal cutset* berikutnya kecil. Karena *minimal cutset* terdiri atas kombinasi kejadian dasar, maka salah satu cara untuk memperkecil probabilitas gagal sistem pada RNS dapat dilakukan dengan memperkecil probabilitas kejadian dasar.



Gambar 5. Probabilitas gagal sistem yang berkontribusi dalam mencegah kecelakaan parah.

Sistem yang termasuk dalam DiD level 3 juga masih dalam batas pedoman IAEA yaitu diantara 10^{-2} sampai dengan 10^{-4}, bahkan dari Gambar 5 terlihat bahwa probabilitas gagalnya jauh lebih kecil dari batas minimal 10^{-4}, kecuali untuk PRHR dan PCS. Probabilitas gagal PRHR kelihatan menonjol, dikarenakan dalam analisis pohon kegagalan digunakan asumsi yang sangat konservatif yaitu pada kegagalan PRHR dimasukkan kejadian dasar tersumbatnya tabung (*tube*) PRHR. Secara deterministik, perhitungan tersumbatnya tabung yang dapat diklasifikasikan sebagai kegagalan dalam pendinginan berdasarkan sejumlah tabung yang tersumbat, sedangkan dalam analisis probabilistik ini, tersumbatnya 1 tabung PRHR sudah dianggap gagal. Sedangkan untuk PCS, kejadian yang mempunyai kontribusi terbesar menyebabkan kegagalan kegagalan sistem adalah sistem aktuasi. Kejadian ini merupakan hal

yang penting, karena dalam PCS kegagalan sistem aktuasi akan menyebabkan air dalam tangki tidak dapat mengguyur pengungkung.

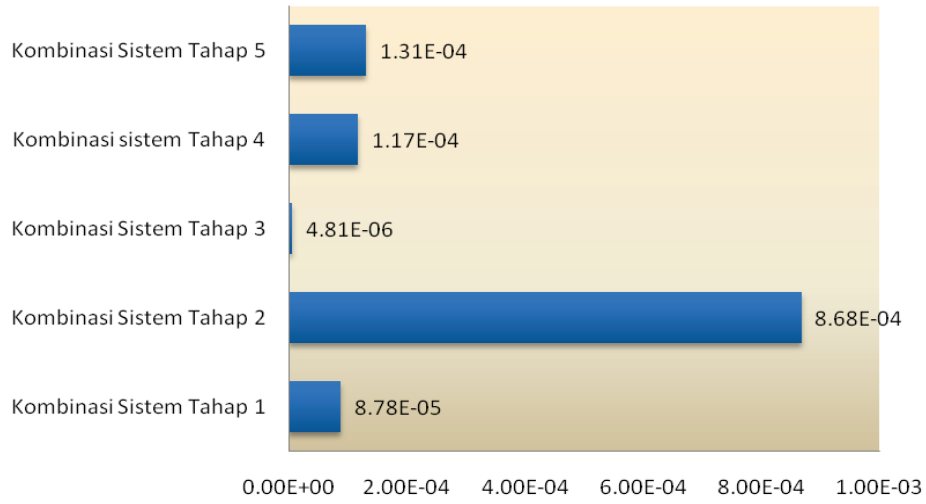
Berdasarkan nilai probabilitas ini menunjukkan bahwa pada AP1000, sistem yang termasuk dalam DiD level 3 dan berdasarkan prinsip sistem pasif mempunyai tingkat keandalan yang tinggi, karena mempunyai probabilitas gagal yang kecil. Seperti terlihat dalam Gambar 5, sistem yang mempunyai probabilitas terkecil yang termasuk dalam kelompok DiD level 3 adalah ADS sebesar 8,75 x 10^{-13}. Hal ini disebabkan ADS terdiri atas 4 redundansi dan *minimal cutset* terbesar terdiri atas 7 kejadian dasar, sedangkan untuk sistem yang lain mempunyai *minimal cutset* terbesar antara 1 sampai dengan 6 kejadian dasar.

Skenario Sistem Dalam Mencegah Kecelakaan Parah

Seperti diuraikan dalam metodologi, kecelakaan parah terjadi apabila semua rekayasa kombinasi sistem yang terdiri atas 5 tahap kombinasi sistem tersebut mengalami kegagalan. Dari hasil perhitungan didapatkan probabilitas terjadinya kecelakaan parah sebesar 6,17 x 10^{-10}, dengan probabilitas gagal untuk setiap tahap kombinasi sistem seperti ditunjukkan dalam Gambar 6. Apabila dilakukan validasi dengan membandingkan acuan dari analisis yang dilakukan Westinghouse pada kejadian awal yang sama [18, 19], didapatkan probabilitas kecelakaan parah untuk AP 1000 dan AP 600 masing-masing 9,6 x 10^{-10} dan 1 x 10^{-9} (≈ 10 x 10^{-10}). Maka dapat dikatakan hasil analisis lebih kecil dari analisis Westinghouse, walaupun secara probabilistik menunjukkan perbedaan yang tidak terlalu besar karena mempunyai orde yang sama yaitu 10^{-10}. Demikian pula bila divalidasi dengan PWR generasi III^{+} lainnya (EPR, US-APWR dan US-EPR) menunjukkan hasil yang lebih kecil pula [6, 20, 21], karena hasil probabilitas kecelakaan parah pada tipe reaktor tersebut masing-masing sebesar 1,4 x 10^{-9}; 5,8 x 10^{-7} dan 1,5 x 10^{-7}. Hasil yang diperoleh lebih kecil bila dibandingkan dengan analisis dari Westinghouse dan PWR generasi III^{+} lainnya, karena dalam analisis ini digunakan pendekatan yang konservatif. Hasil analisis sangat kecil bila dibandingkan dengan EPR, US-APWR dan US-EPR, karena ketiga tipe reaktor tersebut termasuk tipe PWR aktif. Dengan demikian pemodelan yang disusun (analisis pohon kegagalan) mendekati dengan analisis yang dilakukan oleh Westinghouse. Perbedaan yang terjadi kemungkinan disebabkan oleh penyusunan model pohon kegagalan dalam penentuan kejadian dasar yang dipilih dan beberapa data kegagalan komponen yang digunakan. Namun demikian, beberapa kejadian dasar yang muncul adalah sama antara hasil analisis dan model yang dilakukan Westinghouse.

Dari Gambar 6 tersebut terlihat semua tahap mempunyai probabilitas gagal yang cukup kecil, dan terjadinya kecelakaan parah terjadi apabila seluruh tahap kombinasi sistem mengalami kegagalan, sehingga hal ini akan berdampak pula terhadap probabilitas terjadinya kecelakaan parah juga akan menjadi kecil. Dari Gambar 6 terlihat bahwa bahwa probabilitas gagal terbesar adalah 8,6 x 10^{-4} dan terjadi pada kombinasi sistem tahap 2 yang terdiri atas PRHR, CMT atau PCS. Walaupun mempunyai probabilitas yang diklasifikasikan kecil, namun harus mendapat perhatian lebih untuk meningkatkan keandalan ketiga sistem tersebut. Hal ini juga sesuai dengan analisis deterministik, karena ketiga sistem tersebut yang diskenariokan dalam sekuensi kecelakaan. Secara probabilistik, kontribusi terbesar dari penyebab kegagalan tahap ini adalah probabilitas gagal PRHR. Untuk pengembangan analisis lebih lanjut dapat dilakukan analisis mengenai kinerja PRHR yaitu dengan mencoba beberapa kegagalan komponen yang mempunyai dampak besar terhadap kegagalan sistem dalam memindahkan panas, baik secara deterministik maupun eksperimental. Dari hasil tersebut dapat dilakukan sebagai validasi dalam penyusunan analisis pohon kegagalan yaitu dalam menentukan kejadian dasar yang dipilih.

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012



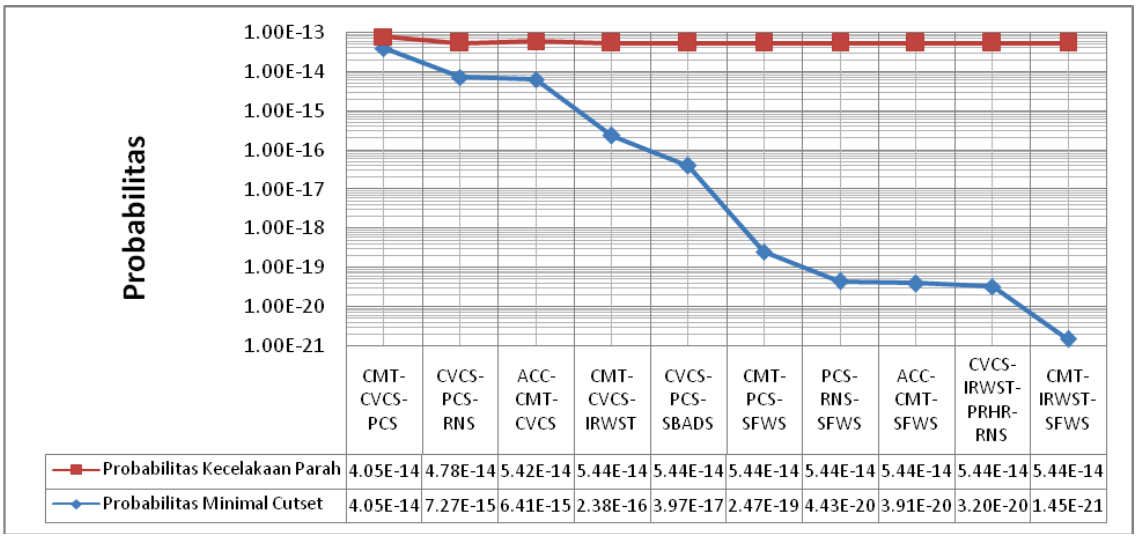
Gambar 6. Probabilitas gagal setiap tahap kombinasi sistem.

Bila diasumsikan sampai dengan tahap kombinasi sistem kedua diharapkan sistem sudah harus mampu mencegah terjadinya kecelakaan parah, hal ini sesuai dengan kriteria pehitungan deterministik, maka probabilitas kecelakaan parah adalah sebesar 7,62 x 10^{-8}. Bila dibandingkan dengan semua kegagalan tahap 1 sampai dengan tahap 5, maka dengan adanya kombinasi sistem, probabilitas terjadinya kecelakaan parah akan mengecil 1,24 x 10^{2} kali atau terdapat faktor pengecilan sebesar 8,10 x 10^{-3}. Atau bila menggunakan asumsi skenario yang digunakan secara analisis deterministik, yaitu sistem-sistem yang digunakan untuk mencegah kecelakaan dasar desain hanya sistem yang sesuai dengan DiD level 3 karena sistem yang digunakan dalam rekayasa sistem tahap 1 mempunyai fungsi mengembalikan kejadian abnormal menjadi normal, maka akan didapatkan faktor pengecilan sebesar 7,11 x 10^{-7}.

Dalam gambar tersebut juga terlihat bahwa probabilitas gagal terkecil adalah tahap kombinasi sistem ketiga yaitu 4,81 x 10^{-6} yang terdiri dari kegagalan sistem CMT, sebagian ADS atau RNS. Sebagai kontribusi terbesar *minimal cutset* dari kejadian dasar yang termasuk dari sistem CMT dan hal ini sesuai dengan Gambar 5, CMT mempunyai probabilitas gagal terbesar diantara ke-3 sistem tersebut.

Analisis Sensitivitas Probabilitas Kecelakaan Parah

Apabila diasumsikan probabilitas gagal setiap sistem dalam mencegah kecelakaan parah sebagai kejadian dasar, maka diperoleh probabilitas kecelakaan parah sebesar 5,44 x 10^{-14} dengan *minimal cutset* seperti ditunjukkan dalam Gambar 7. Probabilitas kecelakaan parah merupakan jumlah dari probabilitas setiap *minimal cutset*. Dari hasil tersebut terlihat bila setiap sistem diasumsikan sebagai kejadian dasar, maka membuktikan bahwa terjadinya kecelakaan parah cukup kecil. Hal ini ditunjukkan dengan setiap *minimal cutset* terdiri atas 3 (tiga) kejadian dasar dan minimal *cutset* pertama mempunyai probabilitas sangat kecil yaitu sebesar 4,05 x 10^{-14} dan *minimal cutset* berikutnya semakin kecil.



Gambar 7. Hasil perhitungan probabilitas kecelakaan parah dengan asumsi kegagalan sistem sebagai kejadian dasar (*basic event*).

Dari Gambar 7 terlihat bahwa kontribusi terbesar terhadap kecelakaan parah adalah *minimal cutset* pertama sampai dengan ketiga yaitu masing-masing sebesar 74%, 13% dan 12%, dan *minimal cutset* lainnya lebih kecil dari 1%. Dari ketiga *minimal cutset* yang mempunyai kontribusi terbesar tersebut, modus dari sistem yang termasuk dalam DiD level 2 adalah CVCS, sedangkan modus yang termasuk dalam DiD level 3 adalah PCS dan CMT, hal ini juga sesuai dengan analisis setiap sistem seperti ditunjukkan dalam Gambar 5 menunjukkan CVCS, PCS dan CMT mempunyai probabilitas gagal yang besar. Dari hasil analisis ini dihubungkan dengan probabilitas gagal setiap kombinasi sistem (Gambar 6) serta sekuensi kecelakaan pada analisis deterministik, maka sistem CMT dan PCS harus mempunyai tingkat keandalan yang tinggi. Secara rekayasa sistem untuk meningkatkan keandalan fungsi dari kedua sistem tersebut, PCS akan lebih mudah dibandingkan CMT. Hal ini disebabkan CMT berhubungan dengan bejana tekan reaktor yaitu pada bagian lengan dingin (*cold leg*) dan DVI (*direct vessel injection*), sedangkan PCS di bagian luar reaktor yaitu pada posisi pengungkung, sehingga dapat dilakukan rekayasa atau inovasi lebih lanjut untuk meningkatkan fungsi ketersediaannya.

Dari Gambar 7 juga terlihat bahwa *minimal cutset* yang mengandung kejadian dasar PRHR terjadi pada *minimal cutset* kesembilan yang berarti sangat kecil kontribusinya terhadap kejadian puncak. Namun demikian bila dibandingkan dengan Gambar 5, PRHR mempunyai probabilitas yang cukup besar. Hal ini disebabkan PRHR muncul bergabung dengan 3 kejadian dasar (sistem) yang lain, sehingga menghasilkan probabilitas yang sangat kecil, dan dapat dianggap PRHR mempunyai peran yang tidak signifikan. Namun demikian karena analisis probabilistik melengkapi analisis deterministik, maka setiap kombinasi sistem yang perlu mendapat perhatian sebaiknya dianalisis lebih lanjut secara deterministik.

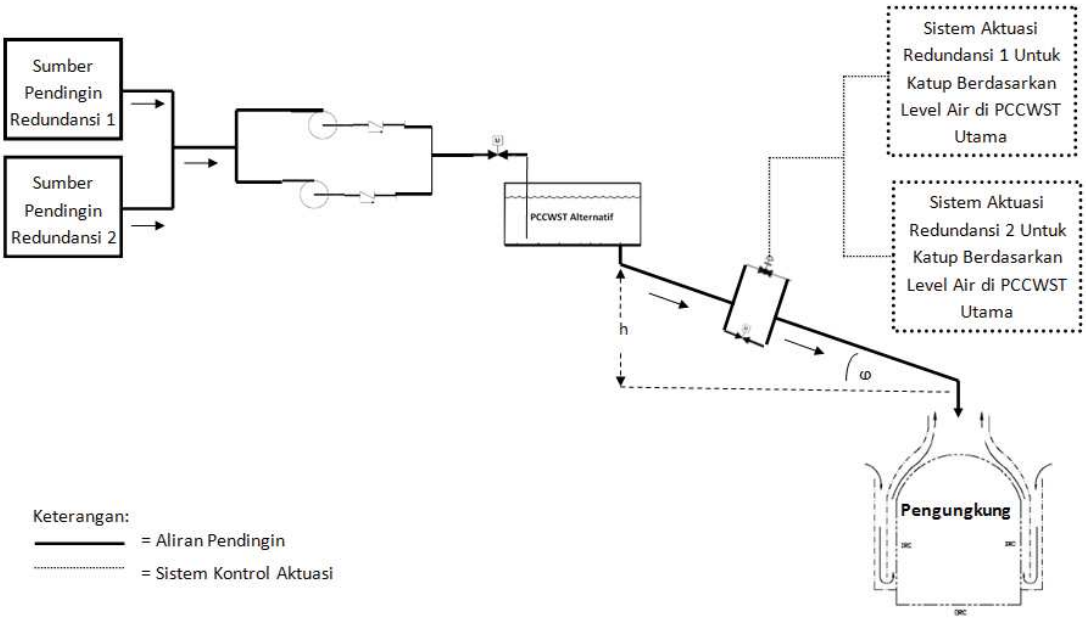
Inovasi Rekayasa Sistem Untuk Memperkecil Probabilitas Kecelakaan Parah

PCS secara teknis merupakan pembuangan panas akhir (*ultimate heat sink*), dan seperti terlihat dalam Gambar 7, hasil analisis menunjukkan dari 7 (tujuh) *minimal cut set* pertama yang berkontribusi terhadap probabilitas kecelakaan parah, 5 (lima) *minimal cut set* selalu terdapat kejadian dasar PCS. Hal ini berarti PCS merupakan salah satu sistem yang sangat signifikan dalam mencegah kecelakaan parah. Selain itu berdasarkan beberapa analisis peneliti lainnya menunjukkan walaupun pendinginan pengungkung dilakukan secara sirkulasi alam dengan 2 (dua) cara yaitu dengan perantara udara atau air, akan tetapi unjuk kerja PCS akan efektif apabila pendinginan dilakukan dengan air [22]. Dalam hal

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012

ini, yang dapat dilakukan untuk meningkatkan kinerja PCS dalam kaitannya dengan analisis probabilistik adalah menyediakan cadangan pendingin yang cukup. Pada PCS terdapat 1 sumber pendingin yaitu pendingin tangki utama (*passive containment cooling water storage tank,* PCCWST), dan tangki cadangan yaitu *passive containment cooling ancillary water storage tank* (PCCAWST). Serta sumber pendingin lainnya yang diambil dari alih fungsi sistem lainnya yaitu *demineralized water storage tank, fire protection water storage tank (FPWST),* dan *service water tank* (SWT). Maka dari itu secara konsep keandalan sistem, prinsip redundansi sudah terpenuhi karena terdiri atas 4 (empat) tangki cadangan.

Namun demikian, pada kondisi kejadian eksternal (*external event*) yang dipengaruhi dari alam yang sangat ekstrim, dimungkinkan jumlah pendingin yang berada di tangki PCS akan mengalami gangguan. Pada kondisi ini dimungkinkan 4 tangki cadangan lainnya tidak dapat dioperasikan, karena memerlukan tindakan operator serta pendingin pada tangki cadangan tersebut dapat digunakan apabila dialirkan melalui tangki utama (PCCWST) terlebih dahulu. Berdasarkan hal tersebut, diusulkan suatu inovasi rekayasa sistem adanya persediaan pendingin yang terletak di luar reaktor dan sesuai dengan konsep keselamatan yaitu penambahan tangki cadangan tersebut harus berprinsip pada keterpisahan (*physical separation*), mandiri (*independent*), redundansi dan pasif, seperti ditunjukkan dalam Gambar 8.



Gambar 8. Rekayasa sistem yang diusulkan untuk memperkecil probabilitas kegagalan pendinginan pada PCS.

Secara konsep desain, komponen yang diusulkan adalah terdiri atas sumber pendingin, pompa, katup, tangki penampung berfungsi sebagai PCCWST alternatif, sistem kontrol untuk mengaktuasi pendingin beroperasi secara pasif (2 redundansi), dan *nozzle* untuk mengguyur pengungkung. Sesuai dengan prinsip keterpisahan, maka PCCWST alternatif diletakkan diluar *nuclear island*. Sedangkan secara mandiri, komponen/sistem yang digunakan tidak ada satupun yang juga digunakan bersamaan dengan sistem lainnya. Prinsip pasif diperoleh dengan meletakkan PCCWST alternatif pada posisi yang lebih tinggi dari pengungkung tetapi tidak tepat di atas pengungkung, sehingga pendingin dapat mengalir secara sirkulasi alam karena faktor gravitasi dengan optimal. Dalam hal ini, faktor yang sangat penting adalah tinggi PCCWST alternatif terhadap pengungkung (h) atau sudut kemiringan (φ) posisi PCCWST alternatif terhadap pengungkung. Aktuasi aliran secara pasif dilakukan dengan

membukanya katup yang dioperasikan berdasarkan perubahan level air atau parameter lainnya di PCCWST utama.

Bila dihubungkan dengan tapak yang dipilih, maka posisi PCCWST alternatif dapat diletakkan pada dataran yang lebih tinggi (perbukitan), sehingga tidak memerlukan pondasi khusus untuk meletakkan PCCWST alternatif tersebut. Sedangkan prinsip redundansi diperoleh dengan setiap komponen yang penting terdiri atas 2 unit. Dengan rekayasa sistem yang diusulkan ini, diharapkan secara kualitatif akan mengurangi probabilitas gagal untuk fungsi PCS. Namun demikian secara kuantitatif perlu dilakukan analisis probabilistik dan deterministik (eksperimental). Analisis deterministik maupun eksperimen terutama diperlukan untuk mendapatkan faktor ketinggian atau sudut kemiringan pipa yang optimal sehingga diperoleh keluaran *nozel* merupakan lapisan air dengan ketipisan tertentu. Pada kondisi ini diharapkan akan diperoleh proses pendinginan yang optimal serta lamanya air mengalir untuk mengguyur secara maksimal.

KESIMPULAN

Telah dilakukan analisis skenario kegagalan sistem pada AP1000 untuk menentukan probabilitas kecelakaan parah yaitu dengan melakukan kombinasi beberapa kegagalan sistem yang termasuk dalam DiD level 2 dan 3. Dari analisis dapat disimpulkan bahwa probabilitas gagal untuk sistem yang termasuk dalam DiD level 2 dan 3 masih di bawah batas kriteria dari IAEA, serta probabilitas kecelakaan parah didapatkan sebesar $6{,}17 \times 10^{-10}$. Maka dapat dikatakan bahwa AP1000 mempunyai tingkat keselamatan yang cukup tinggi, karena melalui skenario kegagalan sistem didapatkan probabilitas kecelakaan parah sangat kecil. Dari analisis juga diusulkan konsep inovasi pendinginan untuk sungkup yang memenuhi peryaratan keterpisahan, mandiri, redundansi, dan pasif, sehingga secara keseluruhan semakin memperkecil terjadinya kecelakaan parah dikarenakan kejadian eksternal.

DAFTAR PUSTAKA

1. International Atomic Energy Agency. Safety of Nuclear Power Plant: Design, SSR-2/1, IAEA, Vienna; 2012, 3-12.
2. Kementrian Hukum Dan HAM RI. Keselamatan dan keamanan instalasi nuklir. Peraturan Pemerintah No. 54 Tahun 2012; 2014, 22-27.
3. World Nuclear News, Chinese AP1000 Containment Capped, 2013. Available from: URL: http://www.world-nuclear-news.org. Accessed 26 Agustus 2013.
4. World Nuclear News. Construction Officially Starts at Summer, 2013. Available from: URL: http://www.world-nuclear-news.org. Accessed 26 Agustus 2013.
5. IAEA Mission Report. IAEA international fact finding expert mission of the Fukushima Dai-ichi NPP accident following the great east Japan Earthquake and Tsunami, IAEA. Vienna; 2011: 13-18.
6. Wenisch A., Hirsch H., Kromp R., Mraz G., NPP Loviisa-3: Expert Statement to the EIA Report, Umweltbundesamt GmbH, Vienna; 2008, 15-30.
7. Cillik I., Vrtik L. PSA analysis focused on Mochovce NPP safety measures evaluation from operational safety point of view. International Conference Nuclear Energy in Central Europe; 2001; 305:1-8 .
8. Yang J. Development of an integrated risk assessment framework for internal/external and all power modes. Nuclear Engineering And Technology. 2014: 459-470.

ISSN 1411–240X
Nomor : 402/AU2/P2MI-LIPI/04/2012

9. Sony Tjahyani D. T., Ekariansyah A. S. Analisis probabilistik kecelakaan parah PWR sistem pasif untuk meningkatkan manajemen kecelakaan. Prosiding Seminar Nasional SDM Teknologi Nuklir, BATAN, Yogyakarta; 2012, 31-36.
10. Sony Tjahyani D. T. Analisis keandalan sistem non-keselamatan dalam memperkecil probabilitas kecelakaan parah AP1000. Prosidng Seminar Nasional Pengembangan Energi Nuklir VI, Jakarta; 2013, 311-319.
11. Sony Tjahyani D. T. Analisis probabilistik terhadap modifikasi sistem untuk meningkatkan keselamatan pada reaktor daya AP1000. Prosiding Pertemuan dan Presentasi Ilmiah Penelitian Dasar Ilmu Pengetahuan Dan Teknologi Nuklir; 2013, 219-225.
12. International Atomic Energy Agency. Component reliability data for use in probabilistic safety assessment. TECDOC-478, IAEA, Vienna; 1988, 95-297.
13. Westinghouse Electric Company LLC. AP1000 Pre-construction safety report, UKP-GW-GL-732, Pittsburgh; 2008, 190-230.
14. Westinghouse Electric Company. AP1000 probabilistic risk assessment, Pittsburgh. 2007; 8:1-11.7.
15. United State Nuclear Regulatory Commission. Passive core cooling system-AP1000 technology: Chapter 4, Human Resources Training & Development; 2010, 1-36.
16. Westinghouse. Passive safety system and timeline for station blackout, 2012. Available from: URL: http://www.ukap1000application.com. Accessed 27 Agustus 2012.
17. International Atomic Energy Agency. Deterministic safety analysis for nuclear power plant. SSG-2, Vienna; 2009, 7-12.
18. Matzie R., Goossen, J. How will the new plants be built. Westinghouse Electric Company LLC; 2008, 36-37.
19. Sterdis A. AP1000 regulatory overview. Westinghouse Electric Company LLC; 2007, 102-105.
20. Mitsubishi Heavy Industries. Probabilistic risk assessment and severe accident evaluation; 2008, 19.1.146-171.
21. Areva. US EPR final safety analysis report: Probabilistic Risk Assessment and Severe Accident; 2006, 19.1.180-196.
22. Sofrany A., Susyadi E., Widodo S. Pemodelan sistem pendingin sungkup secara pasif menggunakan RELAP5. Jurnal Teknologi Reaktor Nuklir Tri Dasa Mega. 2012; 14(3):137-145.