LAMPIRAN I

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

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

AS NATIO LASMAN

LAMPIRAN II

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

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[1] 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[2];

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;

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

---

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

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

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

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,

AS NATIO LASMAN