BERITA NEGARA REPUBLIK INDONESIA

No.535, 2011 BADAN PENGAWAS TENAGA NUKLIR. Desain Reaktor Daya. Ketentuan Keselamatan.

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

REPUBLIK INDONESIA

NOMOR 3 TAHUN 2011

TENTANG

KETENTUAN KESELAMATAN DESAIN REAKTOR DAYA

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN PENGAWAS TENAGA NUKLIR REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 12 ayat (3) Peraturan Pemerintah Nomor 43 Tahun 2006 tentang Perizinan Reaktor Nuklir perlu menetapkan Peraturan Kepala Badan Pengawas Tenaga Nuklir tentang Ketentuan Keselamatan Desain Reaktor Daya;

Mengingat :

1. Undang-Undang Nomor 10 Tahun 1997 tentang Ketenaganukliran (Lembaran Negara Republik Indonesia Tahun 1997 Nomor 23, Tambahan Lembaran Negara Republik Indonesia Nomor 3676);
2. Peraturan Pemerintah Nomor 43 tahun 2006 tentang Perizinan Reaktor Nuklir (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 106, Tambahan Lembaran Negara Republik Indonesia Nomor 4668);
3. Peraturan Pemerintah Nomor 33 tahun 2007 tentang Keselamatan Radiasi Pengion dan Keamanan Sumber Radioaktif (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 74, Tambahan Lembaran Negara Republik Indonesia Nomor 4730);

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR TENTANG KETENTUAN KESELAMATAN DESAIN REAKTOR DAYA.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Kepala ini yang dimaksud dengan :

1. Reaktor daya adalah reaktor nuklir berupa pembangkit tenaga nuklir yang memanfaatkan energi panas untuk pembangkitan daya baik untuk kepentingan komersial maupun nonkomersial.
2. Konstruksi adalah kegiatan membangun reaktor nuklir di tapak yang sudah ditentukan, mulai dari persiapan atau pengecoran pertama pondasi sampai dengan pemasangan dan surveilan komponen reaktor beserta sistem penunjang hingga teras reaktor tersebut siap diisi dengan bahan bakar nuklir.
3. Kejadian Awal Terpostulasi (*postulated initiating event*) yang selanjutnya disingkat PIE adalah kejadian yang teridentifikasi pada desain yang menimbulkan kejadian operasional terantisipasi atau kondisi kecelakaan dan ancaman terhadap fungsi keselamatan.
4. Batasan dan Kondisi Operasi, yang selanjutnya disingkat BKO, adalah seperangkat aturan yang menetapkan batasan parameter, kemampuan fungsi dan tingkat kinerja peralatan dan petugas yang disetujui oleh Kepala BAPETEN untuk mengoperasikan reaktor daya secara selamat.
5. Operasi Normal adalah operasi di dalam BKO yang ditentukan.
6. Kejadian Operasi Terantisipasi (*anticipated operational occurrences*) yang selanjutnya disingkat AOO adalah proses yang menyimpang dari operasi normal yang diperkirakan terjadi paling tidak satu kali selama umur operasi instalasi, tetapi menurut pertimbangan desain tidak menyebabkan kerusakan berarti pada peralatan yang penting untuk keselamatan atau mengarah pada kondisi kecelakaan.
7. Kecelakaan Dasar Desain (*design basis accident*) yang selanjutnya disingkat DBA adalah kondisi kecelakaan yang digunakan sebagai dasar untuk desain reaktor daya menurut kriteria desain yang ditetapkan, dengan kerusakan bahan bakar dan lepasan zat radioaktif tidak melampaui batas yang diizinkan.
8. Kecelakaan yang melampaui dasar desain (*beyond design basis accident*) yang selanjutnya disingkat BDBA adalah kondisi kecelakaan yang lebih parah dari Kecelakaan Dasar Desain.

9. Kecelakaan Parah adalah kondisi kecelakaan yang melampaui Kecelakaan Dasar Desain yang mengakibatkan kerusakan teras yang berarti.
10. Kondisi Operasi adalah keadaan yang mencakup kondisi operasi normal dan Kejadian Operasi Terantisipasi.
11. Kondisi Kecelakaan adalah kondisi penyimpangan dari operasi normal yang lebih parah dari pada Kejadian Operasi Terantisipasi, yang mencakup Kecelakaan Dasar Desain dan Kecelakaan Parah.
12. Manajemen Kecelakaan adalah sejumlah tindakan yang diambil selama Kecelakaan Yang Melampaui Dasar Desain, untuk mencegah kejadian meluas menjadi kecelakaan parah, memitigasi konsekuensi kecelakaan parah; dan mencapai keadaan selamat yang stabil dalam jangka panjang.
13. Komponen Bertekanan Sistem Pendingin Reaktor (*reactor coolant system pressure boundary*) adalah semua komponen reaktor yang bertekanan dan merupakan bagian dari sistem pendingin reaktor atau terhubung ke sistem pendingin reaktor.
14. Fungsi Keselamatan adalah fungsi yang harus dipenuhi untuk mencapai keselamatan.
15. Sistem Proteksi adalah sistem yang memantau pengoperasian reaktor dan yang apabila mendeteksi kejadian abnormal, secara otomatis menginisiasi tindakan untuk mencegah reaktor ke kondisi tidak selamat.
16. Sistem Keselamatan adalah sistem yang penting untuk keselamatan, yang disediakan untuk menjamin *shutdown* reaktor dengan selamat atau pembuangan panas sisa teras, atau untuk membatasi konsekuensi memperkecil akibat Kejadian Operasi Terantisipasi dan kondisi Kecelakaan Dasar Desain.
17. Kegagalan Tunggal adalah kegagalan yang mengakibatkan hilangnya kemampuan suatu komponen untuk melakukan fungsi keselamatan, dan semua kegagalan yang diakibatkannya.
18. Pertahanan berlapis adalah penerapan upaya proteksi sehingga tujuan keselamatan dapat terwujud meskipun bila salah satu upaya proteksi menemui kegagalan.

Pasal 2

(1) Peraturan Kepala BAPETEN ini bertujuan untuk memberikan persyaratan keselamatan bagi pemegang izin dalam memastikan pembuatan desain dan analisis keselamatan desain agar reaktor daya dapat dioperasikan secara selamat pada semua kondisi instalasi.

(2) Persyaratan keselamatan dalam pembuatan desain sebagaimana dimaksud pada ayat (1) meliputi:

a. persyaratan umum desain; dan

b. persyaratan khusus desain.

(3) Kondisi instalasi sebagaimana dimaksud pada ayat (1) meliputi:

a. operasi normal;

b. kejadian operasi terantisipasi; dan

c. kecelakaan dasar desain dan kecelakaan yang melampui dasar desain.

Pasal 3

Peraturan Kepala BAPETEN ini berlaku untuk reaktor daya berpendingin air yang dibangun di daratan.

Pasal 4

Pemegang izin harus menjamin reaktor daya didesain dengan tingkat keandalan yang tinggi untuk mencapai tujuan keselamatan nuklir.

Pasal 5

(1) Tujuan keselamatan nuklir sebagaimana dimaksud dalam Pasal 4 meliputi tujuan umum dan tujuan khusus keselamatan nuklir.

(2) Tujuan umum keselamatan nuklir sebagaimana dimaksud pada ayat (1) adalah untuk melindungi pekerja, masyarakat dan lingkungan hidup yang dilakukan melalui upaya pertahanan yang efektif terhadap timbulnya bahaya radiasi di reaktor daya.

(3) Tujuan khusus keselamatan nuklir sebagaimana dimaksud pada ayat (1) meliputi tujuan proteksi radiasi dan tujuan keselamatan teknis.

(4) Tujuan proteksi radiasi sebagaimana dimaksud pada ayat (3) meliputi:

a. menjamin paparan radiasi pada setiap kondisi instalasi atau setiap pelepasan zat radioaktif yang terantisipasi dari instalasi serendah-rendahnya yang secara praktik dapat dicapai dan di bawah pembatas dosis yang ditetapkan; dan

b. menjamin mitigasi dampak radiologi dari suatu kecelakaan yang ditimbulkan selama pengoperasian reaktor daya.

(5) Tujuan keselamatan teknis sebagaimana dimaksud pada ayat (3) adalah:

a. mencegah terjadinya kecelakaan selama pengoperasian reaktor daya serta melakukan mitigasi dampak radiologi apabila kecelakaan tetap terjadi;

b. memastikan dengan tingkat kepercayaan tinggi bahwa semua kecelakaan yang telah dipertimbangkan dalam desain reaktor daya memberikan risiko serendah-rendahnya; dan

c. memastikan bahwa kecelakaan dengan dampak radiologi yang serius mempunyai kebolehjadian yang sangat kecil.

Pasal 6

Pertahanan yang efektif sebagaimana dimaksud dalam Pasal 5 ayat (2) diwujudkan melalui penerapan pertahanan berlapis untuk memenuhi fungsi keselamatan dasar reaktor.

Pasal 7

Pertahanan berlapis sebagaimana dimaksud dalam Pasal 6 meliputi:

a. tingkat 1, pencegahan kegagalan dan kejadian operasi terantisipasi yang dilakukan dengan desain konservatif, konstruksi dan operasi yang berkualitas tinggi;

b. tingkat 2, pencegahan terhadap berkembangnya kejadian operasi terantisipasi menjadi kecelakaan melalui pengendalian terhadap kejadian operasi terantisipasi serta deteksi kegagalan yang dilakukan dengan sistem pengendalian, pembatasan dan proteksi serta fitur surveilan yang lain;

c. tingkat 3, pengendalian kecelakaan dasar desain untuk membawa kondisi reaktor ke keadaan terkendali dan mempertahankan pengungkungan zat radioaktif dengan fitur keselamatan teknis dan prosedur kecelakaan;

d. tingkat 4, pengendalian terhadap kondisi yang parah untuk menjaga agar pelepasan zat radioaktif serendah mungkin, termasuk pencegahan perambatan kecelakaan dan mitigasi kecelakaan parah yang dilakukan dengan upaya tambahan dan manajemen kecelakaan; dan/atau

e. tingkat 5, mitigasi konsekuensi radiologi untuk pelepasan zat radioaktif signifikan, yang dilakukan dengan tindakan penanggulangan kedaruratan nuklir baik di dalam maupun luar tapak.

Pasal 8

Fungsi keselamatan dasar reaktor sebagaimana dimaksud dalam Pasal 6 meliputi:

a. mengendalikan reaktivitas;

b. memindahkan panas dari teras reaktor; dan

c. mengungkung zat radioaktif dan menahan radiasi.

Pasal 9

(1) Fungsi keselamatan dasar reaktor sebagaimana dimaksud dalam Pasal 8 harus dilaksanakan selama status operasi, selama dan sesudah terjadi DBA, dan kecelakaan yang melampaui DBA yang ditetapkan.

(2) Pemegang izin harus mengidentifikasi struktur, sistem, dan komponen yang diperlukan untuk melaksanakan fungsi keselamatan sebagaimana dimaksud pada ayat (1) sesuai dengan PIE yang ditetapkan.

Pasal 10

(1) Pemegang izin harus menetapkan kode dan standar (*code and standard*) terkini yang diberlakukan terhadap struktur, sistem dan komponen yang penting untuk keselamatan.

(2) Dalam hal digunakan kode dan standar *(code and standard)* yang berbeda untuk struktur, sistem dan komponen yang berbeda, Pemegang izin harus memastikan kesetaraan kode dan standar *(code and standard)* sesuai dengan klasifikasi.

(3) Kode dan standar sebagaimana dimaksud pada ayat (1) dan (2) harus memenuhi standar yang berlaku di Indonesia.

Pasal 11

Dalam hal tidak tersedia kode dan standar (*code and standard*) untuk struktur, sistem dan komponen di Indonesia, Pemegang izin harus menerapkan kode dan standar (*code and standard*) terkini yang berlaku untuk struktur, sistem dan komponen yang serupa dari negara pemasok (*vendor*).

Pasal 12

Kode dan standar sebagaimana dimaksud dalam Pasal 10 dan Pasal 11 wajib mendapat persetujuan dari Kepala BAPETEN.

Pasal 13

Upaya desain yang konservatif harus diberlakukan, dan praktik rekayasa yang baik harus dipatuhi untuk seluruh kondisi operasi reaktor daya sehingga menjamin tidak ada kerusakan yang signifikan terhadap teras reaktor dan paparan radiasi tetap berada di bawah nilai batas yang ditetapkan.

Pasal 14

Reaktor daya yang digabungkan instalasi pemanfaatan panas dan/atau instalasi desalinasi air harus didesain untuk mencegah perpindahan zat radioaktif dari reaktor nuklir ke instalasi pemanfaatan panas dan/atau instalasi desalinasi air dalam kondisi operasi normal, kejadian operasi terantisipasi, dan kondisi kecelakaan.

Pasal 15

(1) Pemegang izin harus menetapkan tim independen diluar dari pendesain.

(2) Pemegang izin dan tim bertanggung jawab terhadap integritas desain reaktor daya selama umur reaktor.

(3) Dalam melaksanakan tanggung jawabnya, tim bertugas melakukan konfirmasi desain dalam mencapai tujuan dan persyaratan keselamatan.

(4) Dalam penetapan tim sebagaimana dimaksud pada ayat (1) Pemegang izin tetap bertanggungjawab terhadap keselamatan**.**

Pasal 16

Tim sebagaimana dimaksud dalam Pasal 15 ayat (1) harus menjamin:

a. desain reaktor daya memenuhi kriteria keselamatan, keandalan, dan mutu sesuai dengan peraturan perundang-undangan, kode dan standar melalui verifikasi dan penilaian keselamatan desain, penetapan standar teknis, persetujuan dokumen teknis kunci (*key engineering documents*) dan penerapan budaya keselamatan;

b. pengetahuan tentang desain yang diperlukan untuk operasi dan perawatan yang selamat tersedia dan dimutakhirkan, dengan mempertimbangkan pengalaman operasi dan hasil penelitian yang tervalidasi;

c. konfigurasi desain telah terkendali;

d. koordinasi dengan pendesain atau pemasok dibentuk dan terkendali;

e. semua perubahan desain telah diverifikasi, dinilai, didokumentasikan dan disetujui; dan

f. dokumentasi tetap terjaga untuk memudahkan pelaksanaan dekomisioning.

Pasal 17

Pemegang izin harus memastikan bahwa verifikasi dan penilaian

keselamatan sebagaimana dimaksud dalam Pasal 16 huruf a telah dilaksanakan sebelum desain diajukan kepada Kepala BAPETEN.

Pasal 18

(1) Pemegang izin harus melakukan penilaian keselamatan secara menyeluruh untuk membuktikan bahwa desain yang diajukan untuk fabrikasi, konstruksi dan desain terbangun (*as built design*) memenuhi persyaratan keselamatan yang ditetapkan pada awal proses desain.

(2) Penilaian keselamatan harus merupakan bagian proses desain, dengan iterasi antara kegiatan desain dan analitis untuk keperluan konfirmasi dan meningkatkan lingkup serta tingkat kerincian sesuai dengan kemajuan program desain.

(3) Penilaian keselamatan sebagaimana dimaksud pada ayat (1) harus didasarkan pada data yang diperoleh dari analisis keselamatan, pengalaman operasi terdahulu, hasil penelitian pendukung dan praktek rekayasa yang telah teruji.

Pasal 19

Ketentuan mengenai Verifikasi dan Penilaian Keselamatan Reaktor Daya diatur tersendiri dengan Peraturan Kepala BAPETEN.

Pasal 20

(1) Pemegang izin wajib melakukan analisis keselamatan deterministik terhadap desain untuk setiap kondisi instalasi.

(2) Untuk reaktor daya komersial, Pemegang izin wajib melakukan analisis keselamatan probabilistik terhadap desain untuk setiap kondisi instalasi.

(3) Pemegang izin menjamin program komputer, metode analitis, dan model instalasi yang digunakan di dalam analisis keselamatan telah diverifikasi dan divalidasi.

Pasal 21

(1) Analisis keselamatan deterministik sebagaimana dimaksud dalam Pasal 20 ayat (1) meliputi:

a. penetapan dan konfirmasi dasar desain untuk struktur, sistem dan komponen yang penting untuk keselamatan;

b. karakterisasi PIE yang tepat untuk desain dan tapak instalasi;

c. analisis dan evaluasi mengenai urutan kejadian yang diakibatkan oleh PIE;

d. perbandingan hasil analisis dengan kriteria keberterimaan radiologi dan batasan desain;dan

e. pembuktian bahwa respons terhadap kejadian operasi terantisipasi dan kecelakaan dasar desain dilakukan dengan respon otomatis sistem keselamatan yang dikombinasikan dengan tindakan operator yang telah ditentukan sebelumnya.

(2) Asumsi analitik, metode, dan tingkat konservatisme yang digunakan harus diverifikasi.

(3) Pemegang izin harus memperbaharui analisis keselamatan desain reaktor dalam hal terjadi perubahan penting dalam konfigurasi desain reaktor, dan berdasarkan pengalaman operasi dari reaktor lain, dan perkembangan teknologi.

Pasal 22

Analisis keselamatan probabilistik sebagaimana dimaksud dalam Pasal 20 ayat (2) dilaksanakan untuk:

a. menetapkan bahwa desain yang seimbang telah tercapai sehingga tidak ada fitur atau PIE memberikan sumbangan tak proporsional atau ketidakpastian yang signifikan terhadap keseluruhan risiko, dan bahwa dua tingkat pertama pertahanan berlapis menjadi pertimbangan utama dalam menjamin keselamatan nuklir;

b. memberikan tingkat kepercayaan bahwa penyimpangan kecil dalam parameter instalasi yang mengarah pada kecelakaan parah dapat dicegah;

c. memberikan penilaian terhadap kebolehjadian timbulnya keadaan kerusakan teras yang parah dan penilaian terhadap risiko pelepasan zat radioaktif yang besar ke luar-tapak yang memerlukan penanggulangan luar-tapak jangka pendek, terutama untuk pelepasan zat radioaktif yang berhubungan dengan kegagalan penyungkup;

d. memberikan penilaian terhadap kebolehjadian timbulnya dan konsekuensi bahaya eksternal, khususnya yang berlaku pada tapak;

e. mengidentifikasi sistem yang apabila dilakukan perbaikan desain atau modifikasi pada prosedur operasinya dapat mengurangi kebolehjadian kecelakaan parah atau memitigasi konsekuensi kecelakaan parah;

f. menilai kelayakan prosedur penanggulangan kedaruratan reaktor; dan

g. melakukan verifikasi kesesuaiannya dengan sasaran probabilistik.

Pasal 23

(1) Pemegang izin harus menetapkan dasar desain struktur, sistem dan komponen yang penting untuk keselamatan sehingga mampu berfungsi pada:

a. kondisi instalasi; dan

b. kondisi yang ditimbulkan oleh bahaya internal dan eksternal,

dengan memenuhi persyaratan proteksi radiasi yang ditetapkan.

(2) Dasar desain struktur, sistem dan komponen harus didokumentasikan dan tersedia untuk pengoperasian reaktor dengan selamat.

(3) Dasar desain sebagaimana dimaksud pada ayat (1) memuat:

a. spesifikasi struktur, sistem dan komponen untuk setiap kondisi instalasi;

b. klasifikasi keselamatan;

c. keandalan;

d. asumsi penting;

e. metode analisis; dan

f. identifikasi dan kuantifikasi ketidakpastian.

Pasal 24

Pemegang izin wajib menetapkan batas desain struktur, sistem dan komponen yang sesuai dengan parameter fisik kunci untuk setiap kondisi operasi dan kondisi kecelakaan dasar desain.

Pasal 25

(1) Pemegang izin harus menentukan dan menganalisis PIE dalam penetapan dasar desain sebagaimana dimaksud dalam Pasal 21 ayat (1).

(2) PIE sebagaimana dimaksud pada ayat (1) yang relevan ditentukan berdasarkan daftar kejadian yang terdapat dalam Lampiran I mengenai PIE yang merupakan bagian tak terpisahkan dari Peraturan Kepala BAPETEN ini.

(3) Dalam hal PIE tidak terdapat dalam lampiran I, Pemegang izin harus menetapkan PIE dengan memperhitungkan semua kecelakaan yang mungkin terjadi yang mempengaruhi keselamatan reaktor khususnya kecelakaan dasar desain.

Pasal 26

(1) Dalam menentukan dan menganalisis PIE sebagaimana dimaksud dalam Pasal 25 ayat (1), Pemegang izin harus mempertimbangkan bahaya eksternal dan internal yang mempengaruhi keselamatan reaktor daya.

(2) Bahaya eksternal sebagaimana dimaksud pada ayat (1) meliputi aspek:
   a. kegempaan;
   b. kegunung apian;
   c. dispersi zat radioakatif;
   d. geoteknik;
   e. meteorologi; dan
   f. kejadian eksternal akibat ulah manusia.

(3) Bahaya internal sebagaimana dimaksud pada ayat (1) meliputi:
   a. kebakaran dan ledakan internal;
   b. banjir internal;
   c. kehilangan sistem bantu;
   d. kecelakaan terkait keamanan;
   e. malfungsi operasi reaktor;
   f. kegagalan aliran pendingin; dan
   g. reaksi kimia eksotermis.

Pasal 27

Ketentuan mengenai desain yang terkait dengan bahaya eksternal dan internal diatur tersendiri dengan Peraturan Kepala BAPETEN.

Pasal 28

(1) Pemegang izin harus menetapkan BKO berdasarkan proses desain.

(2) BKO sebagaimanan dimaksud pada ayat (1) meliputi:
   a. batas keselamatan;
   b. pengesetan (*setting*) sistem keselamatan;
   c. kondisi batas untuk operasi normal;
   d. persyaratan surveilan; dan
   e. persyaratan administrasi.

(3) Reaktor harus didesain sehingga respon reaktor terhadap AOO akan memungkinkan operasi secara selamat atau, *shutdown* cukup dengan menggunakan pertahanan berlapis tingkat pertama atau, paling tinggi tingkat kedua.

Pasal 29

Ketentuan mengenai BKO reaktor daya diatur tersendiri dengan Peraturan Kepala BAPETEN.

Pasal 30

(1) Pemegang izin harus menetapkan serangkaian kecelakaan dasar desain berdasarkan PIE yang telah dipilih.

(2) Pemegang izin harus memastikan desain reaktor dapat secara otomatis menginisiasi sistem keselamatan untuk serangkaian kondisi kecelakaan dasar desain sebagaimana dimaksud pada ayat (1), sehingga mengurangi tindakan manual operator.

(3) Struktur, sistem dan komponen yang penting untuk keselamatan harus didesain untuk tahan terhadap efek beban dan kondisi lingkungan yang ekstrim akibat kecelakaan dasar desain

(4) Reaktor daya harus didesain mampu membawa reaktor ke keadaan stabil jangka panjang setelah kecelakaan dasar desain terutama dengan mempertahankan koefisien reaktivitas daya negatif.

Pasal 31

(1) Reaktor daya harus didesain mempertimbangkan tindakan operator yang mungkin diperlukan untuk mendiagnosis keadaan instalasi dan melakukan *shutdown* pada saat yang tepat.

(2) Untuk mendukung tindakan operator, desain harus menyediakan sistem instrumentasi untuk memantau keadaan instalasi dan mengendalikan operasi peralatan secara manual.

Pasal 32

Setiap peralatan yang diperlukan untuk tindakan manual harus ditempatkan di lokasi yang tepat sehingga memudahkan akses operator.

Pasal 33

(1) Reaktor daya harus didesain mengantisipasi kecelakaan yang melampaui dasar desain dan kecelakaan parah melalui tindakan pencegahan dan mitigasi.

(2) Dalam mengantisipasi kecelakaan sebagaimana dimaksud pada ayat (1), harus dipertimbangkan:

a. identifikasi urutan kejadian penting yang mengarah pada kecelakaan melalui kombinasi metode probabilistik, deterministik, dan termasuk pertimbangan teknis;

b. penilaian urutan rangkaian kejadian sebagaimana dimaksud pada huruf a berdasarkan pada kriteria yang ditetapkan untuk menentukan kecelakaan;

c. evaluasi terhadap potensi perubahan desain atau perubahan prosedur yang dapat mengurangi kemungkinan kejadian atau

mengurangi konsekuensi kecelakaan yang ditentukan sebagaimana dimaksud pada huruf b;

d. kemampuan desain maksimum reaktor termasuk penggunaan sistem keselamatan dan sistem lainnya yang melampaui fungsinya, serta penggunaan sistem tambahan untuk mengembalikan instalasi ke keadaan terkendali dan atau mengurangi konsekuensi kecelakaan parah;

e. penggunaan sarana yang tersedia dan atau dukungan dari unit lain apabila pada satu tapak terdapat lebih dari satu unit reaktor; dan

f. penetapan manajemen kecelakaan dengan mempertimbangkan kecelakaan yang paling dominan.

Pasal 34

Pemegang izin harus mengidentifikasi dan mengklasifikasikan struktur, sistem, dan komponen, termasuk perangkat lunak untuk instrumentasi dan kendali, berdasarkan kepentingannya terhadap fungsi keselamatan.

Pasal 35

(1) Klasifikasi keselamatan struktur, sistem, dan komponen harus dilakukan dengan metode deterministik dan dapat dilengkapi dengan metode probabilistik dengan mempertimbangkan:

a. fungsi keselamatan;

b. konsekuensi kegagalan struktur, sistem, dan komponen;

c. kebolehjadian struktur, sistem, dan komponen untuk melakukan fungsi keselamatan; dan

d. waktu yang diperlukan struktur, sistem, dan komponen untuk berfungsi sesudah terjadi PIE.

(2) Antarmuka desain yang memadai antara struktur, sistem dan komponen dengan kelas yang berbeda harus diberikan untuk memastikan agar kegagalan struktur, sistem dan komponen dengan kelas keselamatan yang lebih rendah tidak menyebabkan kegagalan terhadap struktur, sistem dan komponen dengan kelas keselamatan yang lebih tinggi.

Pasal 36

Perangkat lunak sebagaimana dimaksud dalam Pasal 34 dan piranti elektrik yang mempunyai fungsi ganda harus diklasifikasikan sesuai dengan kelas keselamatan tertinggi pada struktur, sistem dan komponen yang menggunakan perangkat lunak dan piranti elektrik.

Pasal 37

Struktur, sistem, dan komponen sebagaimana dimaksud dalam Pasal 34 harus diklasifikasikan berdasarkan kelas mutu dan seismik.

Pasal 38

Ketentuan mengenai klasifikasi keselamatan, seismik dan mutu untuk struktur, sistem dan komponen reaktor daya diatur tersendiri dengan Peraturan Kepala BAPETEN.

BAB II

PERSYARATAN TEKNIS KESELAMATAN DESAIN

Pasal 39

(1) Dalam melaksanakan pembangunan, pengoperasian dan dekomisioning reaktor daya, Pemegang izin harus memenuhi persyaratan teknis keselamatan desain yang meliputi persyaratan umum desain dan persyaratan khusus desain.

(2) Persyaratan umum desain meliputi :

a. desain keandalan struktur, sistem, dan komponen;

b. desain kemudahan pengoperasian, perawatan, surveilan, dan inspeksi;

c. desain kesiapsiagaan dan penanggulangan kedaruratan nuklir;

d. desain kemudahan dekomisioning;

e. desain proteksi radiasi;

f. desain untuk faktor manusia (*human factor*); dan

g. desain untuk meminimalkan penuaan.

(3) Persyaratan khusus desain meliputi :

a. teras reaktor;

b. sistem *shutdown*;

c. sistem proteksi reaktor;

d. sistem pendingin reaktor dan sistem terkait;

e. sistem pendingin teras darurat;

f. sistem dan struktur penyungkup;

g. sistem instrumentasi dan kendali;

h. sistem penanganan dan penyimpanan bahan bakar nuklir;

i. sistem catu daya listrik;

j. sistem penanganan dan pengendalian limbah radioaktif;

k. sistem bantu;

l. sistem konversi daya; dan

m. fitur keselamatan teknis;

Bagian Kesatu

Persyaratan Umum Desain

Paragraf Kesatu

Desain untuk Keandalan Struktur, Sistem, dan Komponen

Pasal 40

(1) Struktur, sistem, dan komponen yang penting untuk keselamatan harus didesain dengan keandalan yang mencukupi sehingga mampu untuk melakukan fungsi keselamatan pada semua kondisi instalasi.

(2) Keandalan harus sesuai dengan kelas keselamatan dan kinerja yang diharapkan.

Pasal 41

(1) Untuk menjamin keandalan sebagaimana dimaksud dalam Pasal 40 ayat (1), Pemegang izin harus menerapkan:

a. redundansi dan kriteria kegagalan tunggal;

b. keragaman;

c. kemandirian; dan

d. desain gagal-selamat.

(2) Penerapan prinsip redundansi, keragaman dan kemandirian harus mempertimbangkan kegagalan dengan penyebab sama.

(3) Penerapan sebagaimana dimaksud pada ayat (1) berlaku untuk sistem bantu yang mendukung sistem yang penting untuk keselamatan.

Pasal 42

(1) Berdasarkan analisis keselamatan, prinsip redundansi sebagaimana dimaksud dalam Pasal 41 ayat (1) huruf a harus diterapkan untuk memastikan tidak terjadi kegagalan tunggal yang menyebabkan sistem

kehilangan kemampuan melaksanakan fungsi keselamatan reaktor.

(2) Tingkat redundansi yang digunakan harus menunjukkan kemampuan menanggulangi kegagalan yang tidak terdeteksi yang dapat menurunkan keandalan.

(3) Fungsi keselamatan sebagaimana dimaksud pada ayat (1) diuraikan dalam lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Kepala BAPETEN ini.

Pasal 43

(1) Kriteria kegagalan tunggal sebagaimana dimaksud dalam Pasal 41 ayat (1) huruf a harus diterapkan dalam desain untuk setiap fungsi keselamatan.

(2) Kriteria kegagalan tunggal harus mempertimbangkan:

a. kegagalan yang terjadi sebagai konsekuensi kegagalan tunggal;

b. *spurious action*;

c. konfigurasi terburuk yang diperbolehkan;

d. tingkat kapasitas dan waktu respons sistem keselamatan untuk melaksanakan fungsi keselamatan dengan memperhitungkan perawatan, surveilan, inspeksi dan perbaikan, serta masa tak-layan (*outage*s) peralatan yang diperbolehkan.

Pasal 44

(1) Penerapan keragaman sebagaimana dimaksud dalam 41 ayat (1) huruf b pada sistem atau komponen harus dilakukan untuk melaksanakan fungsi keselamatan yang sama dengan menggunakan atribut yang berbeda.

(2) Atribut yang berbeda meliputi:

a. prinsip operasi yang berbeda;

b. kondisi operasi yang berbeda; dan/atau

c. manufaktur yang berbeda.

Pasal 45

(1) Penerapan kemandirian sebagaimana dimaksud dalam Pasal 41 ayat (1) huruf c harus dilakukan untuk meningkatkan keandalan sistem terutama berkaitan dengan kegagalan dengan sebab yang sama.

(2) Penerapan kemandirian dapat harus dilakukan dengan cara isolasi fungsi dan pemisahan fisik dengan mempertimbangkan jarak, penghalang, dan tata letak khusus struktur, sistem dan komponen.

Pasal 46

(1) Penerapan gagal-selamat sebagaimana dimaksud dalam Pasal 41 ayat (1) huruf d harus dilakukan pada desain sistem dan komponen yang penting untuk keselamatan.

(2) Sistem reaktor harus didesain mampu tetap dalam kondisi selamat tanpa tindakan pemicu apabila struktur, sistem dan komponen mengalami kegagalan.

Pasal 47

Dalam hal struktur, sistem dan komponen yang penting untuk keselamatan digunakan pada lebih dari satu reaktor, desain harus menjamin struktur, sistem dan komponen tetap dapat melaksanakan fungsi keselamatan dalam kondisi instalasi.

Pasal 48

Penerapan redundansi, kriteria kegagalan tunggal, keragaman, kemandirian, gagal-selamat diuraikan lebih rinci dalam lampiran III mengenai redundansi, keragaman dan kemandirian yang merupakan bagian tidak terpisahkan dari Peraturan Kepala BAPETEN ini.

Paragraf Kedua

Desain untuk Kemudahan Pengoperasian, Perawatan,

Surveilan dan Inspeksi

Pasal 49

Reaktor daya harus didesain untuk kemudahan pengoperasian, perawatan, surveilan dan inspeksi.

(1) Pemegang izin harus menetapkan program kualifikasi dalam desain untuk kemudahan pengoperasian, perawatan, surveilan dan inspeksi.

(2) Program kualifikasi harus dilaksanakan untuk mengkonfirmasi struktur, sistem dan komponen memenuhi persyaratan desain dengan mempertimbangkan program perawatan, surveilan, dan inspeksi, serta kondisi lingkungan.

(3) Kondisi lingkungan sebagaimana dimaksud pada ayat (3) meliputi getaran, iradiasi, dan temperatur.

(4) Dalam hal struktur, sistem dan komponen yang penting untuk keselamatan berpotensi menerima dampak kejadian alam, program kualifikasi harus dilaksanakan melalui surveilan, analisis, atau kombinasi keduanya yang mencerminkan fenomena alam dari kejadian alam.

(5) Program kualifikasi harus mencakup laju kebocoran sungkup dan

instrumentasi yang ditetapkan untuk berfungsi selama kecelakaan yang melampaui dasar desain, selama dan setelah kecelakaan parah.

Pasal 50

Interaksi antara sistem yang penting untuk keselamatan yang diperlukan untuk beroperasi secara simultan harus dievaluasi.

Pasal 51

(1) Reaktor daya harus didesain dapat dirawat, diuji dan diinspeksi untuk memastikan struktur, sistem dan komponen yang penting untuk keselamatan dapat berfungsi dengan keandalan yang ditetapkan.

(2) Faktor yang harus dipertimbangkan dalam desain sebagaimana dimaksud pada ayat (1) meliputi:

a. kemudahan pelaksanaan perawatan, surveilan, dan inspeksi;

b. tingkat perawatan, inspeksi dan surveilan yang mewakili kondisi nyata; dan

c. kebutuhan untuk tetap mempertahankan kinerja fungsi keselamatan selama surveilan.

Pasal 52

(1) Reaktor daya harus didesain dengan struktur, sistem dan komponen yang penting untuk keselamatan dapat dirawat, diuji dan diinspeksi pada kondisi terpasang tanpa perlu *shutdown* instalasi dengan cara meningkatkan redundansi.

(2) Masa tak-layan struktur, sistem dan komponen termasuk ketidaktersediaan akibat kegagalan struktur, sistem dan komponen harus diperhitungkan.

(3) Dampak kegiatan perawatan, surveilan dan inspeksi terhadap keandalan sistem keselamatan harus dipertimbangkan untuk menjamin fungsi keselamatan tetap tercapai.

(4) Waktu masa tak-layan struktur, sistem dan komponen yang penting untuk keselamatan yang dilakukan dan tindakan yang dilakukan selama masa tak-layan harus dianalisis dan ditetapkan.

Paragraf Ketiga

Desain untuk Kesiapsiagaan dan Penanggulangan Kedaruratan Nuklir

Pasal 53

(1) Reaktor daya harus didesain untuk memudahkan pelaksanaan program kesiapsiagaan dan penanggulangan kedaruratan nuklir sesuai dengan potensi bahaya reaktor.

(2) Desain sebagaimana dimaksud pada ayat (1) harus ditetapkan melalui analisis kecelakaan yang melampaui dasar desain.

Pasal 54

(1) Desain sebagaimana dimaksud dalam Pasal 53 ayat (1) mencakup:
   a. jalur evakuasi;
   b. tanda yang jelas dengan penerangan darurat yang andal;
   c. ventilasi; dan
   d. gedung bantu.

(2) Jalur evakuasi didesain dengan mempertimbangkan pembagian daerah radiasi, proteksi terhadap kebakaran dan ledakan, dan proteksi fisik.

Pasal 55

(1) Reaktor daya harus didesain dilengkapi dengan sistem alarm dan alat komunikasi yang memadai dan tersedia setiap saat sehingga setiap orang yang berada di tapak dan dalam gedung reaktor dapat memperoleh informasi dan instruksi kedaruratan.

(2) Selain alat komunikasi yang tersedia sebagaimana dimaksud pada ayat (1), desain harus dilengkapi juga dengan alat komunikasi yang memadai sehingga setiap institusi yang berada di sekitar dan di luar tapak dapat memperoleh informasi dan instruksi kedaruratan.

(3) Alat komunikasi harus didesain dengan mempertimbangkan keragamannya.

Pasal 56

(1) Reaktor daya harus didesain untuk menyediakan pusat kendali tanggap darurat yang terpisah dari ruang kendali utama reaktor.

(2) Pusat kendali tanggap darurat sebagaimana dimaksud pada ayat (1) harus dapat berfungsi:
   a. sebagai tempat pertemuan bagi petugas penanggulangan dalam hal terjadi kedaruratan;
   b. menyediakan informasi mengenai parameter-parameter instalasi yang penting dan kondisi radiologik di instalasi dan di wilayah sekitar tapak;
   c. menyediakan sarana komunikasi dengan ruang kendali utama, ruang kendali tambahan dan titik-titik penting lainnya dalam instalasi, dan dengan organisasi penanggulangan di dalam dan di luar tapak; dan

d. menyediakan ventilasi darurat dengan pasokan udara tersendiri, logistik dan sarana layanan lain untuk kebutuhan paling singkat 3 (tiga) kali 24 (dua puluh empat) jam.

Pasal 57

Ketentuan mengenai desain kesiapsiagaan dan penanggulangan kedaruratan nuklir diatur tersendiri dalam Peraturan Kepala BAPETEN.

Paragraf Keempat

Desain untuk Kemudahan Dekomisioning

Pasal 58

(1) Reaktor harus didesain untuk memudahkan pelaksanaan dekomisioning.

(2) Desain reaktor sebagaimana dimaksud pada ayat (1), harus mempertimbangkan:

a. pemilihan bahan untuk meminimalkan limbah radioaktif yang ditimbulkan dan memudahkan dekontaminasi;

b. kemudahan akses;

c. metode dan peralatan penanganan yang diperlukan;

d. fasilitas yang diperlukan untuk menyimpan limbah radioaktif; dan

e. penanganan limbah radioaktif yang ditimbulkan dari kegiatan dekomisioning.

Paragraf Kelima

Desain untuk Proteksi Radiasi

Pasal 59

(1) Reaktor daya harus didesain sesuai dengan tujuan proteksi radiasi selama kondisi instalasi dan dekomisioning.

(2) Desain sebagaimana dimaksud pada ayat (1) harus mempertimbangkan:

a. pemilihan bahan untuk meminimalkan hasil aktivasi;

b. semua zat radioaktif yang teridentifikasi di dalam instalasi;

c. integritas kelongsong bahan bakar nuklir;

d. terbentuknya produk korosi dan aktivasi, termasuk perpindahannya;

e. pembagian daerah kerja dan penggunaan perisai;

f. tata letak yang menjamin akses personil ke daerah radiasi dan kontaminasi dilengkapi dengan sistem ventilasi yang memadai;

g. tata letak yang menjamin waktu yang dibutuhkan oleh pekerja radiasi dalam daerah radiasi selama kegiatan operasi sesingkat mungkin dan dilengkapi dengan peralatan yang memadai; dan

h. fasilitas dekontaminasi personil, peralatan dan instalasi.

Pasal 60

Pembatas dosis yang digunakan dalam desain harus ditetapkan untuk memastikan nilai batas dosis tidak terlampaui.

Pasal 61

(1) Reaktor daya harus didesain untuk menyediakan perlengkapan proteksi radiasi yang menjamin pemantauan radiasi atau kontaminasi radioaktif di daerah kerja, pemantauan dosis perorangan, dan pemantauan radioaktivitas lingkungan yang memadai dalam kondisi instalasi.

(2) Perlengkapan proteksi radiasi sebagaimana dimaksud pada ayat (1) meliputi:

a. alat ukur laju dosis stasioner untuk pengamatan laju dosis radiasi daerah kerja dan tempat lain yang dimungkinkan terjadi perubahan tingkat paparan radiasi;

b. alat ukur laju dosis stasioner yang dipasang di tempat yang sesuai untuk mendeteksi lepasan zat radioaktif pada kondisi kejadian operasi yang terantisipasi dan kondisi kecelakaan;

c. peralatan stasioner untuk pemantauan kontaminasi udara di daerah kerja dan di tempat lain yang sesuai;

d. peralatan stasioner dan fasilitas laboratorium untuk menentukan konsentrasi radionuklida tertentu dalam sampel gas dan cair yang diambil dari instalasi atau lingkungan pada semua kondisi instalasi;

e. peralatan stasioner untuk pemantauan efluen sebelum atau selama pelepasan ke lingkungan;

f. peralatan pemantau kontaminasi permukaan;

g. peralatan pemantau kontaminasi dan dosis perorangan; dan

h. peralatan pemantau radiasi pada tempat yang menjadi akses manusia dan barang.

(3) Perlengkapan proteksi radiasi sebagaimana dimaksud pada ayat (2) huruf a, b, c, dan e harus didesain untuk memberikan informasi yang

ditampilkan di ruang kendali utama dan di tempat lain yang tepat selama kondisi instalasi.

(4) Desain harus mempertimbangkan dampak radiologi pada daerah sekitar instalasi reaktor daya terhadap:

a. jalur menuju populasi manusia, termasuk rantai makanan;

b. ekosistem setempat;

c. akumulasi zat radioaktif pada lingkungan fisik; dan

d. jalur pelepasan lain yang tidak diperhitungkan sebelumnya.

Pasal 62

Reaktor daya harus didesain dapat mencegah masuknya zat radioaktif dari instalasi reaktor ke unit lain pada kondisi operasi, kecelakaan dasar desain, dan kecelakaan parah yang dipertimbangkan.

Pasal 63

Ketentuan mengenai aspek proteksi radiasi dalam desain reaktor daya diatur tersendiri dalam Peraturan Kepala BAPETEN.

Paragraf Keenam

Desain untuk Faktor Manusia

Pasal 64

(1) Reaktor daya harus didesain dengan mempertimbangkan faktor manusia dan antarmuka manusia-mesin.

(2) Desain reaktor sebagaimana dimaksud pada ayat (1) harus mempertimbangkan:

a. prinsip ergonomi untuk daerah kerja dan kondisi lingkungan kerja pada ruang kendali utama, ruang kendali tambahan, dan akses menuju ruang kendali tambahan;

b. perbedaan sistem manual dan sistem otomatis;

c. antarmuka manusia-mesin untuk menyediakan informasi yang komprehensif dan mudah diolah bagi operator;

d. waktu yang memadai untuk melakukan tindakan; dan

e. faktor psikologi.

(3) Informasi sebagaimana dimaksud pada ayat (2) huruf c harus ditampilkan oleh sistem tampilan informasi secara sederhana dan jelas sehingga memungkinkan operator untuk:

a. melakukan penilaian secara cepat, tepat, dan akurat mengenai kondisi instalasi, dan konfirmasi tindakan keselamatan otomatis;

b. mengoperasikan reaktor sesuai kondisi batas untuk operasi normal;

c. menentukan inisiasi tindakan keselamatan secara tepat; dan

d. menginisiasi tindakan keselamatan yang diperlukan.

Paragraf Ketujuh

Desain untuk Meminimalkan Penuaan

Pasal 65

(1) Reaktor daya harus didesain dengan menyediakan margin yang cukup untuk mengantisipasi pengaruh penuaan dan degradasi terkait umur pada seluruh struktur, sistem, dan komponen yang penting untuk keselamatan selama umur reaktor.

(2) Desain sebagaimana dimaksud pada ayat (1) harus menyediakan ketentuan untuk pemantauan, surveilan, pencuplikan, dan inspeksi untuk menilai mekanisme penuaan yang diperkirakan dan untuk mengidentifikasi perilaku atau degradasi yang mungkin terjadi selama operasi reaktor.

(3) Pengaruh penuaan harus dipertimbangkan untuk semua kondisi instalasi.

Bagian Kedua

Persyaratan Khusus Desain

Paragraf Kesatu

Teras Reaktor dan Sistem terkait

Pasal 66

Teras reaktor dan sistem terkait harus didesain dengan:

a. margin yang memadai untuk menjamin batas desain dan kriteria keberterimaan radiologik yang ditentukan tidak dilampaui dalam semua kondisi instalasi;

b. ketahanan teras reaktor dan struktur internal di dalam bejana reaktor terhadap beban statik dan dinamik yang diperkirakan terjadi pada semua kondisi instalasi dan akibat kejadian eksternal untuk menjamin *shutdown* reaktor secara selamat, kondisi subkritis dan pendinginan teras;

c. pembatasan nilai dan laju kenaikan reaktivitas positif maksimum akibat insersi sehingga tidak mengakibatkan kerusakan pada teras reaktor, kegagalan pada sistem pendingin reaktor bertekanan, dan penurunan kemampuan pendinginan teras;

d. pencegahan kemungkinan terjadi kekritisan ulang atau kenaikan reaktivitas yang melampaui batas desain bahan bakar nuklir setelah PIE;

e. ketersediaan paling sedikit dua sistem *shutdown* reaktor yang berbeda prinsip kerjanya dan independen serta masing-masing memiliki kemampuan penuh untuk memadamkan reaktor, baik dalam keadaan operasional maupun DBA.

Pasal 67

Teras reaktor harus didesain:

a. pada saat pengoperasian normal tetap stabil;

b. dengan kebutuhan pengoperasian sistem kendali untuk mempertahankan bentuk, tingkat, dan kestabilan fluks dalam batas yang ditetapkan diminimalkan; dan

c. menyediakan alat pendeteksi distribusi fluks yang memadai untuk menjamin terdeteksinya daerah teras yang melampaui batas desain.

Pasal 68

(1) Perangkat bahan bakar nuklir didesain untuk mampu mempertahankan integritas struktur terhadap kondisi lingkungan, iradiasi, dan semua proses degradasi lainnya di dalam teras reaktor dalam kondisi operasi.

(2) Degradasi sebagaimana dimaksud pada ayat (1) disebabkan oleh:

a. ekspansi dan deformasi tidak merata;

b. tekanan dari pendingin;

c. tekanan dari produk fisi dalam bahan bakar nuklir;

d. iradiasi bahan bakar nuklir dan bahan lainnya dalam perangkat bahan bakar nuklir;

e. perubahan tekanan dan temperatur akibat perubahan daya;

f. pengaruh kimia;

g. beban statik dan dinamik, termasuk vibrasi yang diakibatkan aliran pendingin dan vibrasi mekanik; dan

h. perubahan kinerja perpindahan panas yang ditimbulkan oleh pengaruh fisika atau kimia.

(3) Perangkat bahan bakar nuklir harus didesain:

a. mempertimbangkan ketidakpastian pengukuran, perhitungan dan fabrikasi;

b. dapat diinspeksi terhadap bagian-bagian struktur dan komponen setelah diiradiasi; dan

c. tidak terjadi kebocoran produk fisi dari bahan bakar nuklir.

Pasal 69

(1) Perangkat bahan bakar nuklir harus didesain untuk berada dalam posisinya dan tidak mengalami perubahan pada kecelakaan DBA yang mengakibatkan pendinginan teras tidak memadai.

(2) Batas desain bahan bakar nuklir harus ditetapkan dan tidak boleh dilampaui pada DBA.

Pasal 70

Ketentuan mengenai desain teras reaktor dan sistem terkait diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Kedua

Sistem *Shutdown* Reaktor

Pasal 71

(1) Reaktor harus didesain menyediakan sistem *shutdown* reaktor untuk menjamin reaktor mampu di*shutdown* dalam semua kondisi operasi dan DBA dan dipertahankan dalam moda *shutdown* meskipun pada kondisi teras yang paling reaktif.

(2) Desain sistem *shutdown* reaktor sebagaimana dimaksud pada ayat (1) harus:

a. mempertimbangkan kegagalan sistem lain yang menyebabkan sistem *shutdown* tidak berfungsi.

b. memiliki paling sedikit 2 (dua) sistem yang berbeda sesuai dengan prinsip keragaman.

(3) Setiap sistem yang berbeda sebagaimana dimaksud pada ayat (2) huruf b harus didesain mampu mempertahankan reaktor tetap subkritis pada kondisi operasi dan DBA dengan margin yang memadai dan keandalan tinggi meskipun pada kondisi teras yang paling reaktif.

Pasal 72

(1) Sistem *shutdown* reaktor harus didesain mampu mencegah atau menahan kenaikan reaktivitas karena insersi selama *shutdown* termasuk penggantian bahan bakar nuklir atau kegiatan rutin lainnya dalam moda *shutdown.*

(2) Sistem *shutdown* reaktor harus didesain menyediakan instrumentasi dan surveilan untuk menjamin sistem *shutdown* berfungsi sesuai dengan kondisi instalasi yang ditetapkan.

(3) Peralatan kendali reaktivitas harus didesain dengan mempertimbangkan keausan *(wear-out)* dan efek iradiasi.

(4) Efek iradiasi sebagaimana dimaksud pada ayat (3) meliputi *burnup* batang kendali, perubahan sifat fisika, dan produksi gas.

Paragraf Ketiga

Sistem Proteksi Reaktor

Pasal 73

(1) Reaktor daya harus didesain untuk menyediakan sistem proteksi reaktor.

(2) Sistem proteksi sebagaimana dimaksud pada ayat (1) harus didesain:

a. untuk memicu pengoperasian sistem yang tepat secara otomatis, termasuk sistem *shutdown* reaktor, untuk menjamin bahwa batas desain yang telah ditentukan tidak terlampaui pada AOO;

b. untuk mendeteksi DBA dan memicu sistem yang diperlukan guna membatasi konsekuensi kecelakaan tersebut agar tetap berada dalam dasar desain; dan

c. untuk mampu mengatasi tindakan tak selamat sistem kendali.

(3) Interferensi antara sistem proteksi dan sistem kendali harus dicegah dengan menghindari interkoneksi atau dengan isolasi fungsi yang tepat.

Pasal 74

(1) Sistem proteksi reaktor harus didesain mampu menginisiasi tindakan protektif secara otomatis untuk menghentikan PIE secara selamat.

(2) Dalam hal terjadi kegagalan tunggal, sistem proteksi reaktor didesain harus tetap mampu menginisiasi tindakan protektif sebagaimana dimaksud pada ayat (1).

(3) Dalam hal tindakan otomatis sistem proteksi reaktor telah terinisiasi, sistem proteksi reaktor harus didesain untuk memproses tindakan protektif hingga selesai dan tidak dapat dihalangi oleh tindakan operator.

(4) Sistem proteksi reaktor harus didesain untuk tidak membutuhkan tindakan manual beberapa saat setelah kecelakaan terjadi.

Pasal 75

(1) Selain didesain secara otomatis, sistem proteksi reaktor sebagaimana dimaksud dalam Pasal 74 harus didesain mampu beroperasi secara manual dengan mempertimbangkan:
   a. ketersediaan waktu;
   b. ketersediaan informasi yang sudah diproses dan ditampilkan;
   c. kemudahan diagnosis dan kejelasan tindakan; dan
   d. kemudahan pengoperasian bagi operator.

(2) Desain harus mempertimbangkan kemampuan menginisiasi *scram* reaktor dari tempat lain yang ditetapkan.

(3) Sistem proteksi reaktor harus didesain untuk tidak melakukan pengesetan ulang secara otomatis setelah *scram* reaktor.

Pasal 76

Sistem proteksi reaktor sebagaimana dimaksud dalam Pasal 75 harus didesain untuk melindungi *interlock* dan pancung yang penting untuk keselamatan agar tidak dapat dipotong pintas *(bypass)*.

Pasal 77

(1) Sistem proteksi reaktor sebagaimana dimaksud dalam Pasal 75 harus didesain untuk mempertahankan reaktor tetap dalam kondisi selamat sekalipun sistem proteksi reaktor mengalami kegagalan dengan penyebab sama.

(2) Sistem proteksi reaktor harus didesain dengan margin yang memadai antara titik pengesetan dan batas keselamatan sehingga sistem proteksi reaktor mampu menghentikan PIE sebelum batas keselamatan tercapai.

(3) Penetapan margin sebagaimana dimaksud pada ayat (2) harus memperhatikan faktor-faktor:
   a. akurasi instrumentasi;
   b. ketidakpastian dalam kalibrasi;
   c. osilasi instrumen; dan
   d. waktu respons instrumen dan sistem.

Pasal 78

Dalam hal sistem proteksi reaktor sebagaimana dimaksud dalam Pasal 77 menggunakan sistem berbasis komputer, Pemegang izin harus:

a. mengupayakan reaktor daya menggunakan perangkat keras dengan kualitas tinggi dan praktik terbaik;

b. mengupayakan reaktor daya menggunakan perangkat lunak yang sudah diverifikasi, divalidasi dan diuji;

c. melakukan dokumentasi dan penilaian terhadap keseluruhan proses pembuatan, termasuk pengendalian, pengujian, dan komisioning untuk perubahan desain; dan

d. menunjuk ahli yang independen dari pendesain dan pemasok untuk mengkonfirmasi keandalan sistem berbasis komputer.

Pasal 79

(1) Reaktor daya harus didesain untuk menyediakan sistem proteksi yang mampu mendeteksi kondisi yang melampaui KBO dan memicu beroperasinya sistem keselamatan secara otomatis untuk mempertahankan KBO tidak terlampaui.

(2) Sistem proteksi harus didesain:

a. mampu mengatasi tindakan sistem kendali yang mengakibatkan kondisi operasi melampaui KBO;

b. mempertahankan kondisi reaktor daya tetap dalam KBO bila terjadi kegagalan;

c. mencegah tindakan operator yang dapat mengurangi keefektifan sistem proteksi dalam semua kondisi operasi;

d. meminimalkan kebutuhan tindakan operator dalam hal PIE atau kecelakaan, dan menyediakan tindakan segera sesuai dengan LAK; dan

e. dapat dilakukan *bypass* selama kegiatan surveilan dan perawatan sistem keselamatan dan harus disediakan petunjuk dan pengaturan yang jelas.

Pasal 80

Ketentuan mengenai sistem proteksi reaktor diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Keempat

Sistem Pendingin Reaktor dan Sistem Terkait

Pasal 81

(1) Sistem pendingin reaktor dan sistem terkait harus didesain dengan margin yang memadai untuk memastikan batas desain bahan bakar

nuklir dan sistem pendingin reaktor bertekanan tidak terlampaui dalam kondisi operasi.

(2) Sistem perpipaan yang dihubungkan dengan sistem pendingin reaktor bertekanan harus didesain dengan peralatan isolasi yang memadai untuk membatasi hilangnya pendingin.

(3) Komponen sistem pendingin reaktor sebagaimana dimaksud pada ayat (1) harus didesain dan dikonstruksi dengan bahan, standar desain, fabrikasi dan inspeksi sesuai dengan kelas mutu.

(4) Reaktor harus didesain untuk meminimalkan kerapuhan pada komponen sistem pendingin reaktor bertekanan yang disebabkan oleh kondisi instalasi.

(5) Komponen di dalam sistem pendingin reaktor bertekanan harus didesain untuk meminimalkan kemungkinan kegagalan pada struktur, sistem dan komponen lain yang penting untuk keselamatan dalam kondisi operasi dan DBA, dengan memberikan margin terhadap degradasi yang mungkin terjadi selama operasi.

Pasal 82

(1) Sistem pendingin reaktor bertekanan sebagaimana dimaksud dalam Pasal 81 harus didesain membatasi inisiasi cacat.

(2) Dalam hal cacat sebagaimana dimaksud pada ayat (1) telah terinisiasi, cacat harus dapat terdeteksi tepat waktu dengan menerapkan konsep bocor-sebelum-pecah (*leak before break*).

Pasal 83

Sistem pendingin reaktor harus didesain:

a. untuk memastikan alat pembebas tekanan mampu melindungi sistem pendingin reaktor bertekanan dari tekanan lebih tanpa menyebabkan pelepasan zat radioaktif yang tidak terkendali pada kondisi operasi dan DBA;

b. mengendalikan inventori, temperatur dan tekanan pendingin untuk menjamin batas desain yang ditetapkan tidak terlampaui pada kondisi operasi, dengan mempertimbangkan perubahan volumetrik dan kebocoran.

Pasal 84

(1) Sistem pendingin reaktor harus didesain menyediakan fasilitas untuk membersihkan pendingin reaktor dari zat radioaktif dan nonradioaktif,

termasuk produk korosi teraktivasi dan produk fisi yang bocor dari bahan bakar.

(2) Kemampuan fasilitas untuk membersihkan pendingin reaktor harus berdasarkan pada batas desain kebocoran bahan bakar nuklir yang ditetapkan dengan margin yang konservatif.

Pasal 85

Sistem pendingin reaktor harus didesain menyediakan:

a. sarana yang andal untuk memindahkan panas residu dari teras reaktor sehingga batas desain dari bahan bakar nuklir, dari sistem pendingin reaktor bertekanan dan dari struktur yang penting untuk keselamatan tidak terlampaui.
b. pendinginan teras untuk mempertahankan pendinginan bahan bakar nuklir dalam kondisi kecelakaan, termasuk dalam hal terjadi kegagalan pemindahan panas normal atau kehilangan integritas sistem pendingin primer.

Pasal 86

Pendinginan teras sebagaimana dimaksud dalam Pasal 85 huruf b harus menjamin:

a. parameter pembatas untuk integritas kelongsong atau integritas bahan bakar nuklir tidak melampaui nilai yang ditetapkan untuk DBA;
b. reaksi kimia dibatasi pada tingkat yang ditetapkan;
c. perubahan di dalam bahan bakar nuklir dan perubahan struktur internal tidak akan mengurangi efektivitas dari pendingin teras darurat; dan
d. pendinginan teras terjadi dalam kurun waktu yang memadai.

Pasal 87

(1) Sistem pendingin reaktor harus didesain untuk memindahkan panas sisa yang ditimbulkan struktur, sistem dan komponen yang penting untuk keselamatan ke pembuangan panas akhir.
(2) Sistem yang berpengaruh terhadap perpindahan panas harus didesain sesuai tingkat pengaruhnya terhadap fungsi pemindahan panas.
(3) Sistem pembuangan panas akhir harus didesain dengan keandalan yang memenuhi ketentuan penerapan sebagaimana dimaksud dalam Pasal 41 dalam kondisi operasi dan DBA.

Pasal 88

Ketentuan mengenai sistem pendingin reaktor dan sistem terkait diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Kelima

Desain Sistem Pendingin Teras Darurat

Pasal 89

Sistem pendingin teras darurat harus didesain:

a. untuk mencegah kerusakan bahan bakar dalam hal terjadi kecelakaan kehilangan pendingin;

b. mampu menjaga temperatur teras di bawah batas keselamatan yang ditentukan selama periode waktu yang memadai;dan

c. untuk memudahkan inspeksi komponen dan surveilan secara berkala.

Paragraf Keenam

Sistem dan Struktur Penyungkup (*Containment)*

Pasal 90

(1) Sistem penyungkup harus didesain untuk memenuhi fungsi berikut:
   a. mengungkung zat radioaktif pada semua kondisi instalasi;
   b. melindungi reaktor terhadap kejadian alam dan kejadian akibat ulah manusia; dan
   c. sebagai perisai radiasi pada semua kondisi instalasi.

(2) Desain sistem penyungkup sebagaimana dimaksud pada ayat (1) harus:
   a. menjamin setiap pelepasan zat radioaktif ke lingkungan dalam kecelakaan dasar desain dengan nilai berada di bawah batas yang dapat diterima;
   b. mencegah kegagalan penyungkup selama kecelakaan parah yang merugikan integritas penyungkup;
   c. memudahkan perawatan, inspeksi, dan surveilan kondisi penyungkup dan fitur terkait;
   d. menjamin laju kebocoran maksimum yang ditetapkan tidak terlampaui dalam kecelakaan dasar desain dan serendah mungkin dalam kecelakaan yang melampaui dasar desain;dan
   e. memudahkan pengujian kebocoran selama operasi reaktor secara berkala baik pada tekanan desain maupun tekanan lebih rendah agar laju kebocoran sistem penyungkup pada tekanan desain dapat diketahui.

(3) Desain sistem penyungkup sebagaimana dimaksud pada ayat (1) harus memiliki paling sedikit:
   a. struktur kedap (*leaktighness*);

b. sistem pengendali level tekanan, temperatur, dan kelembaban; dan

c. fitur untuk mengisolasi, mengolah, mengendalikan dan memindahkan produk fisi, hidrogen, oksigen, dan zat radioaktif yang mungkin terlepas dari penyungkup ke lingkungan.

Pasal 91

(1) Kekuatan struktur penyungkup, termasuk akses, penetrasi dan katup isolasi, harus dihitung dengan margin keselamatan yang memadai berdasarkan potensi kejadian internal dan eksternal.

(2) Potensi kejadian internal sebagaimana dimaksud pada ayat (1) meliputi tekanan lebih (*overpressure*), tekanan kurang (*underpressure*), temperatur, efek dinamik yang ditimbulkan dari kejadian internal, gaya reaksi akibat kecelakaan dasar desain termasuk kemungkinan reaksi kimia dan radiolitik, dan penuaan.

(3) Potensi kejadian eksternal sebagaimana dimaksud pada ayat (1) meliputi kejadian alam dan kejadian akibat ulah manusia.

Pasal 92

(1) Struktur, sistem dan komponen penyungkup yang mempengaruhi kekedapan sistem penyungkup harus didesain dan dikonstruksi agar laju kebocoran penyungkup dapat diuji pada tekanan desain setelah seluruh penetrasi terpasang.

(2) Penetrasi sebagaimana dimaksud pada ayat (1) harus ada sesedikit mungkin dan memenuhi persyaratan desain sistem penyungkup.

Pasal 93

(1) Setiap jalur penetrasi yang menembus penyungkup sebagai bagian dari sistem pendingin reaktor atau yang terhubung langsung ke ruang penyungkup harus didesain mampu terisolasi secara otomatis dan andal pada kecelakaan dasar desain.

(2) Jalur penetrasi sebagaimana dimaksud pada ayat (1) harus memiliki paling sedikit 2 (dua) katup isolasi penyungkup yang memadai, yang terpasang secara seri pada bagian dalam dan luar penyungkup dan sedekat mungkin dengan penyungkup.

(3) Setiap jalur penetrasi yang bukan bagian dari sistem pendingin reaktor atau tidak terhubung langsung ke ruang penyungkup harus didesain memiliki paling sedikit 1 (satu) katup isolasi penyungkup yang memadai dan dipasang di luar penyungkup dan sedekat mungkin dengan penyungkup.

(4) Katup isolasi sebagaimana dimaksud pada ayat (2) dan (3) harus didesain mampu teraktuasi secara andal dan mandiri, dan mudah diuji secara berkala.

Pasal 94

(1) Sistem penyungkup harus didesain menyediakan sistem *airlocks* yang dilengkapi pintu-pintu *interlock* untuk akses personil selama kondisi operasi dan kecelakaan dasar desain.

(2) Sistem penyungkup sebagaimana dimaksud pada ayat (1) harus didesain menyediakan ketentuan pemantauan untuk petugas perawatan.

Pasal 95

(1) Sistem penyungkup harus didesain untuk mampu mengendalikan tekanan, temperatur, dan pembentukan produk fisi, padatan atau gas di dalam penyungkup.

(2) Desain sistem penyungkup sebagaimana dimaksud pada ayat (1) harus menyediakan jalur alir (*flow routes*) yang memadai antara kompartemen yang terpisah di dalam penyungkup.

(3) Ukuran tampang lintang bukaan (*openings*) antara kompartemen sebagaimana dimaksud pada ayat (2) harus menjamin agar perbedaan tekanan yang terjadi selama proses penyamaan tekanan dalam kondisi kecelakaan tidak mengakibatkan kerusakan pada:

a. struktur yang terkena beban tekanan; dan/atau

b. sistem lain yang berfungsi membatasi pengaruh kondisi kecelakaan.

(4) Sistem penyungkup harus didesain mampu memindahkan panas dari penyungkup reaktor dengan cara menurunkan tekanan dan temperatur, dan mempertahankan tekanan dan temperatur serendah mungkin yang dapat diterima setelah pelepasan fluida energi tinggi pada kecelakaan dasar desain.

Pasal 96

(1) Pelapis dan pelindung untuk struktur dan komponen di dalam sistem penyungkup harus dipilih dengan tepat.

(2) Metode pemasangan dan peletakan pelapis dan pelindung sebagaimana dimaksud pada ayat (1) harus ditetapkan untuk menjamin terpenuhinya fungsi keselamatan, dan untuk meminimalkan gangguan terhadap fungsi keselamatan struktur, sistem dan komponen lainnya apabila terjadi kerusakan pelapis dan pelindung.

Pasal 97

Ketentuan mengenai desain sistem penyungkup diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Ketujuh

Sistem Instrumentasi dan Kendali

Pasal 98

Reaktor daya harus didesain menyediakan:

a. sistem instrumentasi untuk mengukur semua parameter utama yang mempengaruhi reaksi fisi, integritas teras reaktor, sistem pendingin dan sistem penyungkup reaktor dalam semua kondisi instalasi;

b. sistem kendali yang andal dan tepat untuk mengendalikan dan mempertahankan parameter dalam BKO;dan

c. sistem instrumentasi dan peralatan perekaman untuk memantau kecelakaan dasar desain dan status struktur, sistem yang penting untuk keselamatan, dan untuk memperkirakan lokasi dan jumlah zat radioaktif yang terlepas ke lingkungan.

Pasal 99

(1) Sistem instrumentasi dan kendali harus didesain dengan keandalan yang tinggi, mampu diuji secara berkala sesuai dengan fungsi keselamatan, dan memenuhi kriteria kegagalan tunggal.

(2) Pengujian secara berkala sebagaimana dimaksud pada ayat (1) meliputi:

   a. pengujian kanal secara mandiri; dan

   b. uji fungsi dari sensor hingga aktuator akhir atau penampil.

Pasal 100

(1) Dalam hal desain sistem instrumentasi dan kendali untuk sistem yang penting untuk keselamatan bergantung pada keandalan sistem berbasis komputer, standar yang memadai dan praktek pengembangan dan pengujian perangkat lunak dan keras harus ditetapkan dan diadopsi selama umur sistem.

(2) Tingkat keandalan dari perangkat lunak komputer harus sesuai dengan kepentingan keselamatan sistem.

(3) Apabila sistem berbasis komputer digunakan dalam sistem keselamatan, sistem berbasis komputer harus:

a. menggunakan perangkat keras dan lunak bermutu tinggi dan berdasarkan pengalaman terbaik;

b. dilengkapi dengan sistem pendokumentasian dan penilaian yang sistematis untuk semua proses pengembangan termasuk pengendalian, pengujian dan komisioning perubahan desain;

c. dikaji oleh ahli yang mandiri dari pendesain dan pemasok untuk mengkonfirmasi keandalan sistem;

d. dilengkapi dengan upaya yang beragam untuk memenuhi fungsi proteksi apabila integritas sistem tidak dapat ditunjukkan dengan tingkat keandalan; dan

e. dilengkapi dengan perangkat lunak yang tidak berpotensi mengakibatkan kegagalan penyebab sama.

Pasal 101

(1) Sistem instrumentasi dan kendali harus didesain untuk mencegah interferensi antara sistem keselamatan dan sistem yang memiliki kelas lebih rendah atau komponen yang redundan dari sistem dengan kelas yang sama.

(2) Dalam hal digunakan sinyal yang sama untuk sistem keselamatan dan sistem kendali, desain sistem instrumentasi dan kendali harus memastikan pemisahan yang memadai.

(3) Sumber sinyal sebagaimana dimaksud pada ayat (2) harus diklasifikasi sebagai sistem dalam kelas yang sama dengan sistem keselamatan.

(4) Komponen sistem keselamatan harus mudah diidentifikasi untuk tujuan pemisahan fisik.

Pasal 102

(1) Reaktor daya harus didesain menyediakan ruang kendali utama untuk:

a. mengoperasikan reaktor daya secara otomatis dan manual dengan selamat dalam semua kondisi instalasi; dan

b. mempertahankan reaktor daya dalam kondisi selamat setelah terjadinya kejadian operasi terantisipasi atau kondisi kecelakaan.

(2) Ruang kendali utama sebagaimana dimaksud pada ayat (1) harus didesain:

a. untuk melindungi setiap personil dari bahaya radiasi, pelepasan zat radioaktif, ledakan, kebakaran, atau gas beracun;

b. mempertimbangkan kejadian internal dan eksternal yang memiliki ancaman langsung pada keberlangsungan operasi; dan

c. menyediakan upaya untuk meminimalkan potensi kejadian internal dan eksternal.

Pasal 103

(1) Reaktor daya harus didesain menyediakan ruang kendali tambahan dengan instrumentasi dan kendali yang terpisah secara fisik dan catu daya yang mandiri dari ruang kendali utama.

(2) Ruang kendali tambahan sebagaimana dimaksud pada ayat (1) harus didesain untuk:

a. mampu mempertahankan kondisi *shutdown*, memindahkan panas sisa, dan memantau parameter fungsi keselamatan;dan

b. melindungi setiap petugas pengoperasi reaktor daya dari bahaya radiasi, pelepasan zat radioaktif, ledakan, kebakaran, atau gas beracun.

Pasal 104

Ketentuan mengenai sistem instrumentasi dan kendali yang penting untuk keselamatan dan perangkat lunak untuk sistem berbasis komputer yang penting untuk keselamatan diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Kedelapan

Sistem Penanganan dan Penyimpanan Bahan Bakar Nuklir

Pasal 105

(1) Reaktor daya harus didesain menyediakan sistem penanganan dan penyimpanan bahan bakar nuklir untuk menjamin integritas dan sifat bahan bakar nuklir selama penanganan dan penyimpanan, termasuk fitur untuk kemudahan pengangkutan dan penanganan bahan bakar nuklir segar, bahan bakar nuklir bekas, dan limbah radioaktif.

(2) Desain reaktor daya sebagaimana dimaksud pada ayat (1) harus mempertimbangkan akses dalam pengangkutan bungkusan dan kemampuan bongkar muat bungkusan.

Pasal 106

(1) Sistem penanganan dan penyimpanan untuk bahan bakar nuklir segar harus didesain untuk:

a. mencegah kekritisan dengan margin yang ditentukan melalui upaya fisik atau proses, dan konfigurasi geometri;

b. memudahkan inspeksi bahan bakar nuklir segar;

c. memudahkan perawatan, inspeksi berkala, dan surveilan komponen yang memadai dan penting untuk keselamatan;

d. meminimalkan kebolehjadian kehilangan atau kerusakan bahan bakar nuklir;

e. menyediakan cara indentifikasi perangkat bahan bakar nuklir;

f. menyediakan sarana untuk proteksi radiasi; dan

g. menyediakan prosedur penanganan, dan pertanggungjawaban dan pengendalian bahan nuklir.

(2) Sistem penanganan dan penyimpanan bahan bakar teriradiasi harus didesain untuk:

a. mencegah kekritisan dengan margin yang ditentukan melalui upaya fisik atau proses, dan konfigurasi geometri;

b. mampu memindahkan panas secara memadai dalam kondisi operasi dan kecelakaan dasar desain;

c. memudahkan inspeksi bahan bakar nuklir teriradiasi;

d. memudahkan inspeksi dan surveilan berkala terhadap komponen yang penting untuk keselamatan;

e. mencegah jatuhnya bahan bakar nuklir selama pemindahan;

f. mencegah tegangan mekanik (*stress*) berlebih saat penanganan elemen atau perangkat bahan bakar nuklir;

g. mencegah jatuhnya benda berat pada bahan bakar nuklir;

h. menyimpan secara selamat bahan bakar nuklir yang cacat atau rusak;

i. menyediakan sarana dan metode yang tepat untuk proteksi radiasi;

j. memudahkan identifikasi setiap modul bahan bakar nuklir;

k. memudahkan pengangkatan, pemindahan dan penempatan bahan bakar nuklir teriradiasi;

l. mengendalikan tingkat larutan penyerap jika digunakan;

m. memudahkan perawatan dan dekomisioning fasilitas penanganan dan penyimpanan bahan bakar nuklir;

n. memudahkan dekontaminasi area dan peralatan penanganan dan penyimpanan bahan bakar nuklir;

o. menyediakan prosedur penanganan, dan pertanggungjawaban dan pengendalian bahan nuklir; dan

p. menyimpan semua bahan bakar nuklir yang dikeluarkan dari teras reaktor sesuai strategi perencanaan manajemen teras dan teras penuh dengan marjin yang memadai.

(3) Untuk reaktor yang menggunakan sistem kolam air untuk penyimpanan bahan bakar nuklir, sistem penyimpanan bahan bakar nuklir harus didesain menyediakan paling sedikit:

a. sarana untuk mengendalikan temperatur, sifat kimia dan aktivitas air;

b. sarana untuk memantau dan mengendalikan ketinggian air kolam penyimpanan;

c. sarana untuk mendeteksi kebocoran; dan

d. sarana untuk mencegah kehilangan air kolam akibat kejadian pecahnya pipa melalui upaya pemasangan antisifon.

Pasal 107

Ketentuan mengenai desain penanganan dan penyimpanan bahan bakar nuklir dan desain fasilitas penyimpanan bahan bakar diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Kesembilan

Sistem Catu Daya Listrik

Pasal 108

(1) Reaktor daya harus didesain menyediakan sistem catu daya listrik normal dan darurat.

(2) Desain sistem catu daya listrik sebagaimana dimaksud pada ayat (1) harus memperhitungkan interaksi antara fasilitas dengan jaringan listrik (*grid*).

(3) Interaksi antara fasilitas dengan jaringan listrik (*grid*) sebagaimana dimaksud pada ayat (2) paling sedikit meliputi:

a. independensi jalur pasokan daya listrik;

b. jumlah jalur pasokan daya listrik;

c. variasi tegangan dan frekuensi jaringan listrik; dan

d. level kegagalan sistem, terkait keandalan pasokan daya listrik untuk sistem yang penting untuk keselamatan.

Pasal 109

(1) Sistem catu daya listrik darurat sebagaimana dimaksud dalam Pasal 108 harus didesain mampu memasok daya yang dibutuhkan dalam

setiap kondisi instalasi dalam kejadian kehilangan daya listrik dari jaringan listrik (*grid*).

(2) Untuk menentukan kemampuan, ketersediaan, rentang waktu permintaan pasokan daya listrik, kapasitas dan persyaratan kontinuitas operasinya, dasar desain sistem catu daya listrik darurat sebagaimana dimaksud pada ayat (1) harus memperhitungkan:

a. PIE; dan

b. Kinerja fungsi keselamatan

(3) Sistem catu daya listrik darurat dapat dipasok dari sistem catu daya listrik dan non listrik.

(4) Sistem catu daya listrik darurat sebagaimana dimaksud pada ayat (3) harus memenuhi persyaratan yang sesuai dengan persyaratan sistem keselamatan.

(5) Dasar desain mesin diesel atau sistem catu daya lain yang memasok daya listrik untuk sistem terkait keselamatan paling sedikit memiliki:

a. kemampuan menyimpan dan menyalurkan bahan bakar mesin diesel untuk memenuhi permintaan daya listrik yang dibutuhkan;

b. kemampuan menghidupkan dan mengoperasikan mesin diesel dalam semua kondisi yang ditetapkan dan pada waktu yang dibutuhkan; dan

c. sistem penunjang operasi yang meliputi pendinginan.

Paragraf Kesepuluh

Sistem Penanganan Limbah Radioaktif

Pasal 110

(1) Reaktor daya harus didesain menyediakan sistem untuk menangani limbah radioaktif (efluen) berbentuk padat, cair dan gas untuk mempertahankan kuantitas dan konsentrasi lepasan radioaktif dalam batas yang ditetapkan dan serendah mungkin yang dapat dicapai.

(2) Sistem penanganan limbah radioaktif sebagaimana dimaksud pada ayat (1) harus didesain dalam menangani dan menyimpan limbah radioaktif selama umur operasi reaktor dan pasca-operasi yang direncanakan di tapak secara selamat.

(3) Desain sistem penanganan limbah radioaktif harus mempertimbangkan metode dan cara yang memadai untuk menekan sekecil mungkin dosis yang diterima personil dan pelepasannya ke lingkungan.

(4) Sistem penanganan limbah radioaktif harus didesain menyediakan sistem ventilasi gedung dengan kemampuan membersihkan (*cleanup*) untuk:

a. mencegah terdispersinya zat radioaktif di dalam gedung;

b. mengurangi konsentrasi zat radioaktif di dalam gedung hingga ke level yang sesuai dengan persyaratan agar dapat diakses oleh personil pada area tertentu;

c. mempertahankan lepasan zat radioaktif di dalam gedung di bawah batas yang ditetapkan, dan menerapkan prinsip ALARA dalam kondisi operasi dan kecelakaan dasar desain;

d. mensirkulasikan udara yang mengandung gas mulia dan beracun (*noxious*) tanpa mempengaruhi kemampuan mengendalikan lepasan radioaktif; dan

e. mengendalikan lepasan radioaktif gas ke lingkungan dalam batas yang ditetapkan dan serendah mungkin yang dapat dicapai.

(5) Sistem penanganan limbah radioaktif harus didesain menyediakan peralatan yang dapat menjebak (*offgas/extract stream)* untuk memenuhi batas lepasan dengan sistem saringan yang dapat diuji efisiensinya.

Pasal 111

Ketentuan mengenai desain pengelolaan, pengendalian, penanganan dan penyimpanan limbah radioaktif di instalasi diatur tersendiri dengan Peraturan Kepala BAPETEN.

Paragraf Kesebelas

Sistem Bantu

Pasal 112

(1) Reaktor daya harus didesain menyediakan sistem bantu dengan keandalan yang sesuai dengan struktur, sistem dan komponen yang berhubungan.

(2) Sistem bantu sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:

a. sistem pencuplikan proses dan pascakecelakaan;

b. sistem perpindahan panas bantu (*auxiliary*);

c. sistem udara bertekanan (*air compressed*);

d. sistem ventilasi dan pengkondisi udara;

e. sistem proteksi kebakaran;

f. sistem pencahayaan; dan

g. peralatan angkat-angkut.

Pasal 113

(1) Sistem pencuplikan proses dan pascakecelakaan sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf a harus didesain untuk mampu menentukan konsentrasi radionuklida tertentu secara tepat waktu dalam sistem proses fluida, dan sampel gas dan cairan yang diambil dari sistem atau lingkungan pada kondisi operasi dan kondisi kecelakaan.

(2) Desain sebagaimana dimaksud pada ayat (1) harus menyediakan sarana pemantauan aktivitas sistem fluida yang memiliki kontaminasi yang signifikan, dan untuk pengumpulan sampel proses.

Pasal 114

(1) Sistem perpindahan panas bantu (*auxiliary*) sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf b, harus didesain untuk mampu memindahkan panas dari sistem dan komponen yang penting untuk kondisi *shutdown* selamat pada kondisi normal dan kondisi kecelakaan.

(2) Desain sebagaimana dimaksud pada ayat (1) harus memastikan bagian sistem yang tidak penting dapat diisolasi.

Pasal 115

Sistem udara bertekanan (*air compressed*) sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf c, harus didesain untuk mampu mempertahankan kondisi lingkungan untuk sistem dan komponen yang penting untuk keselamatan dalam kondisi operasi normal dan kondisi kecelakaan.

Pasal 116

Sistem ventilasi, pendingin, pemanas, dan pengkondisi udara sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf d, harus didesain untuk mampu mempertahankan kondisi lingkungan untuk sistem dan komponen yang penting untuk keselamatan dalam kondisi operasi normal dan kondisi kecelakaan.

Pasal 117

(1) Sistem proteksi kebakaran sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf e, harus didesain terpasang di seluruh instalasi berdasarkan pada analisis bahaya kebakaran.

(2) Sistem proteksi kebakaran sebagaimana dimaksud pada ayat (1) paling sedikit mencakup sistem deteksi dan pemadam kebakaran, penghalang kebakaran, dan sistem pengendali asap.

(3) Sistem deteksi kebakaran sebagaimana dimaksud pada ayat (2) harus didesain mampu menberikan informasi kepada operator dengan seketika mengenai asal lokasi kebakaran dan penyebarannya.

(4) Sistem pemadam kebakaran sebagaimana dimaksud pada ayat (2) harus didesain mampu beroperasi secara otomatis dan memastikan beroperasinya karena sinyal palsu atau ketidaksengajaan tidak akan mengganggu kemampuan struktur, sistem, dan komponen yang penting untuk keselamatan, dan tidak mempengaruhi kelompok keselamatan yang redundan secara simultan.

(5) Sistem deteksi dan pemadam kebakaran sebagaimana dimaksud pada ayat (2) untuk menanggulangi kebakaran setelah PIE harus didesain memiliki kualifikasi tahan terhadap pengaruh kejadian awal terspotulasi.

(6) Bahan yang digunakan dalam instalasi harus didesain tahan panas dan tahan api atau tidak terbakar khususnya pada penyungkup dan ruang kendali.

Pasal 118

Sistem pencahayaan sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf f, harus didesain mampu mendukung operasi yang selamat dalam kondisi operasi normal dan kondisi kecelakaan di seluruh area kegiatan operasi.

Pasal 119

(1) Peralatan angkat-angkut sebagaimana dimaksud dalam Pasal 112 ayat (2) huruf g, harus didesain untuk mengangkat dan menurunkan komponen di sekitar struktur, sistem, dan komponen yang penting untuk keselamatan.

(2) Peralatan angkat-angkut sebagaimana dimaksud pada ayat (1) harus didesain:

a. mencegah diangkatnya beban yang berlebih atau yang tidak dapat diterima; dan

b. meminimalkan kemungkinan jatuhnya beban.

(3) Tata letak fasilitas peralatan harus didesain memudahkan pergerakan peralatan sebagaimana yang dimaksud pada ayat (1) secara selamat.

Paragraf Keduabelas

Sistem Konversi Daya

Pasal 120

(1) Reaktor daya harus didesain menyediakan sistem pemasok uap dengan batas desain yang memadai sehingga batas pendingin bertekanan tidak

terlampaui dalam kondisi operasi normal, kejadian operasi terantisipasi, dan kondisi kecelakaan dasar desain.

(2) Sistem pemasok uap sebagaimana dimaksud pada ayat (1) harus didesain dengan memiliki katup isolasi uap air yang terkualifikasi secara memadai yang mampu menutup dalam kondisi tertentu.

(3) Sistem air umpan dan uap harus didesain memiliki kapasitas yang memadai dan mencegah kejadian operasi terantisipasi meningkat menjadi kondisi kecelakaan.

(4) Generator turbin harus didesain menyediakan proteksi terhadap kecepatan lebih dan/atau vibrasi, dan meminimalkan pengaruh desintegrasi turbin terhadap struktur, sistem, dan komponen yang penting untuk keselamatan.

Pasal 121

Reaktor daya harus didesain meminimalkan interaksi antara bangunan yang berisi struktur, sistem, dan komponen yang terkait keselamatan termasuk kabel catu daya dan kendali dengan struktur lainnya, yang disebabkan oleh kejadian eksternal.

Paragraf Ketigabelas

Fitur Keselamatan Teknis

Pasal 122

(1) Fitur keselamatan teknis sebagaimana dimaksud dalam Pasal 39 ayat (3) huruf m harus ditetapkan berdasarkan analisis keselamatan.

(2) Fitur keselamatan teknis harus didesain dengan menyediakan sistem pendingin teras darurat, sistem penyungkup, sistem kemampuhunian (*habitability system*), sistem pemindahan dan pengendali hasil fisi, dan sistem keselamatan teknis lainnya.

(3) Sistem dan subsistem yang penting untuk pengoperasian fitur keselamatan teknis harus tersedia.

(4) Fitur keselamatan teknis harus didesain berfungsi secara otomatis.

(5) Dalam hal sistem otomatis tidak berfungsi, Pemegang izin harus menjamin desain fitur keselamatan teknis berfungsi secara manual.

(6) Pemegang izin harus menjamin desain fitur keselamatan teknis dengan mempertimbangkan:

a. keandalan komponen, kemandirian sistem, redundansi, karakteristik gagal selamat, keragaman dan pemisahan fisik antar sistem redundansi;

b. penggunaan bahan yang tahan terhadap kondisi kecelakaan dasar desain yang terpostulasi; dan

c. tindakan surveilan, inspeksi dan surveilan untuk memastikan fitur keselamatan teknis dapat diandalkan dan efektif saat diperlukan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Kepala Badan Pengawas Tenaga Nuklir ini dengan penempatannya dalam Berita Negara Republik Indonesia

Ditetapkan di Jakarta
pada tanggal 14 Januari 2011
KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA,

AS NATIO LASMAN

Diundangkan di Jakarta
pada tanggal 24 Agustus 2011
MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

PATRIALIS AKBAR

LAMPIRAN I

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

REPUBLIK INDONESIA

NOMOR 3 TAHUN 2011

TENTANG

KETENTUAN KESELAMATAN DESAIN REAKTOR DAYA

KEJADIAN AWAL TERPOSTULASI (PIE)

1.1. Lampiran ini menjelaskan definisi dan penerapan konsep PIE.

1.2. PIE didefinisikan sebagai kejadian yang diidentifikasi pada desain sebagai hal yang mengakibatkan kejadian operasi terantisipasi (AOO) atau kondisi kecelakaan. Dengan demikian, PIE itu sendiri bukan merupakan kecelakaan, tetapi adalah kejadian yang memulai suatu rangkaian kejadian dan yang mengakibatkan kejadian operasi terantisipasi (AOO), kecelakaan dasar desain, atau kecelakaan parah bergantung pada kegagalan tambahan yang terjadi. Contoh umumnya adalah: kegagalan peralatan (termasuk pecahnya pipa), kesalahan manusia, kejadian yang disebabkan oleh manusia atau kejadian alam.

1.3. PIE dapat berupa kejadian yang mempunyai dampak kecil, seperti kegagalan komponen redundan, atau dapat mempunyai dampak serius, seperti kegagalan pipa utama pada sistem pendingin reaktor. Tujuan utama desain adalah mencapai ciri instalasi yang memastikan bahwa mayoritas PIE mempunyai dampak yang kecil atau bahkan tidak signifikan, dan bahwa jika ada PIE yang mengakibatkan DBA, maka dampaknya dapat diterima; atau jika ada PIE yang mengakibatkan kecelakaan parah, maka dampaknya dibatasi oleh fitur desain dan manajemen kecelakaan.

1.4. Rentang kejadian yang lengkap perlu dipostulasikan untuk memastikan bahwa semua kejadian yang dapat terjadi dengan potensi dampak yang serius dan kebolehjadian yang signifikan telah diantisipasi dan dapat diatasi oleh desain instalasi. Tidak ada kriteria yang ketat untuk menentukan pemilihan PIE; prosesnya lebih merupakan kombinasi iterasi antara desain dan analisis, penilaian teknis dan pengalaman dari desain dan operasi instalasi sebelumnya. Jika suatu rangkaian kejadian tidak dimasukkan sebagai PIE, maka hal ini perlu dijustifikasi.

1.5. Jumlah PIE yang digunakan di dalam pengembangan persyaratan kinerja untuk peralatan yang penting untuk keselamatan dan di dalam keseluruhan penilaian keselamatan instalasi dibatasi untuk melakukan pengembangan secara praktis.
Pembatasan jumlah kejadian tersebut dilakukan dengan membatasi analisis rinci menjadi sejumlah rangkaian kejadian yang representatif[1]. Rangkaian kejadian yang representatif mengidentifikasi kasus yang penting dan menyediakan dasar bagi batas desain numerik untuk struktur, sistem, dan komponen yang penting untuk keselamatan.

1.6. Beberapa PIE dapat ditentukan secara deterministik, berdasarkan pada berbagai faktor seperti pengalaman dari instalasi sebelumnya, persyaratan yang ditetapkan atau besarnya dampak yang dapat terjadi. PIE lain dapat ditentukan dengan menggunakan metoda sistematis, seperti analisis probabilistik karena fitur tertentu dari desain, lokasi instalasi atau pengalaman operasi memungkinkan karakteristik instalasi dikuantifikasi secara probabilistik.

Jenis-Jenis PIE

Kejadian Internal
Kegagalan peralatan

1.7. Kejadian awal dapat berupa kegagalan peralatan tunggal yang dapat secara langsung atau tidak langsung mempengaruhi keselamatan instalasi. Daftar kejadian tersebut secara memadai mewakili semua kegagalan sistem dan komponen instalasi yang dapat terjadi.

---

[1] Istilah ‘rangkaian kejadian’ atau ‘rangkaian dari kejadian’ digunakan untuk menyebut kombinasi antara PIE dan tindakan operator selanjutnya atau tindakan untuk peralatan yang penting untuk keselamatan.

1.8. Jenis kegagalan yang perlu dipertimbangkan bergantung pada jenis sistem atau
komponen yang digunakan. Kegagalan dalam pengertian yang paling luas adalah hilangnya kemampuan sistem atau komponen untuk melakukan fungsinya atau terlaksananya fungsi yang tidak dikehendaki. Sebagai contoh, gagalnya suatu pipa dapat berupa bocor, pecah atau penyumbatan jalur aliran. Untuk komponen aktif seperti katup, kegagalan dapat berupa: tidak membuka atau menutup ketika diperlukan, membuka atau menutup ketika tidak diperlukan, membuka atau menutup sebagian, atau membuka atau menutup pada kecepatan yang tidak semestinya. Untuk peralatan seperti transduser, kegagalan dapat berupa kesalahan di luar rentang kesalahan yang diperbolehkan, ketiadaan keluaran, keluaran maksimum yang konstan, keluaran yang tidak menentu atau kombinasinya.

1.9. Dengan meningkatnya penggunaan sistem berbasis komputer dalam penerapan keselamatan dan penerapan yang penting untuk keselamatan, kegagalan piranti keras atau program piranti lunak yang tidak benar dapat menyebabkan tindakan kendali yang signifikan; kemungkinan ini dipertimbangkan.

Kesalahan manusia

1.10. Dalam banyak kasus, dampak kesalahan manusia akan serupa dengan dampak kegagalan komponen. Kesalahan manusia dapat mencakup mulai dari pelaksanaan perawatan yang salah atau tidak lengkap, hingga kesalahan pengaturan batas peralatan kendali atau tindakan operator yang salah atau tidak dilakukan.

Kejadian internal lain

1.11. Kebakaran, ledakan dan genangan dari sumber internal juga berpotensi mempengaruhi kinerja keselamatan instalasi dan umumnya dimasukkan di dalam penyusunan daftar PIE.

Kejadian Eksternal

1.12. Contoh kejadian eksternal dan penentuan masukan dasar desain yang relevan untuk instalasi diberikan di dalam Ketentuan Keselamatan Evaluasi Tapak PLTN berikut pedoman terkait. Kejadian eksternal ini pada umumnya mempersyaratkan desain struktur, sistem dan komponen instalasi untuk beban tambahan jenis getaran, tumbukan dan tekanan.

1.13. Jika kemungkinan kegagalan struktur, sistem atau komponen yang penting untuk keselamatan akibat kejadian eksternal karena faktor alam atau akibat kegiatan manusia dapat dianggap cukup rendah karena desain dan konstruksi yang memadai, maka kegagalan yang disebabkan oleh kejadian tersebut tidak perlu dimasukkan ke dalam dasar desain instalasi.

Kombinasi Kejadian

1.14. Kombinasi kejadian tunggal pada analisis kecelakaan perlu diperhatikan untuk memastikan bahwa terdapat alasan yang dapat diterima untuk kombinasi kejadian tersebut. Kombinasi kejadian yang acak dapat merupakan skenario yang sangat tidak mungkin yang ditunjukkan di dalam analisis keselamatan probabilistik sebagai suatu kejadian yang jarang terjadi dan dapat diabaikan dan tidak diambil sebagai kecelakaan terpostulasi. Dalam analisis keselamatan probabilistik, pendekatan dengan menggunakan analisis estimasi terbaik digunakan untuk kecelakaan parah, sementara tindakan konservatif diterapkan pada pendekatan analitik untuk kecelakaan terpostulasi yang mempunyai kebolehjadian yang lebih besar.

1.15. Dalam menentukan kejadian yang akan dikombinasikan, perlu dipertimbangkan tiga periode waktu:

a. periode jangka panjang, yaitu sebelum kejadian;
b. periode jangka pendek, termasuk timbulnya kejadian dan efek jangka pendeknya;dan
c. periode pemulihan pascakejadian.

1.16. Tindakan koreksi dapat diasumsikan telah diambil untuk kejadian yang terjadi pada periode jangka panjang sebelum timbulnya kejadian lain jika ketentuan yang tepat untuk mengidentifikasinya telah dimasukkan ke dalam desain instalasi dan jika waktu yang diperlukan untuk tindakan koreksinya pendek. Dalam hal ini, kombinasi dari kejadian-kejadian yang demikian tidak perlu dipertimbangkan.

1.17. Untuk periode jangka pendek (biasanya berdurasi jam), probabilitas kejadian tunggal yang diperkirakan sedemikian sehingga kombinasi yang terjadi secara acak dapat diabaikan.

1.18. Untuk periode pemulihan pascakejadian (dalam hitungan hari atau lebih), kejadian tambahan perlu diperhitungkan, bergantung pada lama periode pemulihan dan probabilitas kejadian yang diperkirakan. Untuk periode pemulihan, dapat diasumsikan bahwa keparahan suatu kejadian yang harus diambil dalam suatu kombinasi tidak sebesar yang diasumsikan untuk kejadian sejenis yang dipertimbangkan pada rentang waktu yang setara dengan umur instalasi. Sebagai contoh, dalam periode pemulihan untuk kecelakaan kehilangan pendingin, jika kombinasi acak dengan gempabumi perlu dipertimbangkan, keparahannya dapat dianggap lebih kecil daripada keparahan untuk dasar desain gempa bumi untuk instalasi.

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA,

AS NATIO LASMAN

LAMPIRAN II

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

REPUBLIK INDONESIA

NOMOR 3 TAHUN

TENTANG

KETENTUAN KESELAMATAN DESAIN REAKTOR DAYA

FUNGSI-FUNGSI KESELAMATAN UNTUK REAKTOR
AIR MENDIDIH, REAKTOR AIR BERTEKANAN,
DAN REAKTOR TABUNG TEKAN

2.1. Lampiran ini menjelaskan tiga fungsi keselamatan dasar reaktor sebagaimana dimaksud dalam Pasal 8.

2.2. Fungsi keselamatan ini mencakup fungsi yang diperlukan untuk mencegah kondisi kecelakaan serta memitigasi dampak kondisi kecelakaan. Fungsi keselamatan tersebut dapat dipenuhi dengan menggunakan struktur, sistem atau komponen yang diperlukan untuk operasi normal, untuk mencegah AOO agar tidak mengakibatkan kondisi kecelakaan, atau untuk memitigasi dampak kondisi kecelakaan.

2.3. Tinjauan mengenai berbagai desain reaktor menunjukkan bahwa persyaratan keselamatan desain dapat dipenuhi dengan memiliki struktur, sistem atau komponen yang melaksanakan fungsi-fungsi keselamatan berikut:

a. mencegah transien reaktivitas yang tidak dapat diterima;
b. mempertahankan reaktor dalam kondisi *shutdown* yang aman setelah melalui semua tindakan *shutdown*;
c. me-*shutdown* reaktor apabila diperlukan untuk mencegah terjadinya AOO yang mengakibatkan DBA dan me-*shutdown* reaktor untul memitigasi dampak DBA;
d. mempertahankan inventori pendingin reaktor agar cukup untuk mendinginkan teras selama dan setelah kondisi kecelakaan yang tidak melibatkan kegagalan pada batas tekanan pendingin reaktor;

e. mempertahankan inventori pendingin reaktor agar cukup untuk mendinginkan teras selama dan setelah terjadinya semua PIE yang diperhitungkan di dalam dasar desain;
f. membuang panas dari teras[2] setelah terjadinya kegagalan pada batas tekanan pendingin reaktor guna membatasi kerusakan bahan bakar;
g. membuang panas sisa pada kondisi operasi dan kondisi kecelakaan yang sesuai dengan seluruh batas tekanan pendingin reaktor;
h. memindahkan panas dari sistem keselamatan yang lain ke pembuangan panas akhir[3];
i. menjamin layanan yang diperlukan (seperti listrik, pneumatik, pasokan daya hidrolik, pelumasan) sebagai fungsi pendukung sistem keselamatan;
j. mempertahankan integritas yang dapat diterima dari kelongsong bahan bakar di teras reaktor;
k. mempertahankan integritas batas tekanan pendingin reaktor;
l. membatasi pelepasan zat radioaktif dari pengungkung reaktor dalam kondisi kecelakaan dan kondisi setelah kecelakaan;
m. membatasi paparan radiasi ke masyarakat dan personil pada tapak selama dan sesudah DBA dan kecelakaan parah terpilih yang melepaskan zat radioaktif dari sumber di luar penyungkup reaktor;
n. membatasi pembuangan (*discharge*) atau pelepasan (*release*) limbah radioaktif dan zat radioaktif di udara di bawah batas yang ditentukan pada semua status operasi;
o. mengendalikan kondisi lingkungan di dalam instalasi untuk pengoperasian sistem keselamatan dan untuk kelayakan tempat kerja bagi personil yang diperlukan untuk melaksanakan operasi yang penting untuk keselamatan;

---

2 Fungsi keselamatan ini berlaku pada langkah pertama dari system pembuangan panas. Langkah-langkah berikutnya dicakup di dalam fungsi keselamatan (8).

3 Ini merupakan fungsi pendukung untuk sistem keselamatan yang lain ketika sistem tersebut harus melakukan fungsi keselamatannya.

p. mengendalikan pelepasan zat radioaktif dari bahan bakar teriradiasi yang diangkut atau disimpan di luar sistem pendingin reaktor, tetapi masih di dalam tapak, dalam segala status operasi;
q. membuang panas peluruhan dari bahan bakar teriradiasi yang disimpan di luar sistem pendingin reaktor, tetapi masih di dalam tapak;
r. mempertahankan kesubkritisan yang cukup dari bahan bakar yang disimpan di luar sistem pendingin reaktor, tetapi masih di dalam tapak; dan
s. mencegah kegagalan atau membatasi dampak kegagalan struktur, sistem atau komponen yang kegagalannya akan menyebabkan gangguan pada fungsi keselamatan.

2.4. Daftar fungsi keselamatan ini dapat digunakan sebagai dasar untuk menentukan apakah struktur, sistem+41 atau komponen melaksanakan atau memberikan kontribusi pada satu atau lebih fungsi keselamatan dan untuk memberikan dasar dalam memberikan pemeringkatan kepentingan yang sesuai untuk struktur, sistem, dan komponen keselamatan yang memberikan kontribusi pada berbagai fungsi keselamatan.

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA

AS NATIO LASMAN

LAMPIRAN III

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

NOMOR 3 TAHUN 2011

TENTANG

KETENTUAN KESELAMATAN DESAIN REAKTOR DAYA

REDUNDANSI, KERAGAMAN, DAN INDEPENDENSI

3.1. Lampiran ini menyajikan beberapa upaya desain yang dapat digunakan, jika perlu dalam kombinasi, untuk mencapai dan mempertahankan keandalan yang diperlukan sepadan dengan bobot fungsi keselamatan yang harus dipenuhi di dalam tingkat pertahanan berlapis yang relevan.

3.2. Meskipun tidak ada target kuantitatif universal yang dapat dinyatakan untuk persyaratan keandalan tunggal untuk setiap tingkat pertahanan berlapis, penekanan terbesar diberikan pada tingkat pertama. Hal ini juga konsisten dengan tujuan dari organisasi pengoperasi yang menghendaki ketersediaan yang tinggi dari instalasi untuk menghasilkan daya.

Kegagalan dengan penyebab sama

3.3. Kegagalan sejumlah alat atau komponen untuk melakukan fungsinya dapat terjadi akibat suatu kejadian atau penyebab tunggal. Kegagalan ini dapat mempengaruhi sejumlah peralatan berbeda yang penting untuk keselamatan secara serentak. Kejadian atau penyebabnya dapat berupa cacat desain, cacat fabrikasi, kesalahan operasi atau perawatan, peristiwa alam, kejadian akibat kegiatan manusia atau pengaruh berantai yang tidak diinginkan dari operasi atau kegagalan lain di dalam instalasi.

3.4. Kegagalan dengan penyebab sama dapat juga terjadi ketika sejumlah komponen dari jenis yang sama gagal pada saat yang bersamaan. Ini dapat disebabkan oleh hal-hal seperti perubahan pada kondisi lingkungan sekitar, kejenuhan sinyal, kesalahan perawatan yang berulang atau cacat desain.

3.5. Upaya yang tepat untuk meminimalkan pengaruh kegagalan dengan penyebab sama, seperti penerapan redundansi, keragaman dan independensi, perlu dilakukan sepanjang dapat diterapkan pada desain.

Redundansi

3.6. Redundansi, yaitu penggunaan lebih dari jumlah minimum dari seperangkat peralatan dalam rangka memenuhi fungsi keselamatan tertentu, merupakan suatu prinsip desain yang penting untuk mencapai keandalan yang tinggi pada sistem yang penting untuk keselamatan, dan untuk memenuhi kriteria kegagalan tunggal untuk sistem keselamatan. Redundansi memungkinkan kegagalan atau ketidaktersediaan sedikitnya satu set peralatan dapat ditoleransi tanpa kehilangan fungsinya. Sebagai contoh, tiga atau empat pompa bisa jadi disediakan untuk melakukan suatu fungsi tertentu meskipun dua pompa pun akan mampu melaksanakannya. Untuk tujuan redundansi, komponen yang sama atau berlainan dapat digunakan.

Keragaman

3.7. Keandalan beberapa sistem dapat ditingkatkan dengan menggunakan prinsip keragaman untuk mengurangi potensi kegagalan dengan penyebab sama.

3.8. Keragaman diterapkan pada sistem atau komponen redundan yang melakukan fungsi keselamatan yang sama dengan menggabungkan atribut yang berbeda ke dalam sistem atau komponen. Atribut ini dapat berupa prinsip operasi yang berbeda, variabel fisik yang berlainan, kondisi operasi yang berbeda, atau produk dari fabrikan yang berlainan.

3.9. Perhatian harus diterapkan untuk memastikan agar setiap keragaman yang digunakan benar-benar mencapai peningkatan keandalan yang diinginkan pada desain terbangun *(as built design)*. Sebagai contoh, untuk mengurangi potensi kegagalan dengan penyebab sama pendesain memeriksa penerapan keragaman pada kemiripan dalam bahan, komponen dan proses fabrikasi, atau prinsip operasi atau fitur pendukung umum. Jika komponen atau sistem yang beragam digunakan, harus ada jaminan yang dapat diterima bahwa penerapan keragaman yang demikian secara keseluruhan memberikan keuntungan, dengan memperhitungkan kerugian seperti kesulitan tambahan pada prosedur operasi, perawatan dan surveilan atau dampak penggunaan peralatan dengan keandalan yang lebih rendah.

Independensi

3.10. Keandalan sistem dapat ditingkatkan dengan mempertahankan fitur-fitur berikut untuk independensi dalam desain:

a. independensi di antara komponen sistem redundan;
b. independensi di antara komponen sistem dan pengaruh PIE sedemikian sehingga, misalnya, suatu PIE tidak menyebabkan kegagalan atau kehilangan sistem keselamatan atau fungsi keselamatan yang diperlukan untuk memitigasi dampaknya;
c. independensi yang tepat di antara sistem atau komponen yang berbeda kelas keselamatannya; dan
d. independensi di antara peralatan yang penting untuk keselamatan dan peralatan yang tidak penting untuk keselamatan.

3.11. Independensi diterapkan dalam desain sistem dengan menggunakan isolasi fungsi dan pemisahan fisik:

1. Isolasi fungsi

Isolasi fungsi digunakan untuk mengurangi kemungkinan interaksi yang merugikan di antara peralatan dan komponen redundan atau sistem yang saling terhubung akibat dari operasi normal atau abnormal atau kegagalan suatu komponen di dalam sistem.

2. Pemisahan fisik dan tata letak komponen instalasi

Desain dan tata letak sistem menggunakan pemisahan fisik sedapat mungkin untuk meningkatkan keyakinan bahwa independensi akan tercapai, khususnya dalam kaitannya dengan suatu kegagalan dengan penyebab sama.

Pemisahan fisik meliputi:

1. pemisahan secara geometri (misalnya jarak atau orientasi)
2. pemisahan dengan menggunakan pembatas; atau
3. pemisahan dengan cara kombinasi dari kedua hal di atas.

Pemilihan cara pemisahan akan bergantung pada PIE yang dipertimbangkan di dalam dasar desain, seperti pengaruh kebakaran, ledakan kimia, tubrukan pesawat, tumbukan misil, banjir, temperatur atau kelembaban yang ekstrim.

3.12. Beberapa area di dalam instalasi cenderung menjadi pusat berkumpulnya peralatan atau pengkabelan dari berbagai tingkat (kategori) bobot kepentingan bagi keselamatan. Contoh dari area-area yang demikian dapat berupa penetrasi penyungkup, pusat kendali motor, ruang penyebaran kabel, ruang peralatan, ruang kendali dan komputer proses

instalasi. Upaya yang tepat untuk menghindari kegagalan dengan penyebab sama harus sedapat mungkin dilakukan pada area-area tersebut.

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA,

AS NATIO LASMAN