BRIN
BADAN RISET
DAN INOVASI NASIONAL

JAEA
Japan Atomic
Energy Agency

Nuclear Reactor Safety:

Deterministic and Probabilistic

Analysis

D. T. Sony Tjahyani
Research Center for Nuclear Reactor Technology (PRTRN)

Follow Up Training Course on
Reactor Engineering and Safety:
High-Temperature Gas-Cooled Reactor

Yogyakarta, 18 - 22 May 2026

Biodata

Nama	:	Ir. D. T. Sony Tjahyani, M.Eng
Jabatan/Golongan	:	Peneliti Ahli Utama/IV e
Kepakaran	:	Teknologi Keselamatan Reaktor/Analisis Keselamatan Probabilistik
Institusi Tempat bekerja	:	Pusat Riset Teknologi Reaktor Nuklir - Organisasi Riset Tenaga Nuklir, BRIN

Pendidikan:

- S-2, Nuclear Engineering, Kyoto University, Japan, 1993.
- S-1, Teknik Nuklir, Universitas Gadjah Mada, 1987.

Pelatihan/Workshop:

1. Regional Workshop on Regulatory Control of Nuclear Power Plants, Daejeon–Republic of Korea, 2015.
2. Safety Forum on How to Strengthen the Safety Assessment Capability for Design and Operation of NPP, Cheju Island - Republic of Korea, 2009.
3. Scientifict Exchange on Nuclear Safety, Fugen NPP, JNC (*Japan Nuclear Cycle Development* Institute), Japan, 2002.

Karya Tulis Ilmiah:

1. Modeling and Thermal-hydraulic Analysis of Emergency Cooldown Tank (ECT) in Passive Residual Heat Removal System of the Smart Reactor Using RELAP5 Code, Progress in Nuclear Energy, 2025.
2. Event Sequence Based Fault Tree Analysis to Evaluate Minimal Combination of Event Sequences Leading to the Reactor Core Damage, Gazi University Journal of Science, 2024.
3. Fuzzy Probability and Alpha Cut Based-Fault Tree Analysis Approach to Evaluate the Reliability and Safety of Complex Engineering Systems, Quality and Reliability Engineering International, 2022.

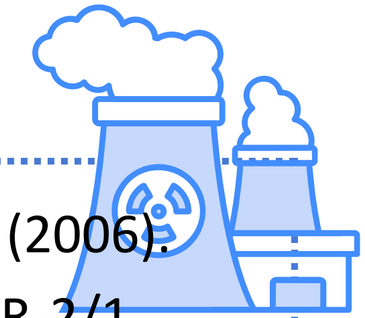
Tujuan Pelatihan

- Memberikan pemahaman dan tujuan analisis keselamatan yang dilakukan pada PLTN serta tahapan melakukan analisis keselamatan deterministik (DSA) dan probabilistik (PSA).

Outline

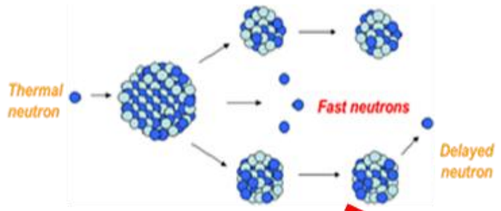
- Pendahuluan
- Analisis Keselamatan
- Deterministik
- Probabilistik
- Analisis Pohon Kejadian (*Event Tree Analysis*, ETA)
- Analisis Pohon Kegagalan (*Fault Tree Analysis*, FTA)

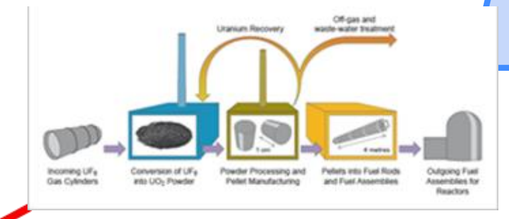
Acuan



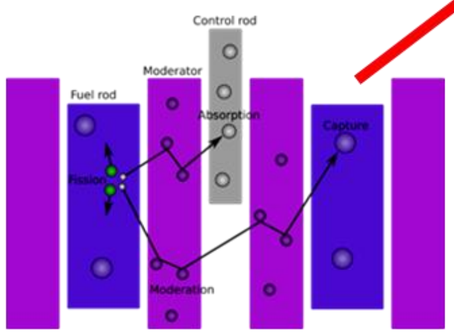
1. IAEA, “Fundamental Safety Principles”, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).
2. IAEA, "Safety of Nuclear Power Plants: Design“, Specific Safety Requirements No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
3. IAEA, “Deterministic Safety Analysis for Nuclear Power Plants”, Specific Safety Guide No. SSG-2 (Rev.1), IAEA, Vienna (2019).
4. IAEA, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants”, Specific Safety Guide No. SSG-3 (Rev.1), IAEA, Vienna (2024).
5. IAEA, “Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants”, Specific Safety Guide No. SSG-4 (Rev.1), IAEA, Vienna (2025).
6. IAEA, “Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactors”, Safety Report Series No. 54, IAEA, Vienna (2008).

Pendahuluan

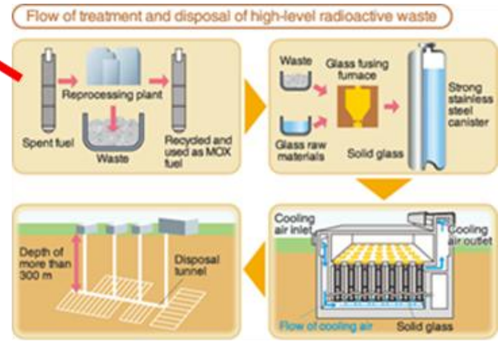




Tujuan dari keselamatan dasar (*fundamental safety)*: melindungi manusia dan lingkungan dari dampak berbahaya radiasi pengion (SF-1)



Prinsip-prinsip Dasar Keselamatan (*Safety Principles*)



Pendahuluan

GSR Part 4 (Rev.1)

SF-1

Prinsip-prinsip Dasar Keselamatan (*Safety Principles*)

- Tanggung jawab atas keselamatan;
- Peran pemerintah;
- Kepemimpinan dan manajemen untuk keselamatan;
- Justifikasi terhadap fasilitas dan kegiatan;
- Optimalisasi perlindungan;
- Pembatasan risiko terhadap individu;
- Perlindungan bagi generasi sekarang dan yang akan datang;
- Pencegahan kecelakaan;
- Kesiapsiagaan dan penanggulangan kedaruratan;
- Tindakan protektif untuk mengurangi risiko radiasi yang ada atau yang tidak teregulasi

Para 3.15 &3.16 (SF-1)

Para 3.24

Safety Assessment for Facilities and Activities

- Identifikasi risiko radiasi diimbangi dgn manfaatnya.
- Menentukan dosis dan risiko radiasi dikendalikan dlm batas yang ditetapkan.
- Perlindungan untuk lokasi yang jauh dari fasilitas/aktivitas.
- Semua upaya dilakukan utk mencegah risiko radiasi.
- Identifikasi seluruh kejadian yg diperkirakan/dipertimbangkan dlm kesiapsiagaan & kedaruratan.
- Menilai besaran risiko radiasi yang ada maupun yang belum diatur.

Pendahuluan

GSR Part 4 (Rev.1)
(Safety *Assessment for Facilities and Activities)*

Para 4.13:
Penilaian keselamatan dilakukan dengan metode kuantitatif secara deterministik dan probabilistik utk evaluasi terhadap keselamatan

Para 4.54 & 4.55:
- DSA menetapkan dan menerapkan serangkaian aturan dan persyaratan deterministik pada desain dan operasi
- PSA mengidentifikasi faktor signifikan yg berkontribusi terhadap risiko radiasi dan menilai desain terhadap pemenuhan kriteria keselamatan probabilistik

8

PSA= Probabilistic Safety Assessment

DSA= *Deterministic Safety Assessment*
DiD= *Defence in Depth*

SSR – 2/1
(*Safety of NPP: Design*)

Requirement 42:
DSA dan PSA dilakukan utk evaluasi kondisi reaktor

Para 5.75 & 5.76:
- Penetapan dan konfirmasi dasar desain utk seluruh item yang penting bagi keselamatan
- Mempertimbangkan hasil PSA utk semua mode dan kondisi operasi (termasuk *shutdown) ,* Independensi DiD serta pencegahan kondisi ekstrim akibat *cliff edge effects*

Pendahuluan

Tujuan Keselamatan Nuklir

Fungsi Keselamatan Dasar (*Fundamental Safety Function*)

- Mengendalikan reaktivitas;
- Memindahkan panas dari reaktor/penyimpan bahan bakar;
- Mengungkung bahan radioaktif, melindungi terhadap radiasi, mengendalikan lepasan bhn radioaktif yg direncanakan.

Pertahanan Berlapis (*Defence in Depth*)

- Pencegahan kondisi tidak normal &kegagalan;
- Pengendalian serta deteksi kondisi tdk normal;
- Pengendalian kecelakaan;
- Pengendalian kecelakaan parah;
- Mitigasi konsekuensi radiologis

Penghalang Ganda (*Multiple Barrier*)

- Serangkaian penghalang fisik
- Kombinasi fitur keselamatan aktif, pasif dan melekat (inherent)

DSA & PSA

Analisis Keselamatan

Analisis keselamatan desain PLTN

Dilakukan dengan menerapkan metode analisis **deterministik dan probabilistik**

untuk evaluasi dan penilaian keselamatan pada berbagai kategori kondisi

harus memberikan jaminan bahwa **pertahanan berlapis (*Defence in Depth*, DiD)** telah diterapkan dalam desain pembangkit

Analisis Keselamatan

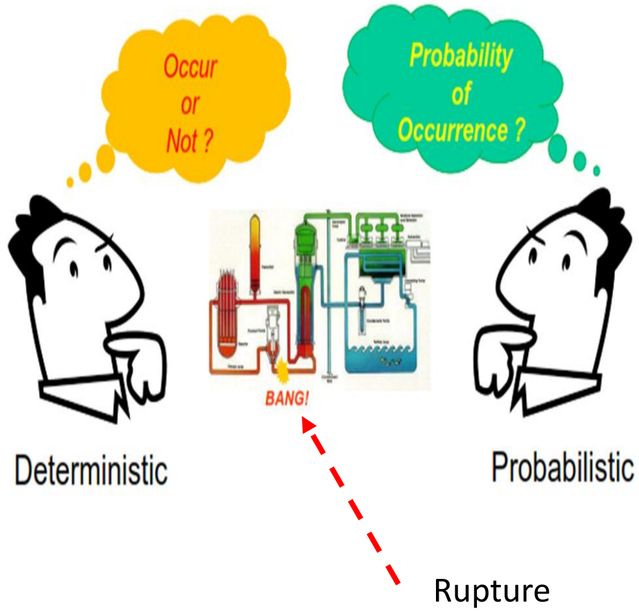
Metode Analisis Keselamataqn

Analisis Keselamatan Deterministik (DSA)

- Memprediksi respon terhadap PIE dengan asumsi-asumsi yg telah ditentukan sebelumnya
- Memeriksa pemenuhan kriteria keberterimaan

Analisis Keselamatan Probabilistik (PSA)

- Mengkombinasikan probabilitas terjadinya PIE, skenario potensial, serta konsekuensinya terhadap CDF/kerusakan bahan bakar, *source term* atau risiko keseluruhan



PIE= Postulated Initiating Event (kejadian awal terpostulasi)
CDF= Core Damage Frequency (Frekuensi kerusakan teras)
Assessment ≈ Analysis

Analisis Keselamatan

Analisis Keselamatan

- Memberikan jaminan bahwa faktor ketidakpastian telah dipertimbangkan secara memadai
- Marjin yang memadai tersedia untuk menghindari *cliff edge effects*
- Menghindari *early radioactive releases / large radioactive releases*.

asumsi analisis, metode, dan tingkat konservatisme yang digunakan dalam desain

- *Diperbarui & Diverifikasi untuk desain saat ini/ dibang*un

Pendekatan Analisis Deterministik

Penetapan dan konfirmasi dasar desain

- Item yang penting utk keselamatan (*important to safety*)

Karakterisasi PIE

- Sesuai dengan tapak (*site*) dan desain

Analisis dan Evaluasi terhadap Ess dari PIE

- Memastikan persyaratan kualitas

Perbandingan hasil analisis

- Kriteria keberterimaan, batas desain, batas dosis untuk tujuan proteksi

Menunjukkan penanganan AOO dan DBA

- Kombinasi sistem keselamatan (otomatis) dan tindakan operator

Menunjukkan penanganan DEC

- Kombinasi pengaktifan otomatis sistem keselamatan, penggunaan fitur keselamatan dalam kombinasi dgn tindakan operator

ES= Event Sequences

A00= Anticipated Operational Occurrences

DBA= Desin Basis Accident

DCE= Design Extension Condition

Deterministik

Tujuan Analisis Keselamatan Deterministik (DSA)

- Memastikan fungsi keselamatan
- SSK yang diperlukan
- Tindakan operator

→

- Mampu dan efektif
- Marjin keselamatan memadai

→

Menjaga lepasan bahan radioaktif di bawah batas yg diterima

Menunjukkan penghalang terhadap lepasan bahan radioaktif mampu mempertahankan integritasnya

SSK= Struktur, Sistem dan Komponen

Deterministik

- Analisis Keselamatan Deterministik
- Analisis Keselamatan Probabilistik
- Analisis yang berkaitan dengan fabrikasi, pengujian, inspeksi
- Evaluasi pengalaman operasi

- Sumber radiasi dan potensi konsekuensi radiologis pada berbagai kondisi operasi pada *plant* **dapat diterima**
- Kemungkinan terjadinya kondisi tertentu yang menyebabkan lepasan bahan radioaktif (*early /large release*) dapat dianggap sebagai ***"practically eliminated"***

Deterministik

Analisis Keselamatan Deterministik

- Memprediksi respons *plant* terhadap PIE (baik tunggal ataupun dikombinaasikan dengan kegagalan lainnya)
- Seperangkat aturan dan kriteria keberterimaan yang spesifik untuk setiap kondisi *plant* (*plant state*) diterapkan
- Simulasi komputasi dilakukan untuk modus operasi dan kondisi (*operating modes and plant states*)

- Analisis neutronik
- Analisis termohidrolik
- Analisis termomekanik
- Aspek struktur
- Aspek radiologis

Hasil Perhitungan:

- **Variabel fisik terpilih yang bergantung pada ruang dan waktu**
- **Fluks neutron; daya termal reaktor; tekanan, suhu, laju aliran dan kecepatan pendingin primer; beban pada penghalang fisik; konsentrasi gas yang mudah terbakar; komposisi fisis dan kimia radionuklida; degradasi teras reaktor atau tekanan pengungkung (*containment*); dan *sourceterm* lepasan ke lingkungan**

Deterministik

Kriteria Keberterimaan pada DSA

Kriteria Keselamatan

Berkaitan langsung dengan:
- Konsekuensi radiologis pada kondisi operasi/kecelaakaan
- Integritas penghalang terhadap lepasan bahan radioaktif
- Memperhatikan secara memadai keberlangsungan fungsi-fungsi keselamatan

Kriteria Desain

Batasan desain untuk masing-masing struktur, sistem dan komponen, yang merupakan bagian dari dasar desain sebagai prasyarat penting untuk memenuhi kriteria keselamatan

Kriteria Operasional

Aturan yang harus dipenuhi oleh operator selama operasi normal dan kejadian operasi terantisipasi, yang menyediakan prasyarat untuk memenuhi kriteria desan dan pada akhirnya kriteria keselamatan

Deterministik

Analisis Ketidakpastian Pada DSA

- Kombinasi penilaian ahli (*expert judgement),* Teknik statistik dan perhitungan sensitivitas
- Penggunaan data dari eksperimen berskala
- Perhitungan skenario konservatif

Deterministik

Source Term Lepasan Bahan Radioaktif ke Lingkungan:

- Komponen penting dalam analisis keselamatan deterministik:
  - Penentuan sumber lepasan bahan radioaktif;
  - Memprediksi penyebaran bahan radioaktif di lingkungan;
  - Dosis radiasi yang diterima personil *plant* maupun masyarakat;
  - Dampak radiologis terhadap lingkungan.
- *E*valuasi *source term:*
  - *I*dentifikasi sumber radiasi;
  - penentuan inventori radionuklida yang dihasilkan;
  - pemahaman mengenai mekanisme perpindahan bahan radioaktif dari sumber melalui instalasi hingga terlepas ke lingkungan.
- Dalam kondisi kecelakaan:
  - Memprediksi lepasan produk fisi dari elemen bahan bakar;
  - Perpindahannya melalui sistem primer dan *containment* atau kolam bahan bakar bekas;
  - Kimia terkait yang mempengaruhi perpindahan tersebut;
  - serta bentuk material radioaktif pada saat dilepaskan.

Deterministik

Kondisi *plant* yang dipertimbangkan dalam DSA

- Operasi normal
- Kejadian operasi terantisipasi (*Anticipated operational occurrences*, AOO)
- Kecelakaan dasar desain (*Design basis Accidents,* DBA*)*
- Kondisi perluasan desain(*Design Extension Conditions*, DEC), termasuk sekuensi kejadian tanpa degradasi bahan bakar yang signifikan dan sekuensi dengan pelelehan teras

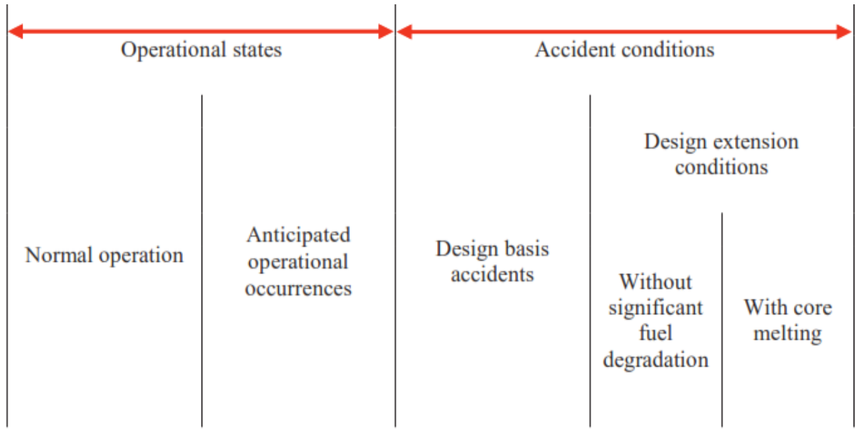


TABLE II–1. EXAMPLE OF ANTICIPATED OPERATIONAL OCCURRENCES AND DESIGN BASIS ACCIDENT CATEGORIES USED IN SOME STATES

Plant state	Alternative names used in some States	Indicative frequency range (per year)
Anticipated operational occurrences	Faults of moderate frequency: DBC-2, PC-2	$f > 10^{-2}$
Design basis accidents	Infrequent faults: DBC-3, PC-3 Limiting faults: DBC-4, PC-4	$10^{-2} > f > 10^{-4}$ $10^{-4} > f > 10^{-6}$

Operasi Normal

- Analisis keselamatan deterministik harus melakukan analisis terhadap PIE yang terjadi di semua mode operasi normal
- Analisis operasi normal yang didefinisikan sebagai operasi dalam batas dan kondisi operasional (BKO)
- Mencakup kondisi operasi:
  - *Startup* reaktor dari padam, mendekati krits dan mendekati daya penuh
  - Operasi daya: daya penuh dan daya rendah
  - Perubahan daya reaktor, termasuk mode mengikuti beban dan kembali ke daya penuh setelah periode Panjang pada daya rendah
  - Reaktor padam pada operasi daya
  - dll

Kecelakaan Dasar Desain (*Design Basis Accident*, DBA)

Kecelakaan Dasar Desain (DBA)

Suatu himpunan kecelakaan yang harus dipertimbangkan dalam desain

ditetapkan berdasarkan kejadian awal terpostulasi (PIE)

Untuk menetapkan kondisi batas agar PLTN mampu bertahan tanpa melampaui batas yang dapat diterima untuk proteksi radiasi

Kondisi Perluasan Desain (*Design Extension Condition*, DEC)

Kondisi Perluasan Desain (DEC)

- Ditetapkan berdasarkan pertimbangan rekayasa (*engineering judgement*), penilaian deterministik, dan penilaian probabilistik
- Untuk tujuan meningkatkan keselamatan PLTN melalui peningkatan kemampuan *plant* menghadapi kecelakaan yang lebih parah daripada kecelakaan dasar desain/ melibatkan kegagalan tambahan
- Tanpa menimbulkan konsekuensi radiologis yang tidak dapat diterima
- Mengidentifikasi skenario kecelakaan tambahan yang perlu dipertimbangkan dalam desain
- Merencanakan ketentuan yang praktis guna mencegah kecelakaan tersebut atau memitigasi konsekuensinya

Kejadian Awal Terpostulasi (*Postulated Initiating Event*, PIE)

Pada desain PLTN dilakukan pendekatan sistematis

Untuk mengidentifikasi serangkaian kejadian pemicu terpostulasi (*Postulated Initiating Event*, PIE)

- Semua kejadian yang mempunyai potensi konsekuensi serius dapat diprediksi
- Semua peristiwa yang dapat diprediksi dengan frekuensi kejadian yang signifikan harus dapat diantisipasi
- Dipertimbangkan dalam desain

Kejadian Awal Terpostulasi (*Postulated Initiating Event*, PIE)

Identifikasi PIE

Engineering Judgement

Kombinasi *Deterministic & Probabilistic Assessment*

Menunjukkan bahwa semua kejadian yang diperkirakan telah dipertimbangkan

Dipertimbangkan:

- Kegagalan struktur, sistem dan komponen
- Kesalahan operasi
- Bahaya internal dan eksternal
- Kondisi daya penuh (*full power*), daya rendah dan padam (*Low power and shutdown*)

Tujuan PIE

Kejadian Awal Terpostulasi (PIE)

- Menetapkan langkah-langkah pencegahan (*preventive*) dan perlindungan (*protective*) yang diperlukan
- Memastikan fungsi keselamatan yang diperlukan

Perilaku PIE

Tidak berpengaruh terhadap keselamatan

Plant selamat berdasarkan prosedur yang telah ditentukan

Perilaku PIE terhadap *Plant*

Plant selamat karena fitur keselamatan pasif/tindakan sistem

Plant selamat karena respon dari sistem keselamatan

Identifikasi PIE

- Dibagi dalam kelompok yang sesuai dengan sekuensi kejadian (*event sequence*)
  - Mempertimbangkan evolusi fisis dari PIE
- Setiap kelompok harus mencakup sekuensi kejadian:
  - Menimbulkan respon serupa terhadap fungsi keselamatan dan penghalang keselamatan, serta memerlukan sistem mitigasi yang serupa untuk membawa instalasi menuju kondisi selamat
  - Dikategorikan sesuai dengan frekuensi kejadiannya
    - Memungkinkan pemilihan kriteria penerimaan dan kondisi awal yang sama
    - Penerapan asumsi dan metodologi yang sama
- PIE yang terkait dengan kejadian operasi terantisipasi dan kecelakaan dasar desain harus mencerminkan karakteristik spesifik dari desain.

Identifikasi PIE

- Kelompok PIE:
  - Peningkatan atau penurunan pembuangan panas (*heat removal*) melalui sistem pendingin reaktor.
  - Peningkatan atau penurunan laju alir sistem pendingin reaktor.
  - Anomali pada reaktivitas dan distribusi daya di teras reaktor, atau anomali reaktivitas. pada bahan bakar baru maupun bahan bakar bekas dalam penyimpanan.
  - Peningkatan atau penurunan inventori pendingin reaktor.
  - Kebocoran pada sistem pendingin reaktor yang berpotensi menyebabkan bypass terhadap pengungkung (*containment*).
  - Kebocoran di luar *containment.*

Kejadian Operasi Terantisipasi (AOO)

- Contoh PIE menyebabkan sekuensi kejadian yang dikategorikan sebagai **kejadian operasi terantisipasi**

Kategori	PIE
Peningkatan pembuangan panas dari reaktor	Terbukanya katup pelepas uap secara tidak sengaja; malfungsi pengendalian tekanan yang menyebabkan peningkatan laju aliran uap; malfungsi sistem air umpan yang menyebabkan peningkatan laju pembuangan panas
Penurunan pembuangan panas dari reaktor	Trip pompa air umpan; penurunan laju aliran uap karena berbagai penyebab (malfungsi sistem kendali, penutupan katup utama uap, trip turbin, kehilangan beban eksternal dan gangguan jaringan eksternal lainnya, kehilangan daya, kehilangan vakum kondensor).
Peningkatan laju aliran sistem pendingin reaktor	Start pompa pendingin utama
Penurunan laju aliran sistem pendingin reaktor	Trip satu atau lebih pompa pendingin; isolasi tidak disengaja pada salah satu loop utama sistem pendingin
Anomali pada reaktivitas dan distribusi daya di teras reaktor	penarikan batang kendali (atau kelompok batang kendali) secara tidak disengaja; pengenceran boron akibat malfungsi pada sistem kendali kimia dan volume (*chemical and volume control system*) pada reaktor air bertekanan (*pressurized water reactor*); kesalahan penempatan elemen bakar
Anomali reaktivitas pada bahan bakar baru atau bahan bakar bekas dalam penyimpanan	pengenceran boron pada kolam bahan bakar bekas (LWR)

Kecelakaan Dasar Desain

- Contoh PIE menyebabkan sekuensi kejadian yang dikategorikan sebagai **kecelakaan dasar desain**

Kategori	PIE
Peningkatan pembuangan panas dari reaktor	Kebocoran/patah pipa uap (*steam line breaks*).
Penurunan pembuangan panas dari reaktor	Kehilangan sistem air umpan (*loss of feedwater*).
Penurunan laju aliran sistem pendingin reaktor	Macetnya (seizure) atau patahnya poros pompa pendingin utama; trip seluruh pompa pendingin
Anomali pada reaktivitas dan distribusi daya	Penarikan batang kendali (atau kelompok batang kendali) yang tidak terkendali; ejeksi batang kendali (reaktor air bertekanan / pressurized water reactor); kecelakaan jatuhnya batang kendali (rod drop accident) pada reaktor air didih (boiling water reactor); pengenceran boron akibat pengaktifan loop yang sebelumnya tidak aktif (reaktor air bertekanan).
Penurunan inventori pendingin reaktor	Spektrum kemungkinan kecelakaan kehilangan pendingin (*loss of coolant accidents);* terbukanya katup pelepas sistem primer secara tidak disengaja; kebocoran pendingin primer ke sistem sekunder
Penurunan atau kehilangan pendinginan bahan bakar pada kolam penyimpanan bahan bakar bekas	Patahnya pipa yang terhubung dengan air kolam.

Kategori dan PIE pada HTGR

HTGR

Category	PIE
Challenge to heat removal	Primary system breaks
Challenge to reactivity control	Loss of primary system heat sink
Challenge to confinement of radioactivity	Air ingress events
Challenge to control of chemical attack	Water ingress events
	Reactivity transients
	Depressurized loss of forced cooling (D-LOFC)
	Pressurized loss of forced cooling (P-LOFC)
	Turbin Trip
	Station blackout

Pendekatan Probabilistik

Mempertimbangkan *balance design*

- Tidak ada fitur/PIE tertentu memberikan kontribusi sangat besar/tidak pasti terhadap keseluruhan risiko serta setiap level DiD saling tidak tergantung (*independent*)

Memberikan jaminan bahwa penyimpangan kecil pada parameter plant tdak menimbulkan variasi yg besar pada plant

- Mencegah *cliff edge effects*

DiD= Defence in Depth

Membandingkan hasil analisis dengan *acceptance criteria* untuk risiko

- Jika *acceptance criteria* untuk risiko telah ditentukan oleh badan regulasi

Penerapan Analisis Keselamatan Probabilistik (PSA)

$$\text{Risiko}\left[\frac{\text{Besarnya konsekuensi}}{\text{Satuan waktu}}\right] = \text{Frekuensi}\left[\frac{\text{Kejadian}}{\text{Satuan Waktu}}\right] \times \text{Konsekuensi}\left[\frac{\text{Besarnya}}{\text{Kejadian}}\right]$$

3

Apakah yang dapat membuat terjadinya penyimpangan/kesalahan

Perlu dibuat skenario/sekuensi kecelakaan

Kemungkinan Terjadinya Skenario

Menghitung frekuensi

Pengaruhnya/Dampaknya

Menentukan konsekuensi

Sesuai Dengan Konsep Risiko

Konsep PSA

SF-1	SSR-2/1 (Rev.1) (Req. 42)	SSR-2/1 (Rev.1) (Para 5.76)
• Untuk menjamin perlindungan pekerja, masyarakat, dan lingkungan, baik saat ini maupun di masa depan, dari dampak berbahaya radiasi pengion	• Analisis keselamatan terhadap desain pembangkit listrik tenaga nuklir harus dilakukan dengan menggunakan metode analisis deterministik dan analisis probabilistik	• Desain harus mempertimbangkan secara memadai analisis keselamatan probabilistik instalasi untuk seluruh mode operasi dan seluruh kondisi instalasi. • Tidak ada PIE yang memberikan kontribusi besar terhadap risiko. • Level pertahanan berlapis (*defence in depth*) bersifat independent. • Untuk memastikan bahwa tidak ada penyimpangan kecil yang menyebabkan *cliff edge effects.* • Untuk membandingkan hasil analisis dengan kriteria penerimaan risiko.

PSA :

- memberikan wawasan keselamatan penting sebagai pelengkap terhadap wawasan yang diperoleh dari analisis deterministik.
- Mengidentifikasi sekuensi kecelakaan yang dapat timbul dari berbagai jenis kejadian pemicu.
- melakukan penentuan secara sistematis dan realistis terhadap kerusakan serta pelepasan radioaktif beserta frekuensi kejadiannya

Output PSA

SSG-3 Rev.1

Probabilistic Safety Assessment

PSA Level 1

- Analisis terhadap desain dan operasi NPP
- Identifikasi sekuensi kejadian terhadap kerusakan teras dan/atau bahan bakar
- Frekuensi kerusakan teras dan/atau bahan bakar

→ Kekuatan dan kelemahan SSK
→ Prosedur mencegah kerusakan teras dan/atau bahan bakar

PSA Level 2

- Rambatan kronologi kerusakan teras dan/atau bahan bakar serta Fenomena kerusakan parah
- Identifikasi Lepasan bahan radioaktif dari bahan bakar ke lingkungan
- Frekuensi dan karakteristik lepasan

→ **Pencegahan kecelakaan dan tindakan mitigasi**
→ **Penghalang secara fisis radionuklida ke lingkungan**

PSA Level 3

- Konsekuensi sosial dan kesehatan masyarakat

→ **Kontaminasi pada daratan dan makanan dari sekuensi kecelakaan yang menimbulkan lepasan bahan radioaktif ke lingkungan**

SSG-3 Rev.1 (*Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*)

Hasil PSA Level 1, 2 dan 3

Level 1

- Identifikasi sekuensi kerusakan teras
- Kuantifikasi frekuensi sekuensi

Sekuensi kerusakan teras dan frekuensi

atau bahan bakar

Level 2

- Evaluasi teras dan respon pengungkung
- Analisis *source term*

Jenis, jumlah dan frekuensi lepasan

Level 3

- Perkiraan transport radionuklida
- Perhitungan konsekuensi

Risiko masyarakat dan lingkungan

Risk Metrics/safety goals:

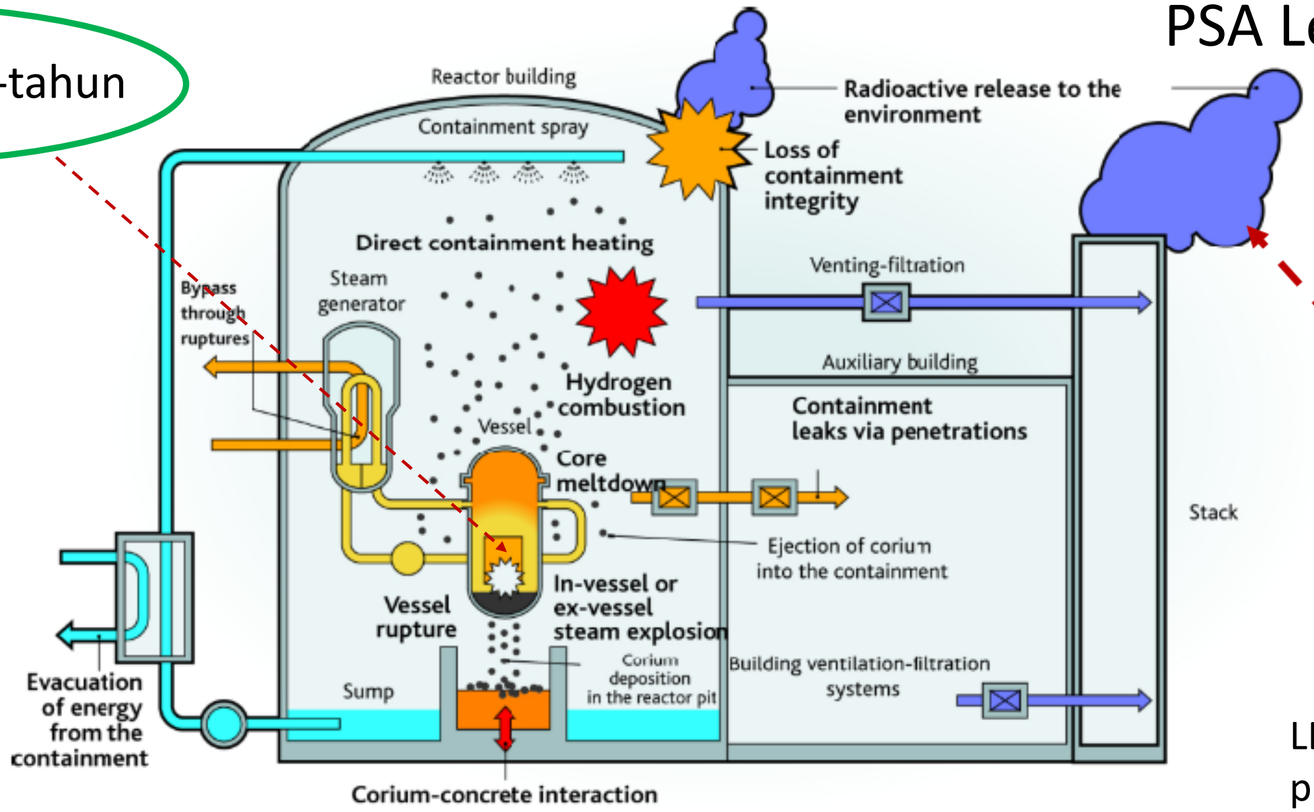
- CDF
- LERF
- Individual/Collective Risk

Hubungan PSA Level 1 dan 2

1.0E-5 per reaktor-tahun

ET= Memodelkan kemungkinan rangkaian kejadian setelah kejadian awal. Menunjukkan respon dari sistem keselamatan.

FT= Menganalisis logika kegagalan sistem/fungsi tertentu.



PSA Level 2 (WCR)

Source term :
The amount and isotopic composition of radionuclides released from facility

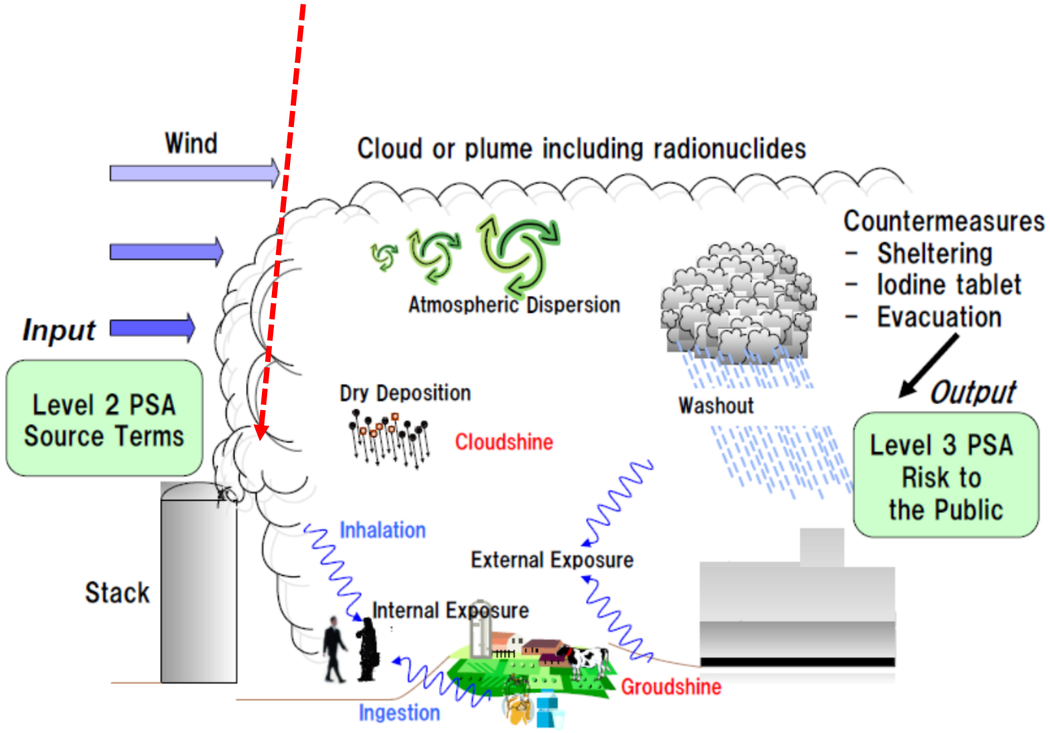
1.0E-6 per reaktor-tahun

Data= laju kegagalan, waktu perbaikan, probabilitas kesalahan manusia, dan batas ketidakpastian. Penting untuk kuantifikasi **ET** dan **FT**

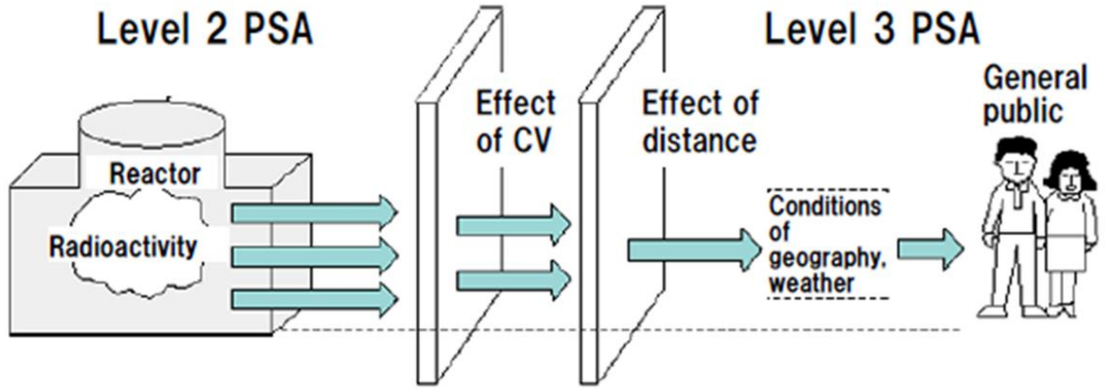
LERF (*Large Early Release Frequency*) probabilitas per tahun per reaktor terjadinya pelepasan awal dalam jumlah besar bahan radioaktif dari containment setelah kerusakan teras

Hubungan PSA Level 2 dan 3

1.0E-6 per reactor-year



PSA Level 3



Penerapan PSA

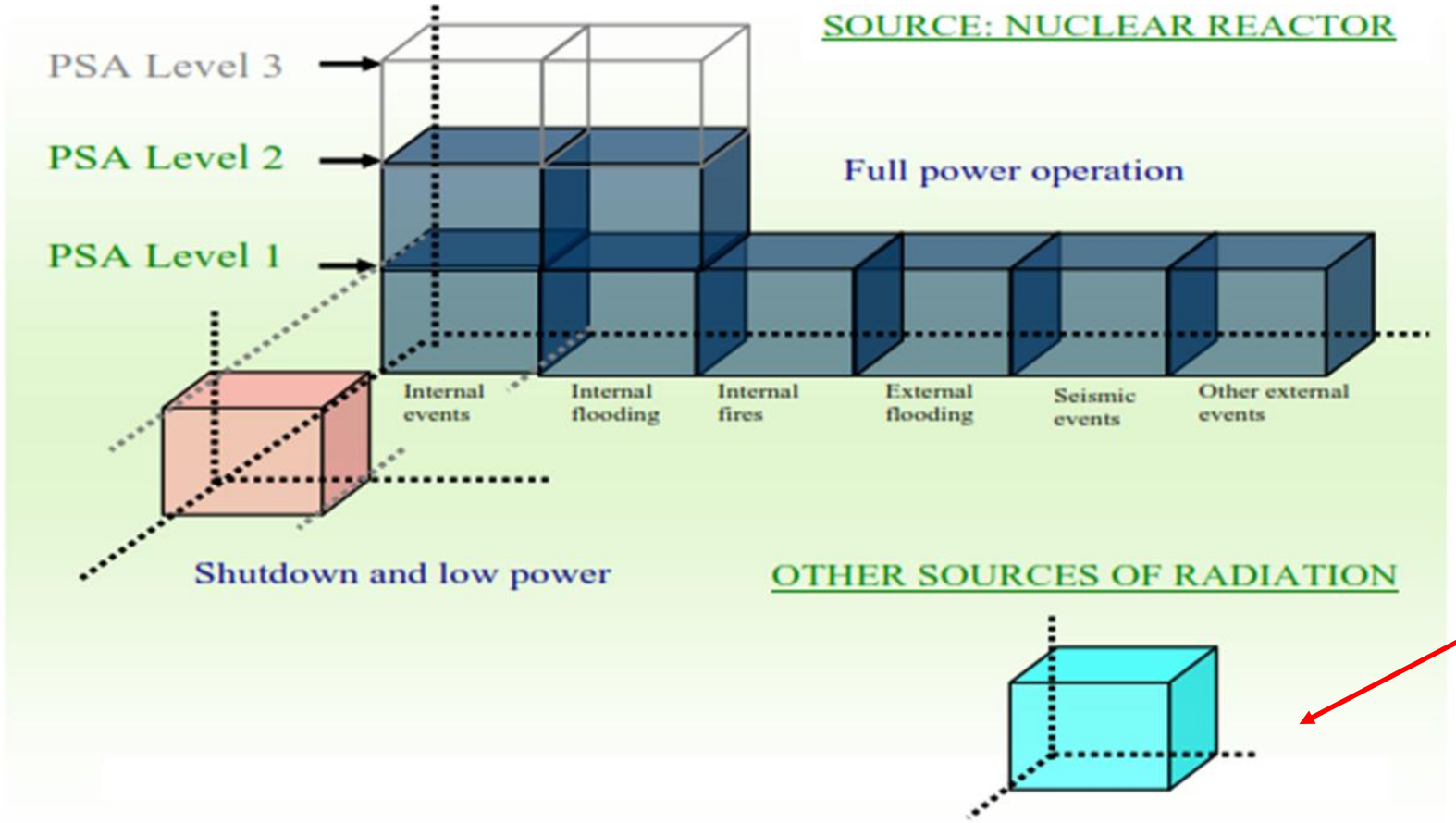
PSA

- *End States* /Konsekuensi
  - Level 1 (*Core/Fuel Damage*)
  - Level 2 (*Containment Integrity*)
  - Level 3 (*Effect on Public /Environment)*
- Daya
  - Daya Penuh (100%)
  - Daya rendah/padam (LPSD)
    - < 20 %
    - *Refueling*
- Kejadian Internal dan Bahaya
  - Kejadian Internal
    - Kegagalan internal pada sistem/komponen
  - Bahaya
    - Internal
    - Eksternal

Kejadian awal dan konfigurasi sistem berbeda pemodelannya dengan kondisi daya penuh

Penerapan PSA

Lingkup PSA



- Penyimpanan bahan bakar
- Limbah Radioaktif

Kejadian Awal Pada PSA

Kejadian Awal
(*Initiating Events*)

Kejadian Awal Internal LWR:
- LOCA
- LOFA
- LOOP/SBO
- LOFW
- SGTR
- RVR
- ATWS (*Anticipated Transient Without Scram)*
- dll

Kejadian Awal Internal HTGR:
- LOFC (Loss of Forced Circulation under Pressurized/Depressurization Condition)
- Rupture with Water Ingress
- Rupture with Air Ingress
- Reactivity Accident
- ATWS
- dll

Bahaya (Hazard)

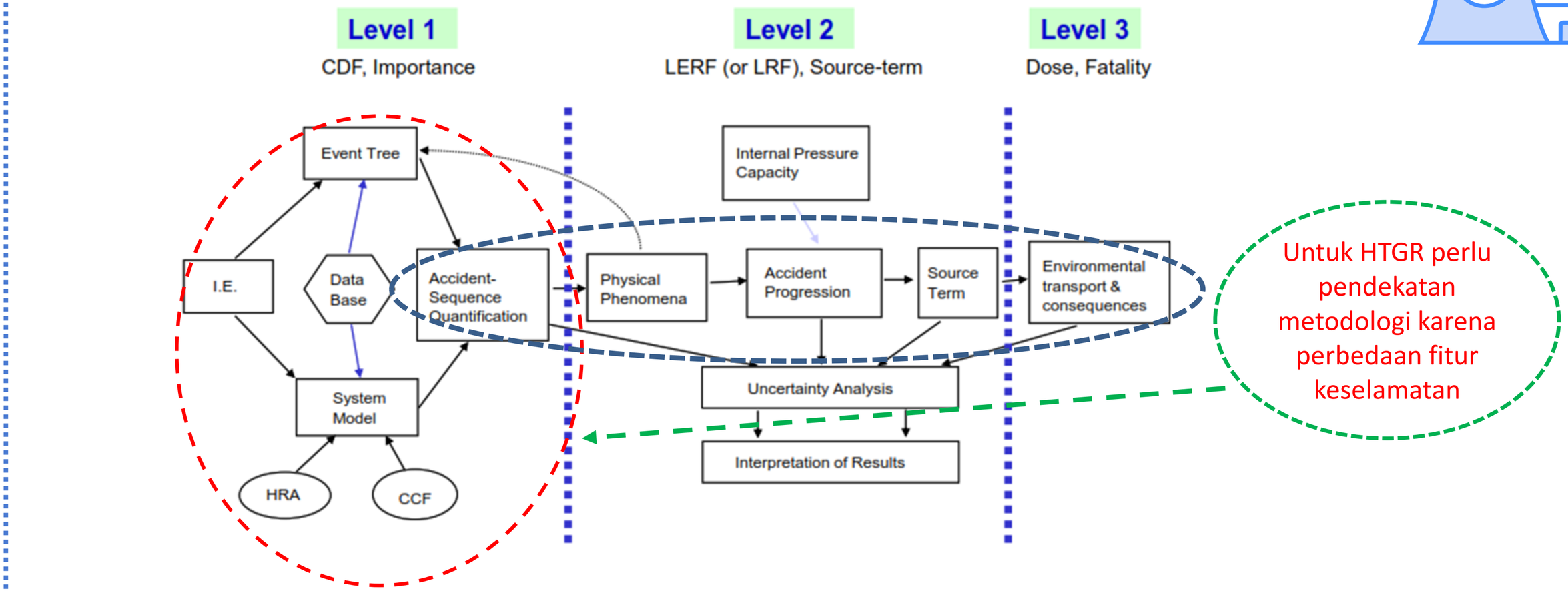
Bahaya Internal:
- Kebakaran
- Ledakan
- *Internal flooding*
- *Internal missiles,*
- *dll*

Bahaya Eksternal

Alam:
- Seismic
- Hydrological
- Meteorological
- Extraterrestrial,
- dll

Human Induced:
- *Accidental aircraft crashes*
- *Military accidents*
- *industrial accidents*
- *dll*

Tahapan Penyusunan PSA

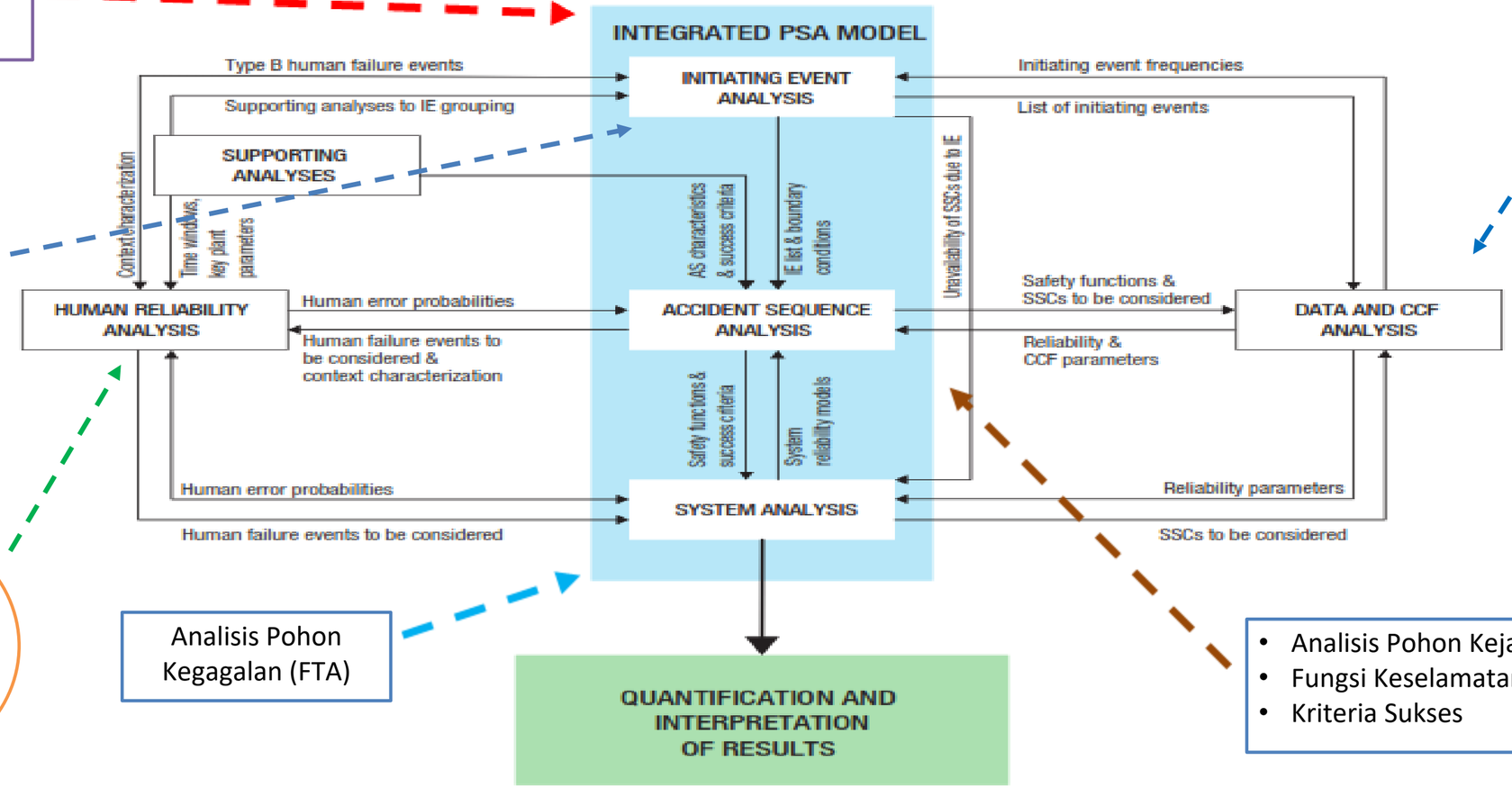


IE= Initiating Event HRA= Human Reliability Analysis CCF= Common Cause Failure

Penyusunan PSA Level 1

Kejadian Awal (IE):
- Pengelompokan
- Kuantifikasi

Kegagalan:
- **Tipe A** (Gagal melakukan tindakan)
- **Tipe B** (Melakukan tindakan tapi salah)
- **Tipe C** (Tindakan benar tetapi terlambat)



Kegagalan Berpenyebab Sama (CCF)untuk sistem dan komponen

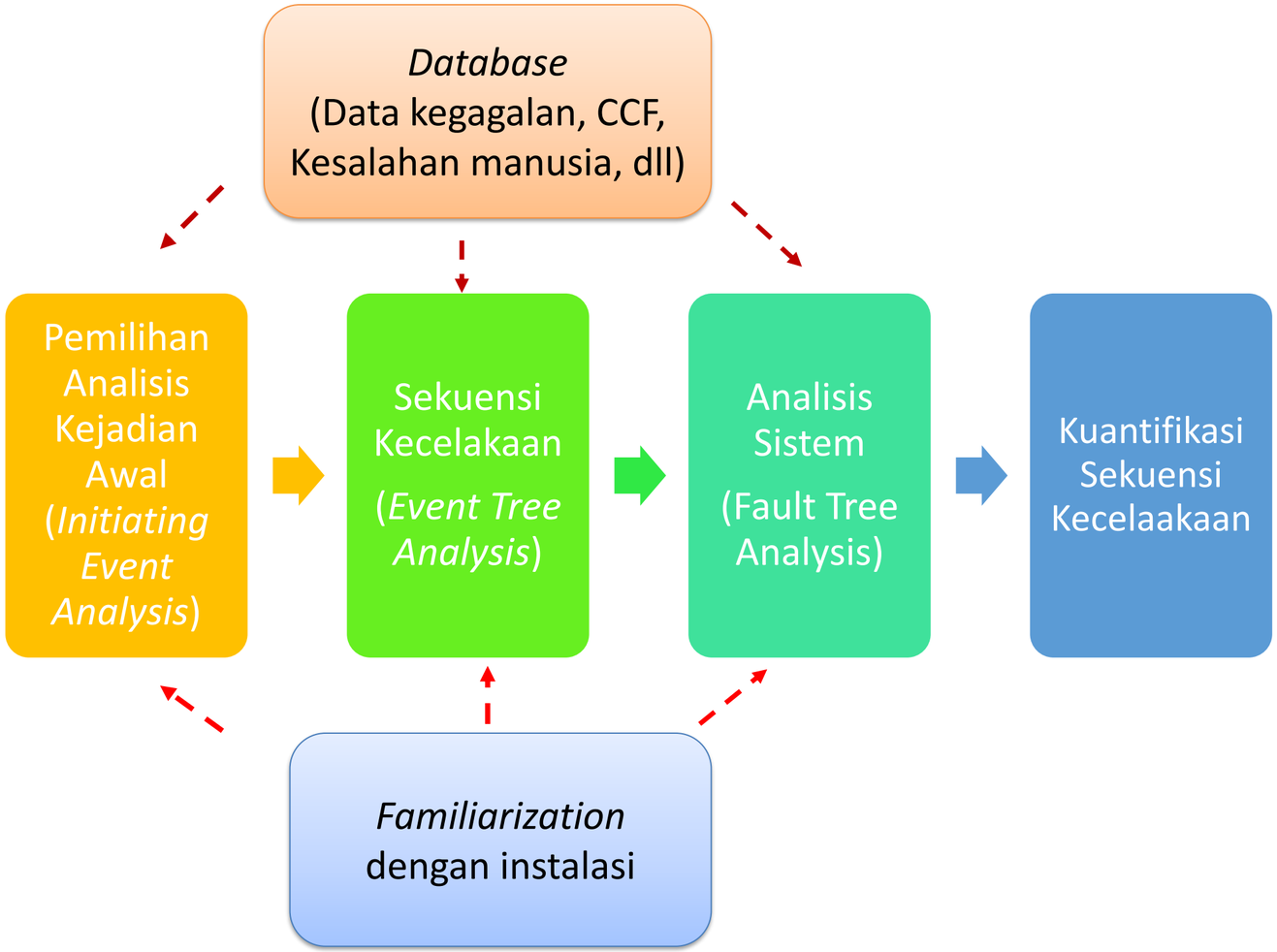
Kuantifikasi Kesalahan Manusia

Analisis Pohon Kegagalan (FTA)

- Analisis Pohon Kejadian (ETA)
- Fungsi Keselamatan
- Kriteria Sukses

Source: SSG-3 Rev.1

Penyusunan PSA level 1



Tahapan PSA

PSA Level 1

Pengenalan terhadap instalasi dan pengumpulan informasi

- LAK
- Spesifikasi teknis
- Deskripsi sistem
- Gambar sistem kondisi terbangun (*as-built*)
- Gambar diagram kelistrikan
- Gambar rangkaian kendali dan aktuasi
- Prosedur (operasi normal , darurat, perawatan, dll)

- Kriteria sukses sistem
- Pengalamanan operasi
- Catatan operator
- Diskusi dengan personil operasi
- Catatan operasi instalasi dan laporan *shutdown*
- *Database* dari instalasi

- Gambar tata letak instalasi
- Gambar lokasi dan rute perpipaan
- Gambar lokasi dan rute kabel
- Laporan inspeksi lapangan
- Persyaratan regulasi
- Dokumen fasilitas lain yang relevan

Kejadian Awal Pada PSA

Kejadian Awal (*Initiating Event*)

- Kejadian yang menimbulkan gangguan pada instalasi dan berpotensi menyebabkan kerusakan teras atau bahan bakar nuklir

Transient

- Loss of off-site power (LOOP)
- Station blackout (SBO)
- Main steam line break (MSLB)
- Steam generator tube rupture (SGTR), dll

LOCA

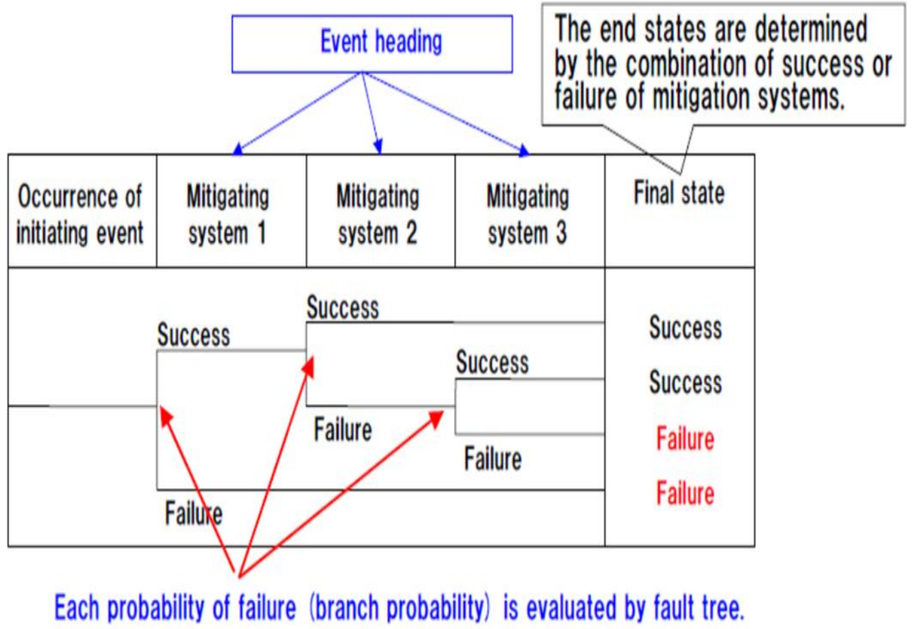
- Small break (SBLOCA), Medium break (MBLOCA), Large break LOCA (LBLOCA)
- Interfacing system LOCA

Sumber kejadian awal

- Pengalaman operasi
- Instalasi yang identik
- Metode analisis: HAZOP (*Hazard and Operability*), FMEA (*Failure Modes and Effects Analysis*) , MLD (*Master Logic Diagram*)

Analisis Pohon Kejadian (ETA)

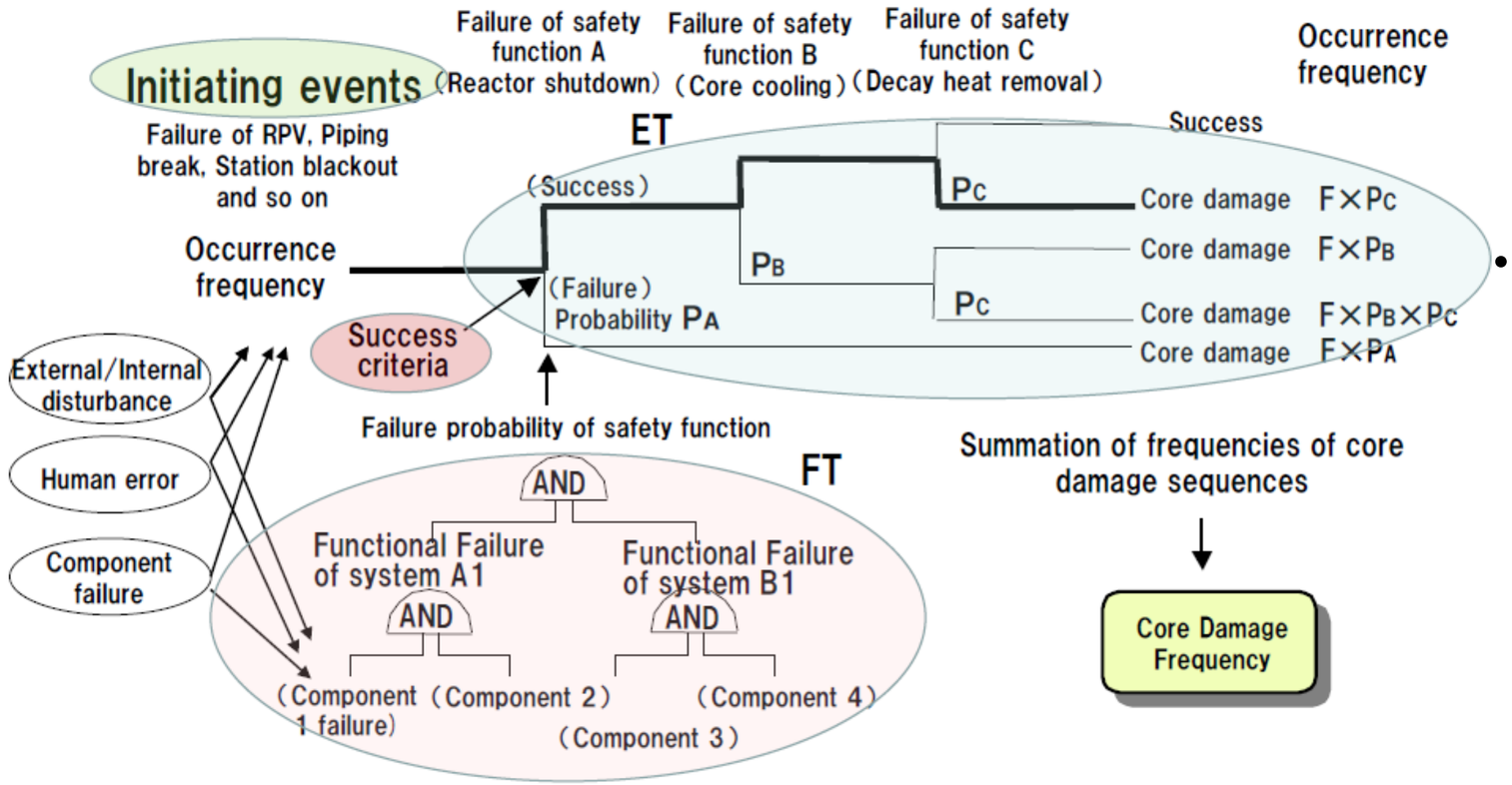
- Pohon kejadian adalah suatu metode untuk menganalisis proses dari sebuah kejadian awal (kelompok kejadian awal) hingga kondisi akhir (*end state*), dengan membagi proses tersebut ke dalam cabang-cabang (seperti pohon). Biasanya digunakan pohon dengan dua cabang.
- Cabang atas menyatakan keberhasilan, sedangkan cabang bawah menyatakan kegagalan.
- Probabilitas untuk mencapai keadaan akhir dianalisis dengan memasukkan probabilitas kejadian dari kejadian awal dan probabilitas cabang (probabilitas keberhasilan dan kegagalan) dari peristiwa atau sistem mitigasi *Event Heading*)



- Menentukan sekuens kecelakaan yang mengarah pada kerusakan teras

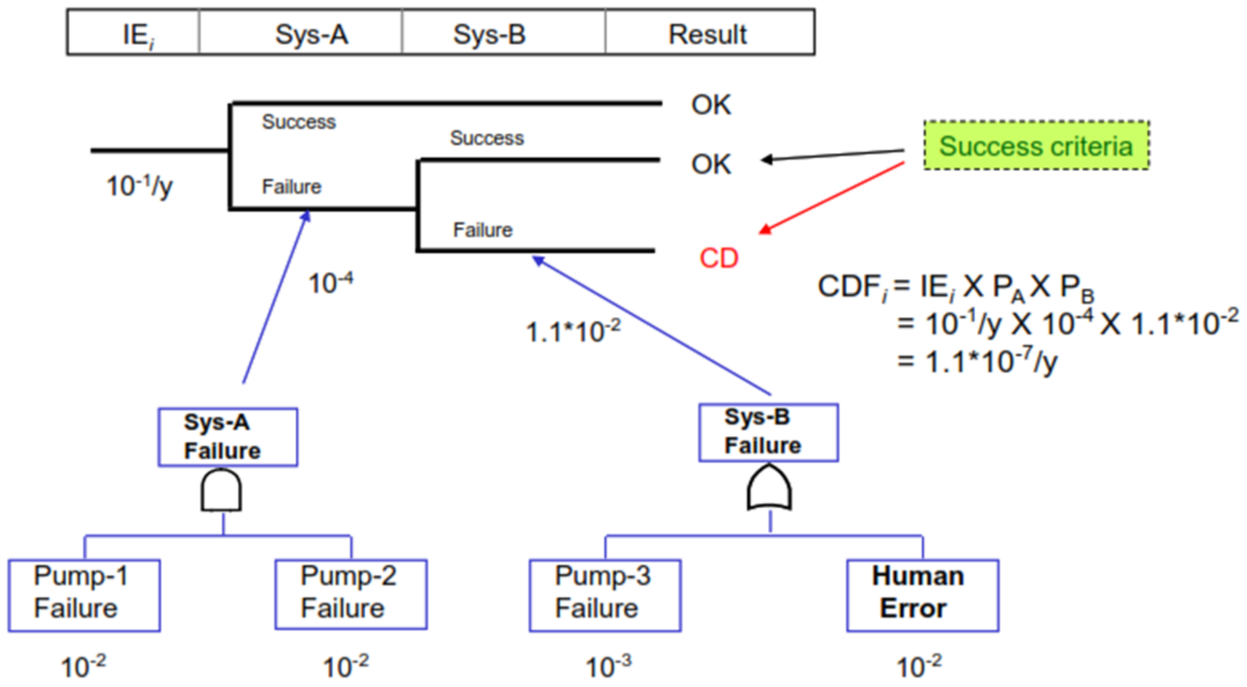
Hubungan ETA dan FTA

Perhitungan Sederhana PSA Level 1



- Kerusakan teras didefinisikan sebagai kegagalan kelongsong bahan bakar atau pellet
- Frekuensi kerusakan teras (CDF)/bahan bakar adalah probabilitas terjadinya kerusakan teras/bahan bakar pertahun operasi reaktor
- Target:
  - 1.0E-04 per reaktor-tahun utk instalasi yang sudah ada
  - 1.0E-05 per reaktor-tahun untuk reaktor yang dibangun
  - < 1.0E-05 per reaktor-tahun untuk Gen-III/III+

Analisis Pohon Kejadian (ETA)



Frekuensi kerusakan teras (CDF)/bahan bakar:

- Frekuensi kejadian yang diharapkan persatuan waktu.
- Sekuensi kecelakaan yang dapat menyebabkan kerusakan teras/bahan bakar reaktor:
  - Kriteria kerusakan teras: teras reaktor tidak terendam pendingin (**Uncovery and heatup** of reactor core)
- Dilakukan untuk semua kejadian awal
- **Kerusakan teras atau tidak:**
  - Ditentukan apakah kombinasi fungsi keselamatan terhadap setiap sekuens kecelakaan memadai atau tidak untuk memenuhi kriteria kerusakan teras di atas

Analisis Pohon Kejadian (ETA)

Kriteria Sukses:

- Ditentukan sebagai jumlah/tingkatan *performance* minimum yang dipersyaratkan dari sistem keselamatan.
- Ditetapkan waktu misi untuk sistem keselamatan berdasarkan analisis transien yang telah dilakukan
- Ditetapkan juga persyaratan untuk sistem pendukung berdasarkan kriteria keberhasilan dari sistem keselamatan (*frontline*)
- Diidentifikasi juga tindakan operator yang diperlukan untuk membawa fasilitas ke kondisi *shutdown* yang aman (*safe shutdown*)

Analisis Pohon Kejadian (ETA)

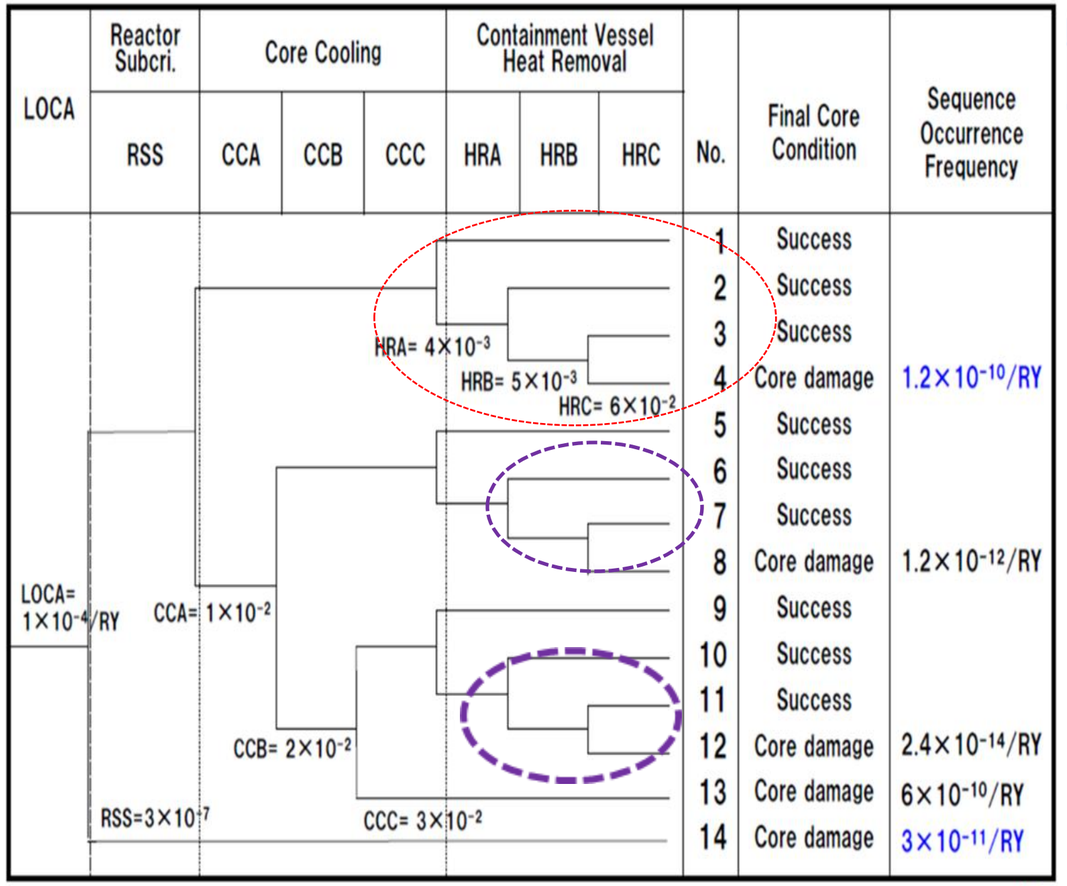
Sebagai contoh perhitungan sederhana dari pohon kejadian:

- Tabel 1 menunjukkan kriteria sukses dari LOCA (Loss of Coolant Accident) suatu PLTN.
- Diasumsikan frekuensi utk LOCA sebesar $1x10^{-04}$/Reaktor Tahun

Table 1. Success Criteria of LOCA for NPP

Mitigating function	Minimum required system	System unavailability
Reactor sub-criticality	RSS	RSS=3×10^{-7}
Core cooling	CCA or CCB or CCC	CCA= 1×10^{-2} CCB= 2×10^{-2} CCC= 3×10^{-2}
Containment Vessel Heat Removal	HRA or HRB or HRC	HRA= 4×10^{-3} HRB= 5×10^{-3} HRC= 6×10^{-2}

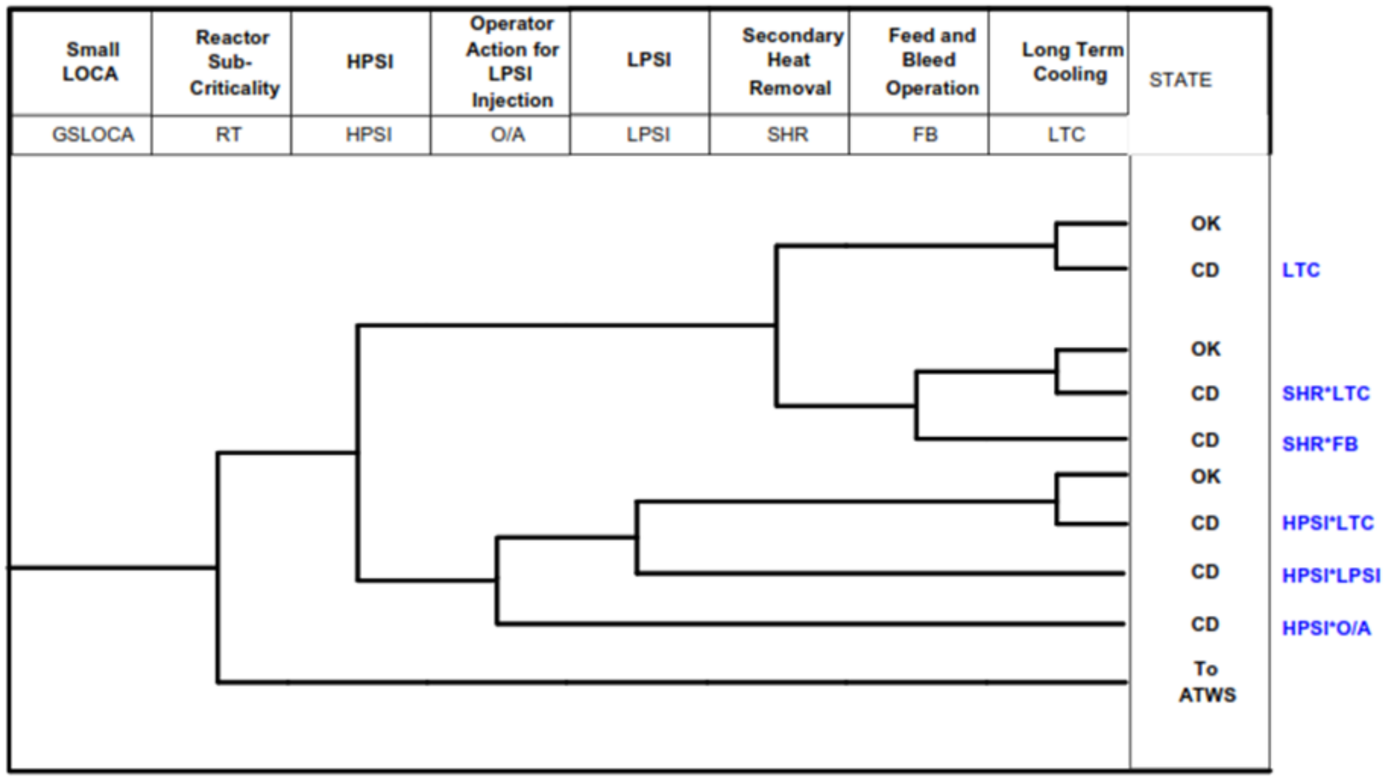
1 out of 3



CDF = 1.2 x 10^{-10} + 1.2 x 10^{-12} + 2.4 x 10^{-14} + 6 x 10^{-10} + 3 x 10^{-11} = 7.51 x 10^{-10} /reaktor tahun

Analisis Pohon Kejadian (ETA)

Contoh Penyederhanaan Sekuensi Kecelakaan

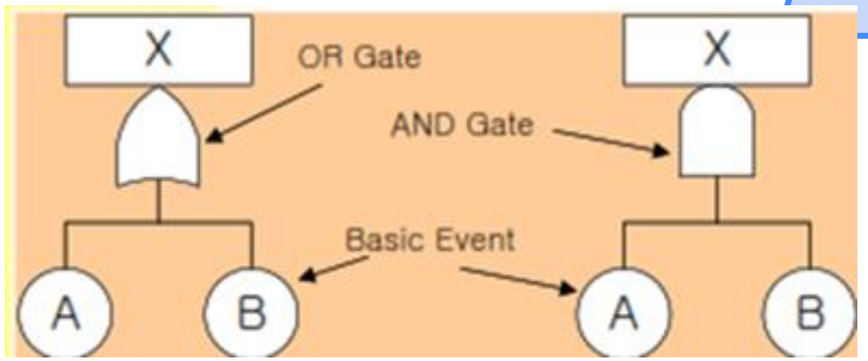


$$CDF_{SL} = GSLOCA*(LTC + SHR*LTC + SHR*FB + HPSI*LTC + HPSI*LPSI + HPSI*O/A)$$
$$= GSLOCA*(LTC + SHR*FB + HPSI*LPSI + HPSI*O/A)$$

Identik dgn CDF sebagai Top Event

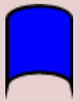
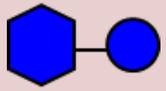
Analisis Pohon Kegagalan (FTA)

- Analisis Pohon Kegagalan (Fault Tree Analysis/FTA) digunakan untuk mengidentifikasi bagaimana suatu sistem, komponen, fungsi, atau operasi dapat mengalami kegagalan
- Kelemahan sistem teridentifikasi
- Terintegrasi dengan CCF dan HRA
- Minimal Cut Set (MCS) adalah kombinasi minimum kejadian dasar (*basic event*) yang menyebabkan suatu sistem gagal.
- Analisis secara deduktif
- Menggunakan aljabar boolean dan logika

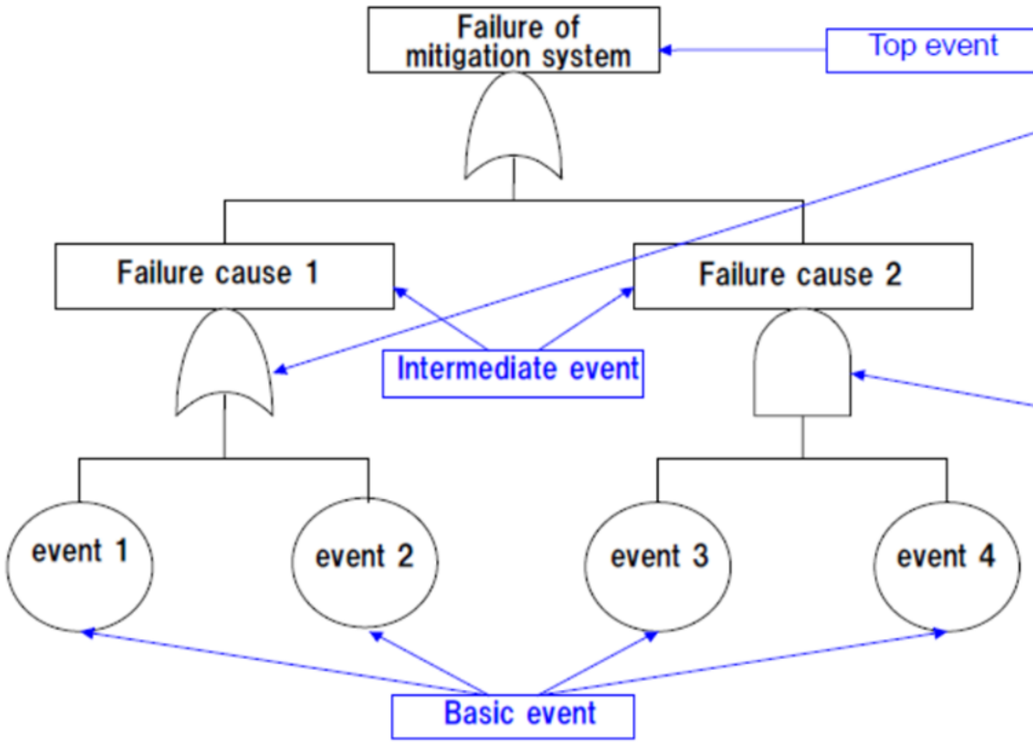


Law	Expression
Idempotent	A + A = A A . A = A
Commutative	A + B = B + A A . B = B . A
Distributive	A . (B + C) = A . B + A . C
Absorption	A + (A . B) = A

Analisis Pohon Kegagalan (FTA)

Simbol	Nama	Deskripsi
	Basic Event	Kejadian dasar yang tidak dapat diuraikan lebih lanjut.
	An Event/Fault	Kejadian antara (*intermediate event*) atau kejadian puncak (*top event*). Keduanya merupakan hasil dari kombinasi logis dari kejadian-kejadian pada tingkat yang lebih rendah.
	OR Gate	Salah satu dari kejadian dasar (*bottom event*) dapat mengakibatkan terjadinya kejadian puncak (*top event*).
	AND Gate	kejadian puncak (*top event*) terjadi, apabila semua kejadian dasar (*bottom events*) terjadi.
	Undeveloped Event	Suatu kejadian yang tidak dikembangkan lebih lanjut, karena keterbatasan data.
	External Event	Suatu kejadian yang berasal dari luar sistem dan dapat menyebabkan kegagalan.
	Inhibit Gate	Kejadian puncak (top event) hanya akan terjadi apabila kejadian dasar (bottom event) terjadi dan kondisi penghambat (inhibit condition) benar/terpenuhi.

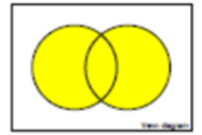
Analisis Pohon Kegagalan (FTA)



OR gate

Occurrence of either event of 1 or 2 results in occurrence of failure cause 1.

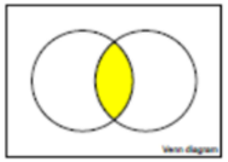
It means logical addition of two events:
(occurrence probability of event 1) +
(occurrence probability of event 2).



AND gate

Concurrent occurrence of both events of 3 and 4 results in occurrence of failure cause 2..

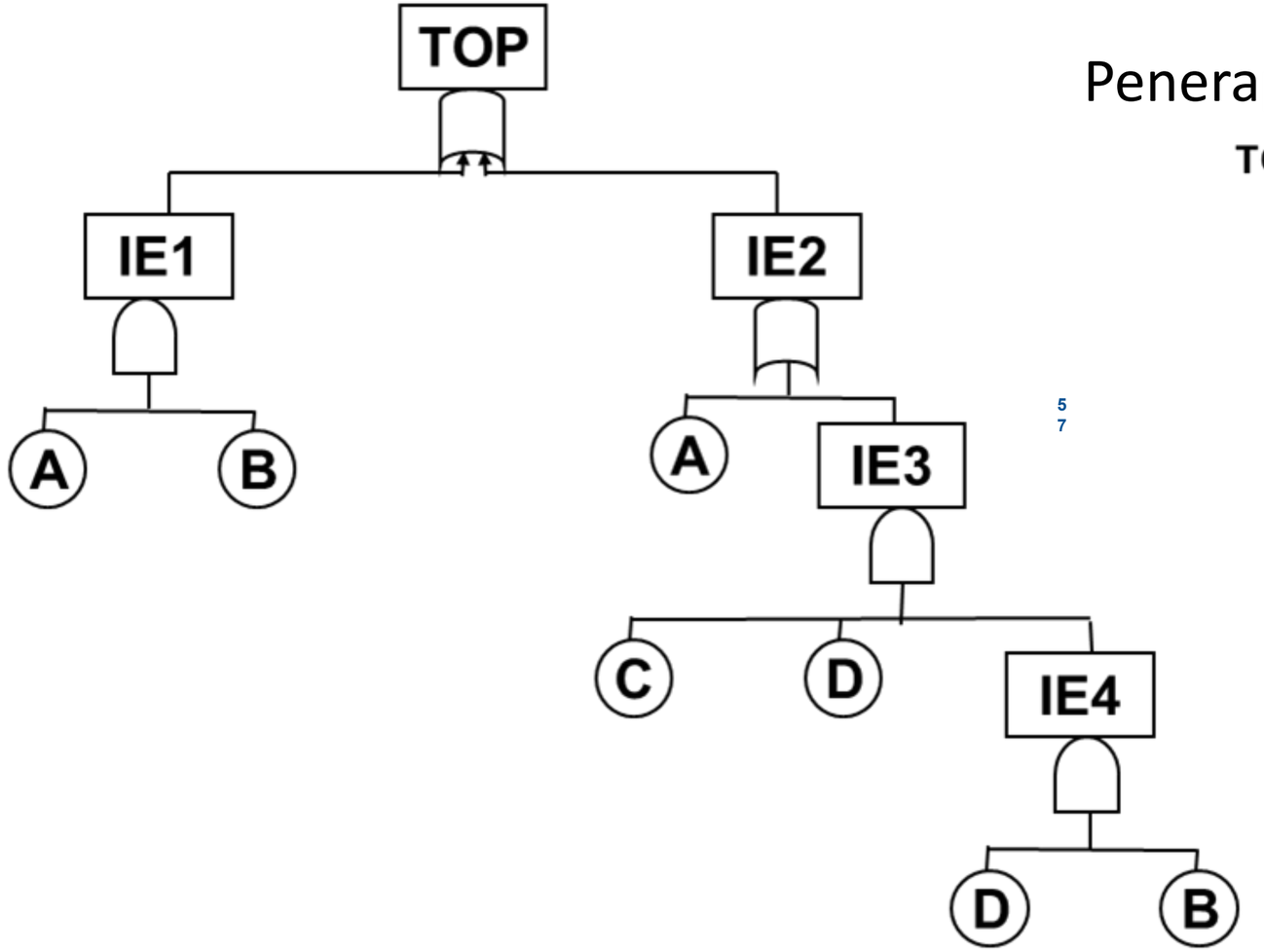
It means logical product of the two events,
(occurrence probability of event 3) x
(occurrence probability of event 4).



This fault tree is expressed in a formula as follows:

(failure of mitigation system) = (occurrence of event 1) + (occurrence of event 2)
+ (occurrence of event 3) x (occurrence of event 4)

Analisis Pohon Kegagalan (FTA)



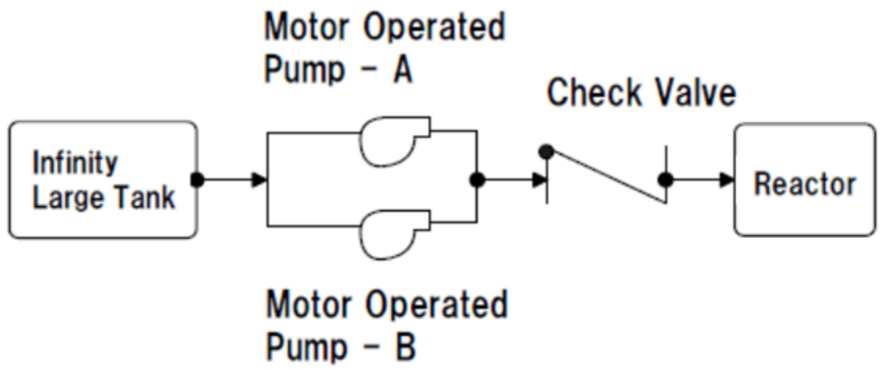
57

Penerapan Reduksi Aljabar Boolean

TOP = IE1 + IE2
= (A.B) + (A + IE3)
= A.B + A + (C.D.IE4)
= A.B + A + (C.D.D.B)
= A + A.B + B.C.D.D (D.D = D)
= A + A.B + B.C.D (A + A.B = A)
= A + B.C.D

- Minimal cut set: A dan B.C.D
- Top Event akan terjadi, apabila A atau (B.C.D) terjadi

Analisis Pohon Kegagalan (FTA)



Gbr 1. Sistem Injeksi Teras

Hitung ketidaktersediaan (unavailability) dari sistem injeksi teras yang disederhanakan sebagaimana ditunjukkan pada Gambar 1 dan Tabel 1.

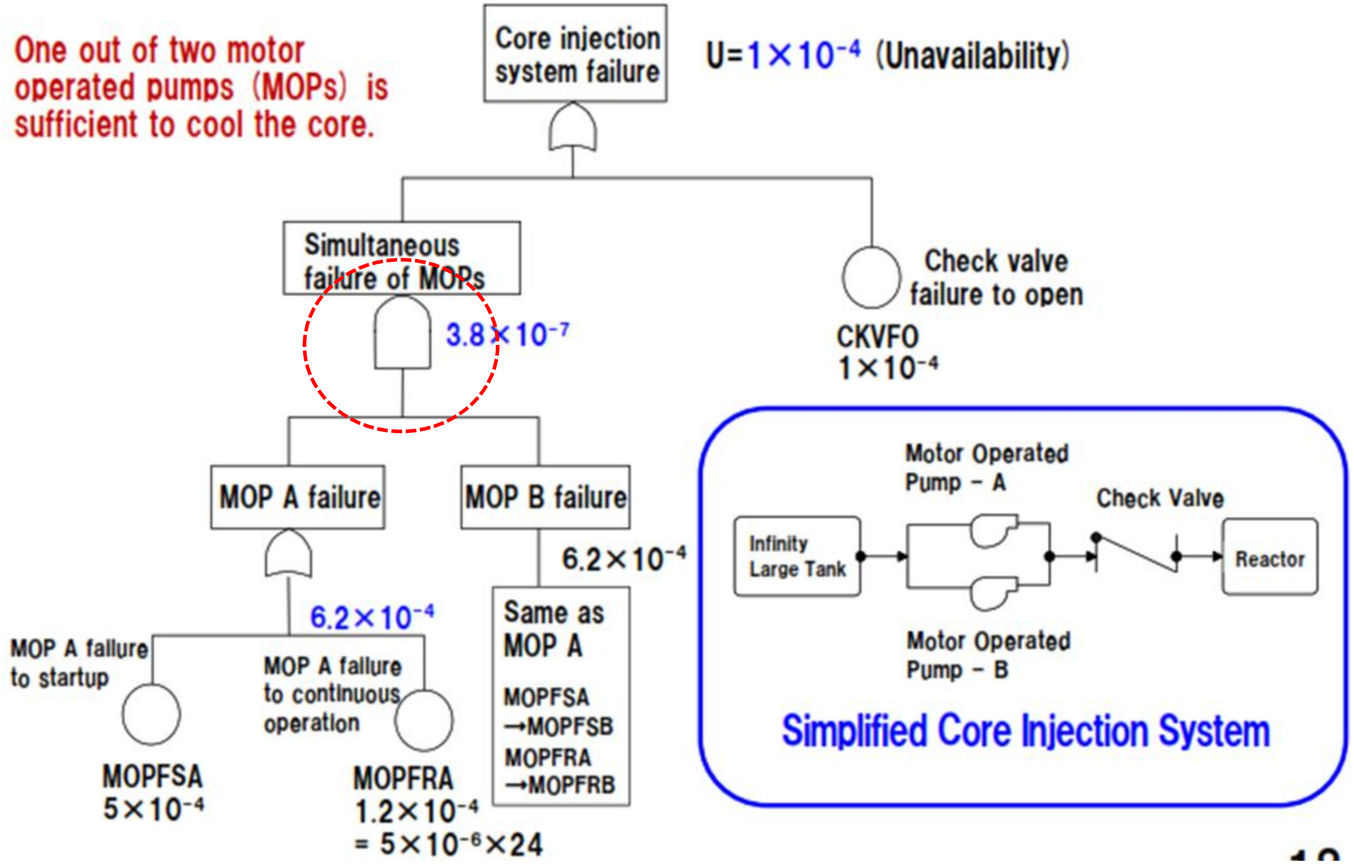
- Sistem mengambil air dari tangki berukuran tak terhingga dengan dua pompa motor yang terpasang paralel (motor operated pumps/MOPs) dan menginjeksikan air ke dalam reaktor.
- MOP[5][3] mampu mendinginkan teras reaktor dengan kriteria 1 out of 2
- Waktu misi 24 jam

Tabel 1. Data Kegagalan Komponen

Komponen	Mode Kegagalan	Data Kegagalan
Motor Operated Pump (MOP)	Failure to Startup (MOPFS)	5×10^{-4} /d
	Failure to continuos operation (MOPFR)	5×10^{-6} /h
Check Valve	Failure to open	1×10^{-4} /d

Analisis Pohon Kegagalan (FTA)

Kriteria sukses 1 out of 2



Analisis Pohon Kegagalan akan berubah, apabila:

- Kriteria sukses 2 out of 2
- Kegagalan suplai daya:
  - Sumber sama
  - Sumber berbeda

Pertimbangan PSA Pada SFR, MSR dan HTGR

Reaktor	Karakteristik	Pertimbangan pada PSA
Fast Reactors (SFR/LFR)	• Tanpa moderator; spektrum neutron cepat • Pendingin logam cair (natrium, timbal) • Risiko reaktivitas kimiawi (e.g., natrium-air atau kebakaran natrium-udara)	Kejadian dan modus kegagalan baru: • Kebocoran pendingin logam cair • Pembekuan atau korosi garam • Kegagalan material pada temperatur tinggi Rentetan kecelakaan berbeda: • Bukan LOCA konvensional • Perubahan geometri teras akibat bahan bakar cair • Fitur keselamatan teknis yang unik Diperlukan model PSA yang disesuaikan: • ET dan FT tradisional tidak sepenuhnya mampu merepresentasikan perilaku dinamis • Pendekatan PSA dinamis dan berbasis simulasi
Molten Salt Reactors (MSR)	• Bahan bakar cair dan tersirkulasi • *On-line refueling* dan modus kegagalan berbeda • Sistem keselamatan pasif berupa *freeze plugs* dan *drain tanks*	
HTGRs	• Penggunaan bahan bakar TRISO dengan kapasitas pengungkungan (containment) yang tinggi • Pendingin helium, densitas daya rendah, marjin termal yang tinggi	

Perbedaan PSA Konvensional dan Dynamic PSA

Aspek	PSA Konvensional (Statis)	Dynamic PSA
Pendekatan	Berdasarkan logika diskrit (pohon kejadian / pohon kegagalan)	Berdasarkan simulasi real-time (misal: Monte Carlo, pemodelan termohidraulik)
Perilaku Sistem	Dianggap tetap / tidak berubah selama kejadian	Diperhitungkan berubah seiring waktu (dinamis)
Interaksi Sistem	Terbatas, diasumsikan independen	Dapat menangani interaksi kompleks antar sistem dan kegagalan berganda
Contoh Penggunaan	Reaktor air ringan (LWR) konvensional	Reaktor generasi lanjut, sistem dengan perilaku dinamis tinggi

Terima kasih