SALINAN

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR
NOMOR 6 TAHUN 2012
TENTANG
DESAIN SISTEM YANG PENTING UNTUK KESELAMATAN
BERBASIS KOMPUTER PADA REAKTOR DAYA

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN PENGAWAS TENAGA NUKLIR,

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 Desain Sistem yang Penting untuk Keselamatan Berbasis Komputer pada 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 Kepala Badan Pengawas Tenaga Nuklir Nomor 3 Tahun 2011 tentang Ketentuan Keselamatan Desain Reaktor Daya;

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR TENTANG DESAIN SISTEM YANG PENTING UNTUK KESELAMATAN BERBASIS KOMPUTER PADA REAKTOR DAYA.

Pasal 1 ...
jdih.bapeten.go.id

Pasal 1

Dalam Peraturan Kepala Badan Pengawas Tenaga Nuklir ini yang dimaksud dengan:

1. Struktur, Sistem, dan Komponen yang Penting untuk Keselamatan adalah struktur, sistem dan komponen yang menjadi bagian dari suatu sistem keselamatan dan/atau struktur, sistem, dan komponen yang apabila gagal atau terjadi malfungsi menyebabkan terjadinya paparan radiasi terhadap pekerja tapak atau anggota masyarakat.
2. Sistem yang Penting untuk Keselamatan Berbasis Komputer adalah sistem yang penting untuk keselamatan yang fungsinya sebagian atau secara keseluruhan dilakukan dengan menggunakan mikroprosesor, peralatan elektronika terprogram atau komputer.
3. Sistem Keselamatan adalah sistem yang penting untuk keselamatan, yang disediakan untuk menjamin *shutdown* dengan selamat, atau pemindahan panas sisa dari teras, atau untuk membatasi dampak kejadian operasi terantisipasi dan kecelakaan dasar desain.
4. Sistem Keselamatan Berbasis Komputer adalah sistem keselamatan yang fungsinya sebagian atau secara keseluruhan dilakukan dengan menggunakan mikroprosesor, peralatan elektronika terprogram atau komputer.
5. Keragaman adalah keberadaan dua atau lebih struktur, sistem, dan komponen untuk melaksanakan satu fungsi yang ditentukan, yang komponen atau sistemnya memiliki atribut yang berbeda untuk meminimalkan kegagalan dengan penyebab sama.
6. Redundansi adalah keberadaan struktur, sistem, dan komponen lebih dari satu, baik identik atau beragam, yang kesemuanya secara bersamaan menjalankan fungsi yang sama, sehingga kehilangan salah satu dari struktur, sistem, dan komponen tidak menyebabkan kehilangan keseluruhan fungsi yang ditentukan.

jdih.bapeten.go.id

7. Kemandirian adalah kemampuan masing-masing komponen atau sistem yang redundan untuk melaksanakan fungsi yang ditentukan, dengan kegagalan salah satu atau beberapa komponen dan sistem tidak mengganggu kemampuan komponen atau sistem yang lain untuk menjalankan fungsinya.
8. Kegagalan Tunggal adalah kegagalan yang mengakibatkan hilangnya kemampuan suatu komponen untuk melakukan fungsi keselamatan, dan semua kegagalan yang diakibatkannya.
9. Validasi adalah proses pengujian dan evaluasi untuk memastikan kesesuaian terhadap persyaratan fungsi, kinerja, dan antar muka.
10. Verifikasi adalah proses untuk memastikan hasil suatu tahap telah memenuhi ketentuan yang ditetapkan pada tahap sebelumnya.
11. Dependabilitas adalah gabungan dari keandalan, ketersediaan dan keselamatan.
12. Pemegang Izin yang selanjutnya disingkat PI adalah orang atau badan yang telah menerima izin Pemanfaatan Tenaga Nuklir dari BAPETEN.
13. Badan Pengawas Tenaga Nuklir yang selanjutnya disebut BAPETEN adalah badan pengawas sebagaimana dimaksud dalam Undang-Undang Nomor 10 Tahun 1997 tentang Ketenaganukliran.

Pasal 2

Peraturan Kepala BAPETEN ini bertujuan memberikan ketentuan bagi PI untuk menjamin terpenuhinya persyaratan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer pada reaktor daya.

Pasal 3

Sistem yang Penting untuk Keselamatan Berbasis Komputer harus didesain dengan memenuhi:

jdih.bapeten.go.id

a. persyaratan umum desain; dan
b. persyaratan teknis desain.

Pasal 4

(1) Persyaratan umum desain sebagaimana dimaksud dalam Pasal 3 huruf a meliputi:
   a. kesederhanaan dalam desain;
   b. jaminan mutu;
   c. pertahanan berlapis;
   d. Redundansi;
   e. Keragaman;
   f. desain gagal selamat, supervisi dan toleransi kegagalan;
   g. keamanan;
   h. kemudahan perawatan;
   i. representasi seluruh moda operasi;
   j. antarmuka manusia-mesin dan antisipasi keterbatasan manusia;
   k. pembuktian Dependabilitas;
   l. penyelesaian tindakan protektif;
   m. integritas sistem; dan
   n. kemudahan pengujian dan kalibrasi.
(2) Rincian persyaratan umum desain sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Kepala BAPETEN ini.

Pasal 5

Persyaratan teknis desain sebagaimana dimaksud dalam Pasal 3 huruf b terdiri dari:
a. persyaratan teknis desain untuk perangkat keras; dan
b. persyaratan teknis desain untuk perangkat lunak.

Pasal 6

(1) Persyaratan teknis desain untuk perangkat keras sebagaimana dimaksud dalam Pasal 5 huruf a meliputi:

jdih.bapeten.go.id

a. kriteria Kegagalan Tunggal;
b. mutu perangkat keras;
c. kualifikasi peralatan;
d. Kemandirian;
e. tampilan informasi; dan
f. inisiasi sistem proteksi.

(2) Rincian persyaratan teknis desain untuk perangkat keras sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Kepala BAPETEN ini.

Pasal 7

(1) Persyaratan teknis desain untuk perangkat lunak sebagaimana dimaksud dalam Pasal 5 huruf b meliputi:
a. fungsi yang akan dikerjakan;
b. keselamatan;
c. ketersediaan dan keandalan;
d. antarmuka;
e. batasan desain;
f. model;
g. kinerja pewaktuan;
h. akurasi komputasi;
i. keamanan;
j. struktur yang mudah dipahami dan diubah;
k. mampu telusur;
l. mampu prediksi;
m. konsistensi dan kelengkapan; dan
n. mampu Verifikasi.

(2) Rincian persyaratan teknis desain untuk perangkat lunak sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Kepala BAPETEN ini.

Pasal 8...

jdih.bapeten.go.id

Pasal 8

(1) PI harus menjamin bahwa tahapan pengembangan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer telah dilaksanakan dan didokumentasikan.
(2) Pada tahapan pengembangan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer sebagaimana dimaksud pada ayat (1) harus dilakukan Verifikasi dan Validasi.
(3) Rincian tahapan pengembangan desain, dan Verifikasi dan Validasi Sistem yang Penting untuk Keselamatan Berbasis Komputer sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Kepala BAPETEN ini.

Pasal 9

PI yang akan melaksanakan perubahan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer harus memperoleh persetujuan Kepala BAPETEN.

Pasal 10

Peraturan Kepala BAPETEN ini mulai berlaku pada tanggal diundangkan.

Agar...

jdih.bapeten.go.id

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Kepala BAPETEN ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 20 Juni 2012
KEPALA BADAN PENGAWAS TENAGA NUKLIR,

ttd.

AS NATIO LASMAN

Diundangkan di Jakarta
pada tanggal 25 Juni 2012
MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd.

AMIR SYAMSUDIN

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2012 NOMOR 654

Salinan sesuai dengan aslinya
BADAN PENGAWAS TENAGA NUKLIR
Kepala Biro Hukum dan Organisasi,

Berthie Isa

jdih.bapeten.go.id

KEPALA BADAN PENGAWAS TENAGA NUKLIR

REPUBLIK INDONESIA

LAMPIRAN I

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

NOMOR 6 TAHUN 2012

TENTANG

DESAIN SISTEM YANG PENTING UNTUK KESELAMATAN BERBASIS KOMPUTER PADA REAKTOR DAYA

PERSYARATAN UMUM DESAIN

Persyaratan umum desain Sistem yang Penting untuk Keselamatan Berbasis Komputer meliputi:

A. kesederhanaan dalam desain;
B. jaminan mutu;
C. pertahanan berlapis;
D. Redundansi;
E. Keragaman;
F. desain gagal selamat, supervisi dan toleransi kegagalan;
G. keamanan;
H. kemudahan perawatan;
I. representasi seluruh moda operasi;
J. antarmuka manusia-mesin dan antisipasi keterbatasan manusia;
K. pembuktian Dependabilitas;
L. penyelesaian tindakan protektif;
M. integritas sistem; dan
N. kemudahan pengujian dan kalibrasi.

A. Kesederhanaan dalam Desain

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain secara modular untuk menghindari kompleksitas fungsi sistem dan penerapannya.

Modul dan antarmuka Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain secara sederhana. Modul Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain menggunakan algoritma sederhana.

jdih.banten.go.id

Perangkat keras Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain mempunyai kinerja dan kapasitas yang memadai.

B. Jaminan Mutu

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memenuhi ketentuan jaminan mutu sesuai dengan sistem manajemen yang telah ditetapkan.

C. Pertahanan Berlapis

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain menerapkan prinsip pertahanan berlapis dalam pengembangannya.

D. Redundansi

Sistem Keselamatan Berbasis Komputer didesain menerapkan prinsip Redundansi.

E. Keragaman

Sistem Keselamatan Berbasis Komputer didesain menerapkan prinsip Keragaman yang meliputi:

1. fungsi dan komponen sistem pada tingkat yang berbeda;
2. metode;
3. bahasa;
4. peralatan; dan/atau
5. personil.

F. Desain Gagal Selamat, Supervisi dan Toleransi Kegagalan

Sistem Keselamatan Berbasis Komputer didesain menerapkan prinsip gagal selamat, supervisi dan mekanisme toleransi kegagalan.

Desain supervisi dicapai melalui penggunaan:

1. perangkat lunak untuk memastikan perangkat keras berfungsi; dan
2. perangkat eksternal seperti *watchdog timer*.

jdih.banten.go.id

Sistem Keselamatan Berbasis Komputer didesain memastikan respons selamat dari semua masukan melalui penggunaan:

1. desain defensif (*defensive design*) yaitu desain untuk mengantisipasi kesalahan pemakaian dan meminimalisasi dampak kesalahan pemakaian; dan
2. bahasa yang tepat, termasuk *safe subsets* dan teknik pengkodean (*coding*).

Toleransi kegagalan diimplementasikan melalui pendeteksian kegagalan perangkat keras dengan menggunakan perangkat lunak atau piranti luar untuk memastikan sistem tetap berfungsi dengan benar.

G. Keamanan

Sistem Keselamatan Berbasis Komputer dilengkapi dengan proteksi terhadap serangan fisik, penyusupan (*intruder*) sengaja dan tidak disengaja, pemalsuan (*fraud*), virus dan sebagainya. Sistem Keselamatan Berbasis Komputer didesain tidak terhubung secara langsung dengan jaringan di luar instalasi.

H. Kemudahan Perawatan

Sistem Keselamatan Berbasis Komputer didesain dapat memudahkan deteksi lokasi dan diagnosis kegagalan sehingga sistem dapat diperbaiki atau diganti secara efisien.

Sistem yang Penting untuk Keselamatan berbasis Komputer didesain menggunakan struktur modular sehingga mudah diperbaiki, dimengerti dan dimodifikasi.

I. Representasi Seluruh Moda Operasi

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain mampu mengakomodasi semua hubungan antara masukan dan luaran untuk tiap moda operasi.

J. Antarmuka Manusia-Mesin dan Antisipasi Keterbatasan Manusia

Antarmuka manusia-mesin Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain menyediakan informasi yang memadai dan

jdih.baneten.go.id

terstruktur, dan juga menyediakan waktu yang memadai bagi operator untuk merespons. Seluruh masukan dari operator divalidasi untuk mencegah kesalahan operator.

K. Pembuktian Dependabilitas

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki Dependabilitas yang dapat dibuktikan.

L. Penyelesaian Tindakan Protektif

Sistem Keselamatan Berbasis Komputer didesain untuk memproses hingga selesai urutan tindakan protektif dari fitur pengeksekusi yang diinisiasi secara otomatis atau manual. Proses penyelesaian urutan tindakan protektif dilakukan tanpa dapat diinterupsi.

Sistem Keselamatan Berbasis Komputer didesain memerlukan tindakan operator untuk mengembalikan ke kondisi normal.

M. Integritas Sistem

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki integritas sehingga mampu melaksanakan fungsi keselamatan untuk mengantisipasi apabila terjadi kondisi pemutusan sistem, kehilangan catu daya, dan kondisi lingkungan yang buruk.

N. Kemudahan Pengujian dan Kalibrasi

Sistem Keselamatan Berbasis Komputer didesain mudah diuji dan dikalibrasi sesuai dengan persyaratan desain.

KEPALA BADAN PENGAWAS TENAGA NUKLIR,

ttd.

AS NATIO LASMAN

jdih.bapeten.go.id

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA

LAMPIRAN II
PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR
NOMOR 6 TAHUN 2012
TENTANG
DESAIN SISTEM YANG PENTING UNTUK KESELAMATAN BERBASIS KOMPUTER PADA REAKTOR DAYA

PERSYARATAN TEKNIS DESAIN

Persyaratan teknis desain Sistem yang Penting untuk Keselamatan Berbasis Komputer terdiri dari:

A. Persyaratan Teknis Desain untuk Perangkat Keras; dan
B. Persyaratan Teknis Desain untuk Perangkat Lunak.

A. Persyaratan Teknis Desain untuk Perangkat Keras

Persyaratan teknis desain untuk perangkat keras Sistem yang Penting untuk Keselamatan berbasis Komputer meliputi:

1. kriteria Kegagalan Tunggal;
2. mutu perangkat keras;
3. kualifikasi peralatan;
4. Kemandirian;
5. tampilan informasi; dan
6. inisiasi sistem proteksi.

A.1. Kriteria Kegagalan Tunggal

Perangkat keras Sistem Keselamatan Berbasis Komputer didesain memenuhi kriteria Kegagalan Tunggal. Kegagalan Tunggal dalam Sistem Keselamatan Berbasis Komputer tidak boleh mencegah tindakan proteksi pada saat diperlukan.

A.2. Mutu Perangkat Keras

Perangkat keras Sistem Keselamatan Berbasis Komputer didesain memiliki mutu komponen dan modul sesuai dengan kelas keselamatan dan mutu, dan memiliki laju kegagalan yang rendah.

A.3. Kualifikasi ...
jdih.bapeten.go.id

A.3. Kualifikasi Peralatan

Perangkat keras Sistem Keselamatan Berbasis Komputer dikualifikasi melalui metode:

a. pengujian jenis peralatan (*type test*);
b. pengalaman operasi sebelumnya; dan/atau
c. analisis.

Perangkat keras Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki ketahanan terhadap gangguan:

a. lingkungan, seperti temperatur, kelembaban, dan radiasi;
b. interferensi elektromagnetik;
c. petir; dan
d. catu daya.

A.4. Kemandirian

Perangkat keras Sistem Keselamatan Berbasis Komputer didesain:

a. mandiri dalam hal catu daya dan komunikasi; dan
b. terpisah secara fisik.

Perangkat keras Sistem Keselamatan Berbasis Komputer didesain mandiri:

1) antar bagian redundan dalam satu sistem keselamatan
   Bagian redundan dalam satu sistem keselamatan terpisah secara fisik untuk mempertahankan kemampuan dalam memenuhi fungsi keselamatan, selama dan setelah kejadian dasar desain;
2) antar sistem keselamatan
   Sistem keselamatan antara satu dan yang lain terpisah secara fisik karena berfungsi untuk memitigasi dampak kejadian dasar desain; dan
3) antara sistem keselamatan dan sistem lain
   Sistem keselamatan didesain tetap mempertahankan kemampuan dalam memenuhi fungsi keselamatan apabila terjadi kegagalan signifikan pada sistem lain.

A.5. Tampilan

jdih.bpk.go.id

A.5. Tampilan Informasi

Perangkat keras Sistem Keselamatan Berbasis Komputer didesain memiliki instrumentasi tampilan:

a. yang menyediakan tindakan pengendalian secara manual apabila tidak terdapat pengendali otomatis; dan
b. yang secara kontinu memberi indikasi status pemintasan (*bypass*) Sistem Keselamatan atau status secara sengaja Sistem Keselamatan tidak dioperasikan.

Perangkat keras Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki instrumentasi tampilan:

a. yang menyediakan informasi mengenai status Sistem Keselamatan secara lengkap, cepat, akurat, dan tidak membingungkan operator. Informasi mengenai status Sistem Keselamatan mencakup indikasi dan identifikasi tindakan proteksi pada fitur deteksi, perintah dan eksekusi; dan
b. dengan karakteristik tampilan informasi (misalnya tata letak, rentang, jenis, dan resolusi) yang memenuhi ketentuan ergonomi, sehingga dapat membantu operator dalam mengawasi status sistem dan status operasi instalasi.

A.6. Inisiasi Sistem Proteksi

Perangkat keras Sistem Keselamatan Berbasis Komputer didesain untuk memiliki inisiasi tindakan protektif secara otomatis dan manual.

B. Persyaratan Teknis Desain untuk Perangkat Lunak

Persyaratan teknis desain untuk perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer meliputi:

1. fungsi yang akan dikerjakan;
2. keselamatan;
3. ketersediaan dan keandalan;
4. antarmuka;
5. batasan desain;
6. model;

jdih.kemenperin.go.id

7. kinerja pewaktuan (*timing performance*);
8. akurasi komputasi;
9. keamanan;
10. struktur yang mudah dipahami dan diubah;
11. mampu telusur;
12. mampu prediksi;
13. konsistensi dan kelengkapan; dan
14. mampu Verifikasi.

Persyaratan teknis desain untuk perangkat lunak memperhatikan persyaratan keselamatan dan potensi kegagalan dari semua moda operasi.

B.1. Fungsi yang akan Dikerjakan

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki perangkat lunak yang mampu melaksanakan fungsi yang akan dikerjakan.

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer menerjemahkan fungsi yang akan dikerjakan menjadi kode program. Kode program merupakan transformasi dari masukan menjadi luaran digital yang ditentukan, berupa:

a. ekspresi logika;
b. fungsi atau hubungan matematika; dan
c. algoritma.

Penamaan dan pengkodean masukan, luaran dan variabel internal pada Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain mampu telusur dan dapat dipahami secara menyeluruh.

B.2. Keselamatan

Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memenuhi persyaratan keselamatan yang mencakup penetapan:

jdih.kemenkeu.go.id

a. fungsi yang penting untuk keselamatan sistem;
b. setiap luaran yang terkait dengan keadaan selamat, pada saat gagal dapat terdeteksi tetapi tidak dapat teratasi; dan
c. faktor keterkaitan antara masukan dan luaran perangkat lunak serta luaran terkait keselamatan dalam desain sistem komputer.

B.3. Ketersediaan dan Keandalan

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki ketersediaan dan keandalan.

B.4. Antarmuka

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki ketentuan mengenai antarmuka perangkat lunak dengan:
a. operator;
b. instrumen (sensor dan aktuator);
c. perangkat keras komputer;
d. perangkat lunak lain pada perangkat keras yang sama; dan
e. sistem lain.

B.5. Batasan Desain

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki batasan desain yang:
a. diperoleh dari penetapan pilihan;
b. ditetapkan dalam ketentuan perangkat lunak;
c. dijustifikasi; dan
d. mampu telusur.

B.6. Model

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain menggunakan ketentuan perangkat lunak yang didasarkan pada model sistem yang akan diimplementasikan.

jdih.bapeten.go.id

Model dan aplikasi perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer dideskripsikan dengan jelas dan didokumentasikan dengan baik.

B.7. Kinerja Pewaktuan (*Timing Performance*)

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki kinerja pewaktuan untuk melakukan transformasi masukan-luaran, seperti:

a. waktu minimum dan maksimum antar:
   1) masukan dan luaran; dan
   2) luaran yang berurutan.
b. karakteristik waktu yang diharapkan; dan
c. laju cuplik masukan yang dibutuhkan perangkat lunak.

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain mampu mendeteksi dan memulihkan kesalahan atau kegagalan dalam waktu yang ditentukan.

B.8. Akurasi Komputasi

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki tingkat akurasi komputasi tertentu. Batas toleransi akurasi komputasi mencakup ketelitian informasi numerik yang akan diproses sesuai dengan dokumen ketentuan perangkat lunak (*software requirements documents*).

B.9. Keamanan

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki ketentuan keamanan, seperti pemeriksaan validitas masukan, data yang tersimpan, dan perangkat lunak itu sendiri.

Informasi yang dapat dimanipulasi oleh perangkat lunak, seperti titik pengesetan (*set point*) terkait keselamatan, hanya dapat diakses secara terbatas.

jdih.bapeten.go.id

B.10. Struktur yang Mudah Dipahami dan Diubah

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain memiliki struktur hirarki yang menyediakan level abstraksi untuk memudahkan dilakukannya tinjau ulang.

Contoh level abstraksi pada sistem komputer, meliputi: BIOS, sistem operasi, dan program.

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain menggunakan prinsip penyembunyian informasi untuk memudahkan:

a. pelaksanaan tinjau ulang sebagian (*piecewise review*) dan verifikasi sebagian; dan
b. pengubahan struktur.

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer dapat didesain:

a. menggunakan teknik grafis dan bahasa formal untuk memudahkan pemahaman; dan
b. setiap modul memiliki antarmuka yang sederhana, dan bila terdapat perubahan, maka hanya terbatas pada sejumlah kecil modul saja yang berubah.

B.11. Mampu Telusur

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain mampu telusur sampai pada unsur-unsur desain seperti modul, prosedur, subrutin atau *file* yang mempunyai identitas unik.

B.12. Mampu Prediksi

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain:

a. memiliki arsitektur dengan karakteristik deterministik yang mampu menunjukkan prediksi respons terhadap masukan dan waktu respons.

b. menggunakan ...

jdih.bapeten.go.id

b. menggunakan protokol komunikasi deterministik dan tidak bergantung pada sistem eksternal.

B.13. Konsistensi dan Kelengkapan

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain:

a. tidak mengandung kontradiksi;
b. tidak membingungkan; dan
c. memiliki deskripsi lengkap tentang antarmuka setiap modul.

Kedua sisi antarmuka setiap modul didesain:

a. saling sesuai; dan
b. menggunakan nama dan urutan variabel yang konsisten.

B.14. Mampu Verifikasi

Perangkat lunak Sistem yang Penting untuk Keselamatan Berbasis Komputer didesain dapat diverifikasi penerapannya sesuai dengan desain rinci.

KEPALA BADAN PENGAWAS TENAGA NUKLIR,

ttd.

AS NATIO LASMAN

jdih.bapeten.go.id

KEPALA BADAN PENGAWAS TENAGA NUKLIR

REPUBLIK INDONESIA

LAMPIRAN III

PERATURAN KEPALA BADAN PENGAWAS TENAGA NUKLIR

NOMOR 6 TAHUN 2012

TENTANG

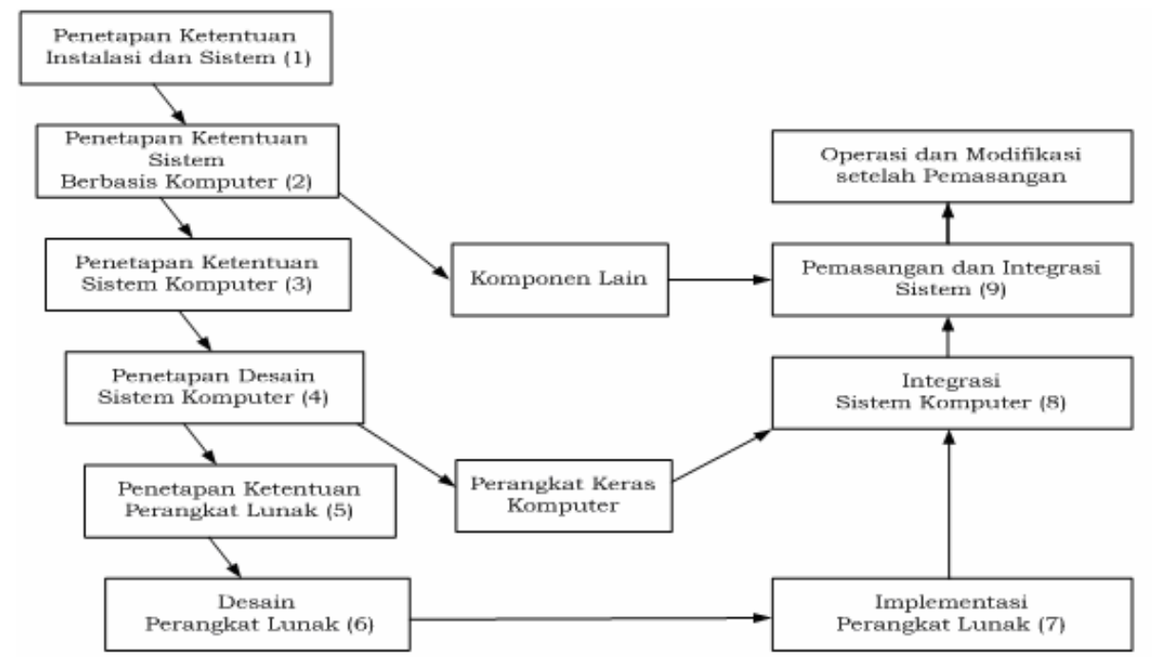
DESAIN SISTEM YANG PENTING UNTUK KESELAMATAN BERBASIS KOMPUTER PADA REAKTOR DAYA

TAHAPAN PENGEMBANGAN DESAIN, DAN VERIFIKASI DAN VALIDASI SISTEM YANG PENTING UNTUK KESELAMATAN BERBASIS KOMPUTER

A. Tahapan Pengembangan Desain

Pengembangan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer dilakukan secara bertahap, berurutan, dan melalui proses iterasi untuk mendapatkan desain yang lebih sederhana dan tersempurnakan.

Setiap tahap pengembangan desain menggunakan informasi yang dikembangkan di tahap sebelumnya dan menyediakan informasi masukan untuk tahap berikutnya. Proses tahapan pengembangan desain ditunjukkan pada Gambar 1.



: menunjukkan tahap kegiatan pengembangan yang dilakukan

→ : menunjukkan urutan dan aliran informasi utama

Gambar 1. Tahapan Pengembangan Desain

Tahapan ...

jdih.bapeten.go.id

Tahapan pengembangan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer meliputi tahap:

1. Penetapan Ketentuan Instalasi dan Sistem (*Plant and System Requirements*)

   Ketentuan instalasi dan sistem ditetapkan dengan menyertakan ahli terkait di bidang keselamatan dan perangkat lunak.

2. Penetapan Ketentuan Sistem Berbasis Komputer (*Computer Based System Requirements*)

   Ketentuan sistem berbasis komputer ditetapkan berdasarkan hasil dari tahapan penetapan ketentuan instalasi dan sistem. Ketentuan ini bertujuan untuk menghindari kesalahan spesifikasi terhadap persyaratan keselamatan. Pada tahap ini dilakukan pembagian sistem menjadi sistem komputer dan komponen lain seperti: peralatan listrik, elektronik analog pengukur variabel reaktor dan aktuator kendali.

3. Penetapan Ketentuan Sistem Komputer (*Computer System Requirements*)

   Penetapan ketentuan sistem komputer dilakukan berdasarkan hasil pada tahap sebelumnya. Ketentuan sistem komputer dibagi menjadi ketentuan perangkat lunak dan perangkat keras. Ketentuan sistem komputer memenuhi kriteria kelas keselamatan tertinggi dari fungsi yang menggunakannya. Ketentuan sistem komputer memuat antarmuka sistem komputer dengan operator, petugas perawatan dan sistem eksternal.

4. Penetapan Desain Sistem Komputer

   Pada tahap ini dilakukan penetapan desain perangkat lunak dan perangkat keras. Desain sistem komputer merupakan pemenuhan ketentuan sistem yang harus dipenuhi sistem komputer dengan menggunakan kombinasi dari:

   a. perangkat lunak yang sudah ada atau sudah dikembangkan atau *firmware*;
   b. *Application Specific Integrated Circuits* (*ASIC*); dan
   c. perangkat lunak yang dikembangkan dengan cara konfigurasi perangkat lunak yang telah ada.

5. Penetapan ...

jdih.bapeten.go.id

5. Penetapan Ketentuan Perangkat Lunak (*Software Requirements*)

   Pada tahap ini dilakukan penetapan ketentuan perangkat lunak. Ketentuan perangkat lunak merupakan bagian dari ketentuan sistem komputer yang akan diimplementasikan sebagai program komputer. Ketentuan perangkat lunak sesuai dengan ketentuan dari desain sistem komputer yang dipilih.

6. Desain Perangkat Lunak

   Pada tahap ini dilakukan pembagian perangkat lunak menjadi sekumpulan modul yang saling berinteraksi dan pendeskripsian modul tersebut. Desain perangkat lunak memuat arsitektur perangkat lunak dan desain rinci dari arsitektur tersebut.

7. Implementasi Perangkat Lunak

   Pada tahap ini perangkat lunak yang telah didesain dipersiapkan untuk dioperasikan pada perangkat keras komputer. Data yang diperlukan pada tahap ini terdiri dari spesifikasi untuk desain internal dan antarmuka modul perangkat lunak. Hasil yang diperoleh pada tahap ini berupa dokumen yang memuat program sumber, program yang dapat dieksekusi, dan hasil pengujian program.

8. Integrasi Sistem Komputer

   Pada tahap ini perangkat lunak diintegrasikan dengan perangkat keras komputer untuk menghasilkan sistem komputer.

   Tahap ini terdiri dari:

   a. pemuatan perangkat lunak ke dalam perangkat keras;
   b. pengujian ketentuan antarmuka perangkat lunak-perangkat keras; dan
   c. pengujian pengoperasian perangkat lunak pada sistem komputer.

9. Pemasangan dan Integrasi Sistem

   Pada tahap ini dilakukan pemasangan sistem komputer dengan komponen lain sehingga menjadi sistem terintegrasi.

Tahapan ...

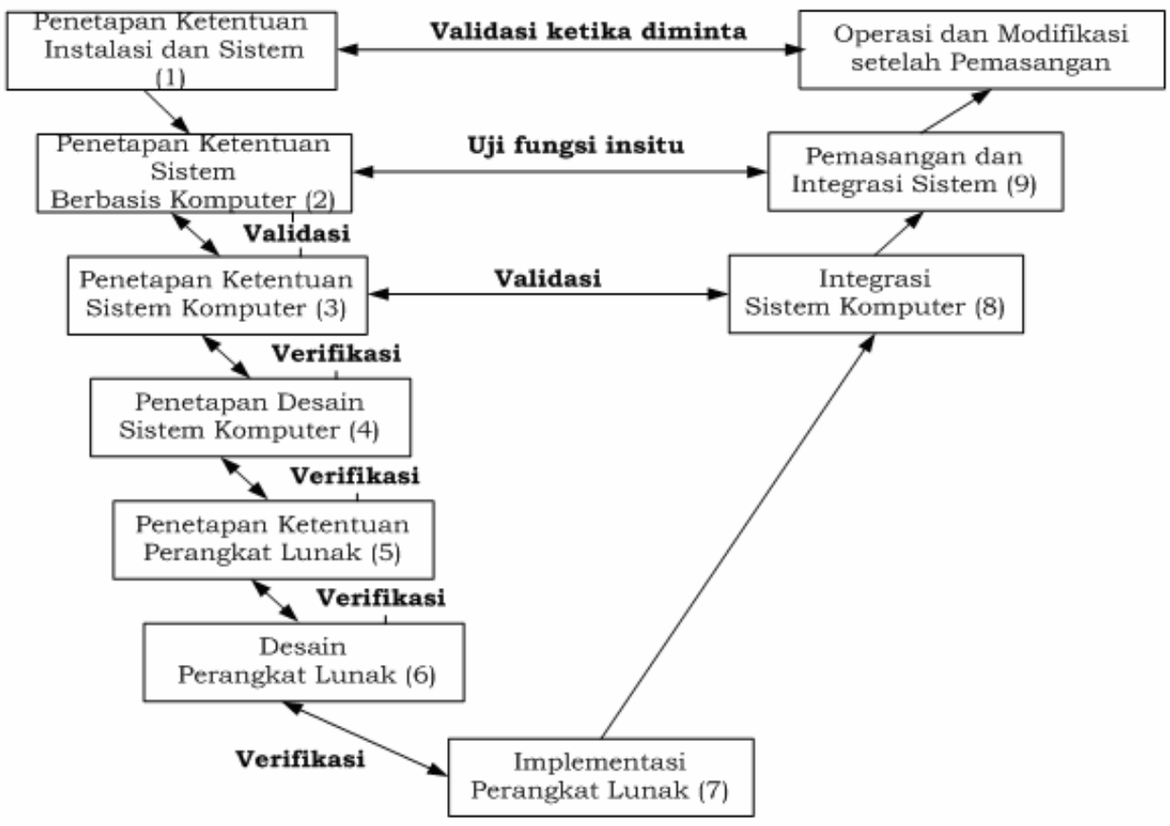
jdih.bapeten.go.id

Tahapan operasi dan modifikasi setelah pemasangan tidak termasuk dalam ruang lingkup Peraturan Kepala BAPETEN ini.

B. Verifikasi dan Validasi

Verifikasi dan Validasi pada tahapan pengembangan desain dilakukan melalui urutan tahapan yang telah ditetapkan dan bertujuan agar desain yang dihasilkan memenuhi ketentuan instalasi dan sistem.

Verifikasi dan Validasi pada tahapan pengembangan desain ditunjukan pada Gambar 2.



Keterangan:

: menunjukkan tahap kegiatan pengembangan yang dilakukan

→ : menunjukkan urutan dan aliran informasi utama

Gambar 2. Verifikasi dan Validasi

jdih.bapeten.go.id

B.1. Verifikasi

Verifikasi dilakukan pada (sebagaimana tertera pada Gambar 2):

a. tahap 4 terhadap tahap 3;
b. tahap 5 terhadap tahap 4;
c. tahap 6 terhadap tahap 5; dan
d. tahap 7 terhadap tahap 6.

Verifikasi dilakukan sesuai rencana Verifikasi. Rencana Verifikasi paling sedikit memuat uraian mengenai:

a. organisasi dan tanggung jawab;
b. metode dan teknik Verifikasi dan analisis yang akan digunakan;
c. kriteria penerimaan;
d. justifikasi bahwa teknik dan analisis Verifikasi yang digunakan telah memadai; dan
e. jenis rekaman, laporan, dan dokumen lain yang akan dibuat.

Verifikasi desain Sistem yang Penting untuk Keselamatan Berbasis Komputer dilakukan oleh tim independen. Anggota tim independen dapat berasal dari dalam atau luar organisasi PI yang tidak terlibat dalam kegiatan desain.

Verifikasi desain Sistem yang Penting untuk Keselamatan Berbasis Komputer terdiri dari:

a. analisis statik;
b. pengujian;
c. analisis potensi bahaya;
d. sarana pengkaji;
e. rekayasa balik (*reverse engineering*); dan
f. evaluasi riwayat operasi.

B.1.a. Analisis Statik

Analisis statik, antara lain:

1) Verifikasi kesesuaian terhadap batasan desain, pengkodean, dan standar;

2) analisis ...

jdih.bapeten.go.id

2) analisis alur kendali;
3) analisis penggunaan data dan alur informasi;
4) eksekusi simbolik; dan
5) Verifikasi kode program secara formal dengan menggunakan model matematika.

Apabila perangkat lunak menggunakan Verifikasi kode program secara formal, Verifikasi kode program secara formal dilakukan oleh ahli dan analis yang terkualifikasi. Analisis statik dilakukan terhadap versi akhir dari perangkat lunak.

B.1.b. Pengujian

Pengujian pada tahap Verifikasi dilakukan melalui analisis perangkat lunak yang meliputi eksekusi kode pada prosesor target atau pada simulator.

Pengujian dilakukan untuk memastikan kesesuaian pada:

1) perangkat lunak;
2) perangkat translasi (*translation tools*);
3) elemen perangkat keras; dan
4) antarmuka.

B.1.b.1). Lingkup dan Strategi Pengujian

Lingkup pengujian terdiri dari pengujian:

a) fungsional yang dapat menggunakan matriks untuk penelusuran (*traceability matrix*);
b) non fungsional, yang meliputi antara lain presisi numerik dan kinerja;
c) antarmuka:
   (1) modul dan modul;
   (2) program modul dan program modul;
   (3) perangkat lunak dan perangkat keras; dan
   (4) bagian internal dan eksternal pada batas sistem.

jdih.kemenkeu.go.id

d) kondisi pengecualian, yang meliputi antara lain kondisi dengan pembagi nol dan kondisi di luar rentang;
e) semua rentang variabel masukan; dan
f) semua moda operasi sistem.

Strategi pengujian dilakukan secara bertahap meliputi:
a) pengujian awal dari program modul terkecil;
b) integrasi program modul yang telah diuji; dan
c) pengujian program modul pada level di atasnya terhadap hasil integrasi.

B.1.b.2). Persiapan dan Pelaksanaan Pengujian

Persiapan pengujian meliputi:
a) penyusunan rencana pengujian;
b) penyediaan personil yang telah memperoleh pelatihan; dan
c) penyediaan peralatan pengujian yang terkalibrasi.

Pelaksanaan pengujian meliputi:
a) pemantauan semua luaran sistem termasuk pemeriksaan hasil-hasil yang tidak sesuai;
b) penyimpanan rekaman pengujian yang dapat diaudit oleh pihak lain;
c) pengendalian kinerja pengujian melalui evaluasi terhadap prosedur pengujian, termasuk kendali perubahannya; dan
d) pengendalian terhadap kesalahan (*error*) pada perangkat lunak atau perangkat keras melalui analisis penyebab, pemeriksaan deteksi dini proses pengembangan dan pengujian regresi, termasuk kendali perubahannya.

jdih.kejaksaan.go.id

B.1.c. Analisis Potensi Bahaya

Analisis potensi bahaya dilakukan pada berbagai tahapan pengembangan desain Sistem yang Penting untuk Keselamatan Berbasis Komputer, yang meliputi:

1) identifikasi potensi bahaya kritis;
2) penelusuran terhadap desain sistem komputer, desain dan kode perangkat lunak, untuk mengidentifikasi bagian desain dan bagian perangkat lunak yang memerlukan fitur desain khusus; dan
3) penelusuran potensi bahaya terhadap ketentuan sebelumnya.

Analisis potensi bahaya mempertimbangkan pemenuhan kriteria keselamatan instalasi pada tahap desain perangkat lunak dan potensi bahaya baru pada tahap implementasi perangkat lunak. Hasil analisis potensi bahaya dimasukkan ke dalam analisis keselamatan instalasi.

B.1.d. Sarana Pengkaji

Sarana pengkaji perangkat lunak mencakup:

1) peralatan (*tools*) pengembang perangkat lunak seperti *code generator*, *compiler*, dan *linker*; dan
2) peralatan (*tools*) Verifikasi perangkat lunak seperti alat untuk analisis statik dan pemantau pengujian.

Dependabilitas diterapkan pada semua peralatan pengembang dan Verifikasi perangkat lunak.

Peralatan pengembang perangkat lunak yang luarannya tidak memerlukan evaluasi lebih lanjut mempunyai tingkat Dependabilitas paling tinggi.

Tingkat Dependabilitas keselamatan peralatan pengembang perangkat lunak dapat diturunkan jika luarannya telah dievaluasi atau rekayasa balik diterapkan.

jdih.bapeten.go.id

Tingkat Dependabilitas keselamatan peralatan Verifikasi perangkat lunak juga dapat diturunkan jika luarannya akan diteliti lebih lanjut secara rinci.

B.1.e. Rekayasa Balik (*Reverse Engineering*)

Rekayasa balik diterapkan pada proses translasi, seperti translasi dari deskripsi desain ke kode sumber (*source code*), atau kode sumber ke kode mesin (*machine code*).

Kelayakan rekayasa balik bergantung pada proses translasi yang terdefinisi dengan baik, mampu telusur, lugas, dan mampu balik.

B.1.f. Evaluasi Riwayat Operasi

Disediakannya informasi tentang riwayat penggunaan sistem khususnya kesesuaian dengan lingkungan dari instalasi yang akan dipasang dan relevansinya dengan aplikasi yang akan digunakan.

B.2. Validasi

Validasi dilakukan pada (sebagaimana tertera pada Gambar 2):

a. tahap 3 terhadap tahap 2; dan
b. tahap 8 terhadap tahap 3.

Validasi terhadap desain Sistem yang Penting untuk Keselamatan Berbasis Komputer dilengkapi dengan analisis yang mampu telusur dan dilakukan:

a. untuk memastikan bahwa sistem dapat melakukan fungsi sesuai yang ditetapkan pada persyaratan teknis desain;
b. sesuai dengan jaminan mutu yang telah ditetapkan;
c. oleh tim independen selain pendesain yang dapat berasal dari dalam atau luar organisasi PI;
d. pada konfigurasi akhir perangkat keras Sistem yang Penting untuk Keselamatan Berbasis Komputer pada instalasi;
e. pada perangkat lunak yang identik; dan
f. pada dokumen manual operasi dan perawatan.

jdih.bapeten.go.id

Jumlah pengujian yang dilakukan dalam Validasi dijustifikasi sesuai dengan ketentuan keandalan sistem komputer yang relevan.

Pengujian interaksi antara instalasi dan sistem berbasis komputer dicakup dalam pengujian instalasi pada uji fungsi insitu.

Pengujian dilakukan dengan mempertimbangkan:

a. semua ketentuan, termasuk pengujian ketahanan (*robustness test*) dan fitur keamanan;
b. semua rentang, termasuk nilai di luar rentang untuk sinyal masukan;
c. penanganan khusus, misalnya demonstrasi karakteristik yang dapat diterima apabila terjadi kegagalan masukan;
d. teknik pengujian, misalnya partisi kelas ekuivalensi (*equivalence class partitioning*) dan analisis nilai batas (*boundary value analysis*);
e. ketentuan yang berhubungan dengan pewaktuan seperti waktu respons, pemindaian sinyal masukan, dan sinkronisasi;
f. akurasi;
g. semua antarmuka seperti antarmuka perangkat keras dan perangkat lunak di dalam integrasi sistem dan antarmuka eksternal selama Validasi;
h. pengujian beban dan tekanan, misalnya untuk mengungkapkan efek sisi curam (*cliff edge effects*)*;* dan
i. semua moda operasi dari sistem komputer, meliputi transisi antar moda dan pemulihan setelah kegagalan catu daya.

Rentang pengujian pada Validasi dilakukan pada rentang yang lebar untuk masukan pengujian statik dan dinamik, dan mencakup kondisi kecelakaan. Pengujian dinamik didasarkan pada analisis transien dari kejadian awal terpostulasi.

Pengujian dilakukan secara statistik untuk memastikan keandalan Sistem yang Penting untuk Keselamatan Berbasis Komputer. Pengujian statistik dilakukan secara acak:

a. dalam rentang masukan operasional; dan
b. untuk semua kombinasi masukan.

Pengujian ...

jdih.bapeten.go.id

Pengujian statistik untuk kombinasi masukan di luar rentang operasional menggunakan pengujian ketahanan.

Pengujian perlu dilakukan untuk memastikan akurasi titik pengesetan (*set point*) dan histeresis.

KEPALA BADAN PENGAWAS TENAGA NUKLIR,

ttd.

AS NATIO LASMAN

jdih.bapeten.go.id