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...

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...

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...

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...

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,

ttd

AS NATIO LASMAN