Nuclear Reactor Safety: Probabilistic Safety Assessment

D. T. Sony Tjahyani

Research Center for Nuclear Reactor Technology

National Research and Innovation Agency (BRIN)

FTC on Reactor Engineering and Safety I

17 – 21 February 2025

Content

- Introduction
- Risk and PSA Concept
- Scope PSA
- Overview PSA (Level 1, 2 and 3)
- Level 1 PSA (Initiating Event, Event tree, Fault Tree)

Introduction

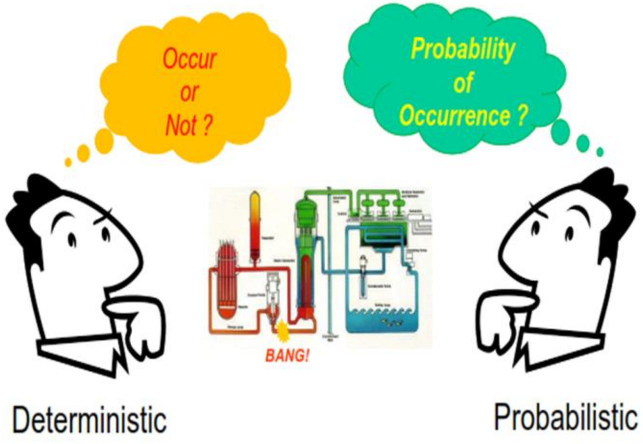
Safety Analysis Methods

Deterministic Safety Analysis (DSA)

- Predicts the response to PIE with predetermined assumptions
- Checks fulfilment of acceptance criteria

Probabilistic Safety Analysis (PSA)

- Combines the likelihood of PIE, potential scenarios and their consequences of CDF, source term or overall risk



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

Introduction

Deterministic	Probabilistic
Analyze only pre selected sequences to prove core damage will not occur	Analyze all sequence that can happen in real situations (Focus on sequences such as core damage sequence that can cause damage to the public and property)
Assume single failure only, assume system either operating or failed/no recovery	Consider multiple failures, assume systems can fail (or operate successfully) with some probabilities, credit for recovery, allow core damage
Does not investigate causes and impact of systems and components failures	Investigate causes and impacts of systems and components failures
Provides little information for risks, major contribution to the risks, and weakness of a plant	Provide more realistic assessment of the risks, evaluate likelihood as well as consequences, major contributors to the risks, and weakness of a plant

Risk Concept

- Probability – likelihood of an event occurring
- Frequency – number of occurrences of an event per unit of time
- Consequence – ultimate result of event in terms of public health impact, economic impact, etc.

  intermediate consequence measures are often used (e.g., core damage frequency, large early release frequency)

Risk Concept

- Risk – the frequency with which a given consequence occurs

$$\text{Risk}\left[\frac{\text{Consequence Magnitude}}{\text{Unit of Time}}\right] = \text{Frequency}\left[\frac{\text{Event}}{\text{Unit of Time}}\right] \times$$

$$\text{Consequences}\left[\frac{\text{Magnitude}}{\text{Event}}\right]$$

PSA Concept

- PSA - an analytical tool that answers three questions:
  - *What can go wrong? (accident scenario/sequence)*
  - *How likely is it to occur? (frequency)*
  - *What are the effects? (consequences)*

- PSA/PRA (Probabilistic Safety/Risk Analysis):
  - PSA is a methodology of risk assessment to provide a comprehensive, structured approach to identifying failure scenarios and deriving numerical estimated of the risks to workers and member of the public
  - PSA is a quantitative assessment of the risk from accidents in nuclear power plants
    - PSA = Probabilistic Safety Assessment (Japan, Korea, Canada etc)
    - PRA = Probabilistic Risk Analysis (USA)

PSA Concept

SF-1	SSR-2/1 (Rev.1) (Requirement 42)	SSR-2/1 (Rev.1) (Para 5.76)
• To ensure the protection of workers, the public and the environment, now and in the future, from harmful effects of ionizing radiation.	• A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis.	• The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states. • No PIE has a major contribution to risk • The levels of defence in depth are independent • To assure that no small deviations cause cliff edge effects • To compare the results of the analysis with the acceptance criteria for risk

PSA :

- To provide important safety insights in addition to those provided by deterministic analysis
- To identifying accident sequences that can follow from a broad range of initiating events
- a systematic and realistic determination of damage and radioactive releases and their frequencies

SF-1: Fundamental Safety Principles SSR-2/1: Safety of Nuclear Power Plants: Design

PSA Concept

Probabilistic Safety Assessment

Level 1 PSA

- The design and operation of the plant are analysed.
- To identify the sequences of events that can lead to core and/or fuel damage.
- To estimate core and/or fuel damage frequencies.

→

- **The strengths and weaknesses of structures, systems and components (SSCs).**
- **Procedures in place or envisaged to prevent core and/or fuel damage.**

Level 2 PSA

- Progression of core and/or fuel damage sequences and phenomena of severe damage.
- identifies ways in which associated releases of
- radioactive material from fuel can result in releases to the environment.
- To estimate the frequency and other relevant characteristics of releases of radionuclides to the environment.

→

- **Accident prevention and mitigation measures.**
- **Physical barriers to the release of radionuclides to the environment.**

Level 3 PSA

- Public health and other societal consequences

→

The contamination of land or food from the accident sequences that lead to a release of radioactive material to the environment.

PSA Concept

Level 1

- Identification of core damage sequences
- Quantification of sequence frequencies

Core damage sequence and frequencies

Level 2

- Evaluation of core and containment response
- Source term analysis

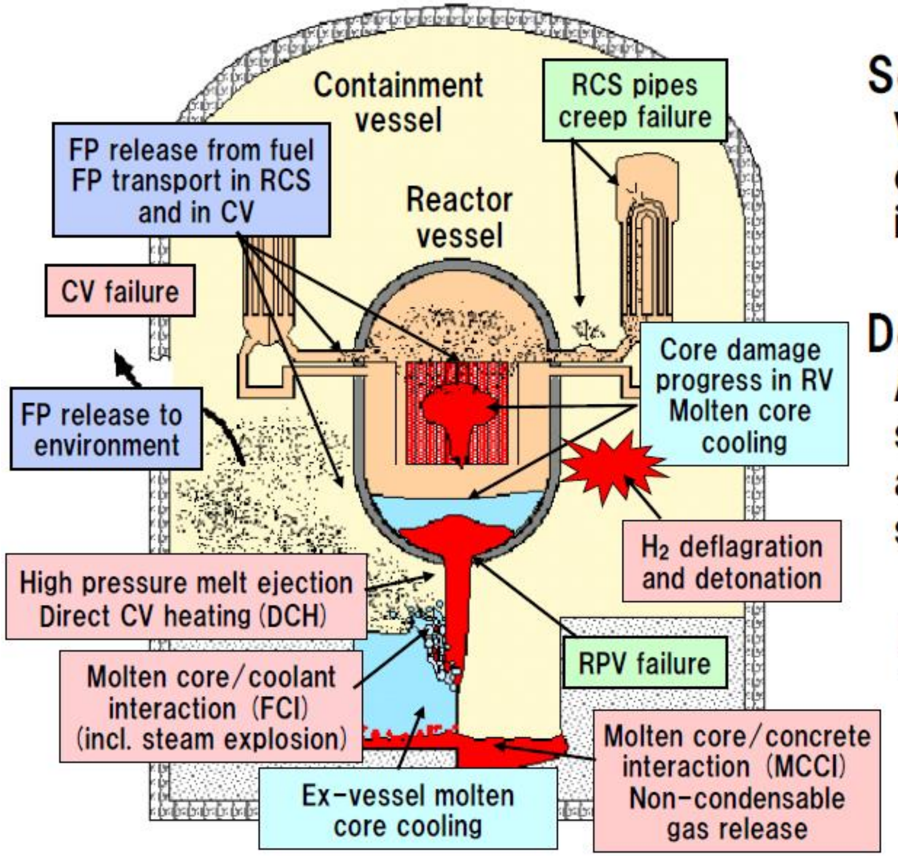
Type, amount and frequencies of release

Level 3

- Prediction of radionuclide transport
- Calculation of consequences

Risk to public health and property

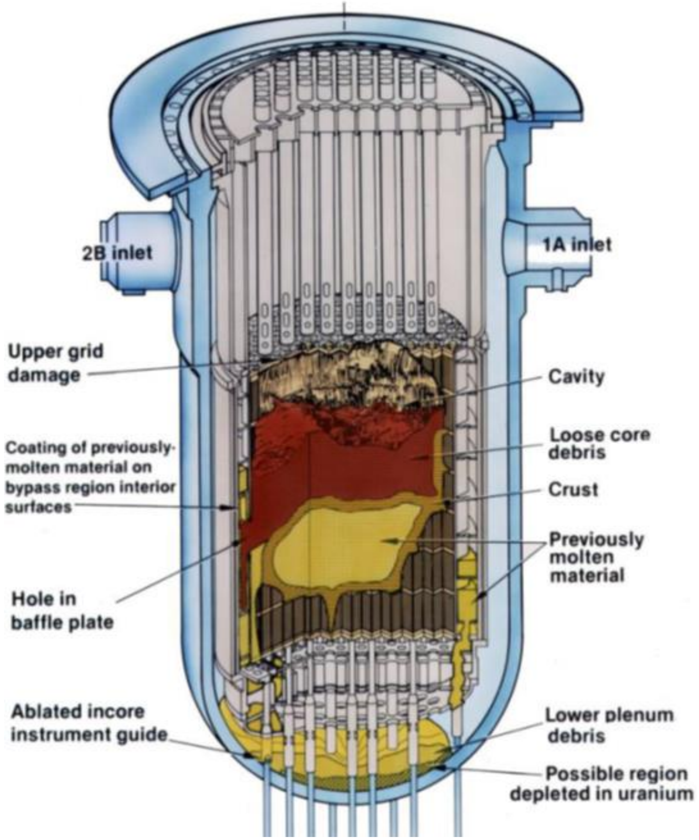
Level 1 PSA



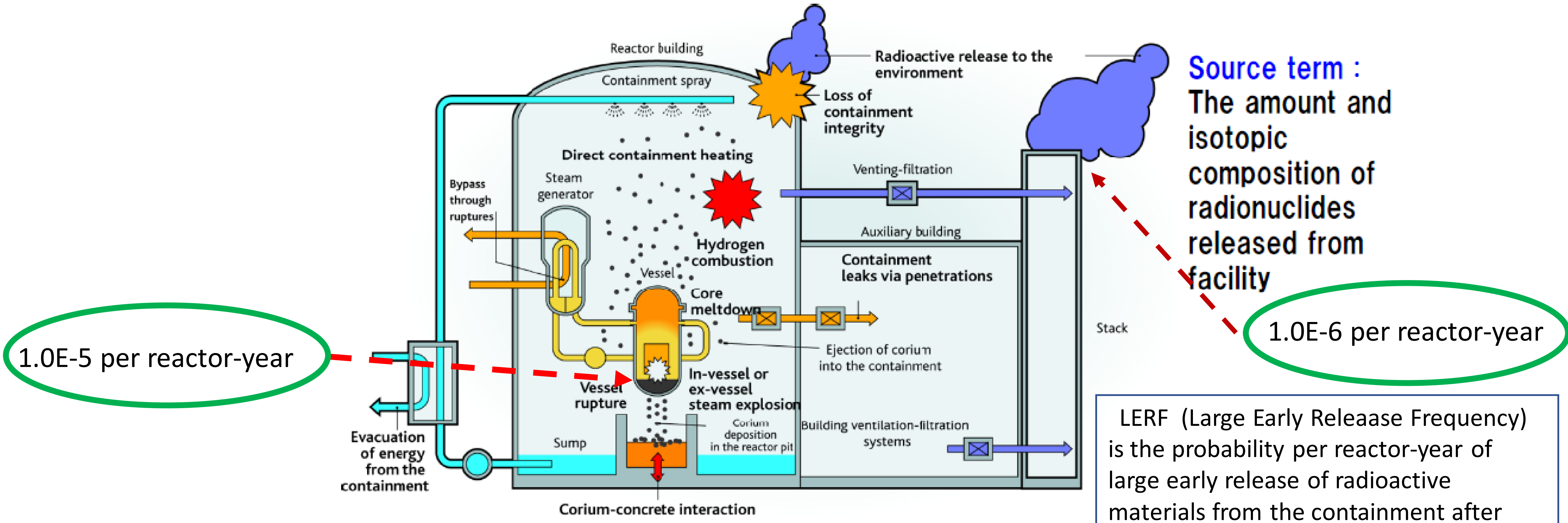
Severe Accident:
Very low frequency of occurrence but large influence on risk

Definition:
Accident conditions more severe than a design basis accident and involving significant core degradation

indicates phenomena that threaten CV integrity.



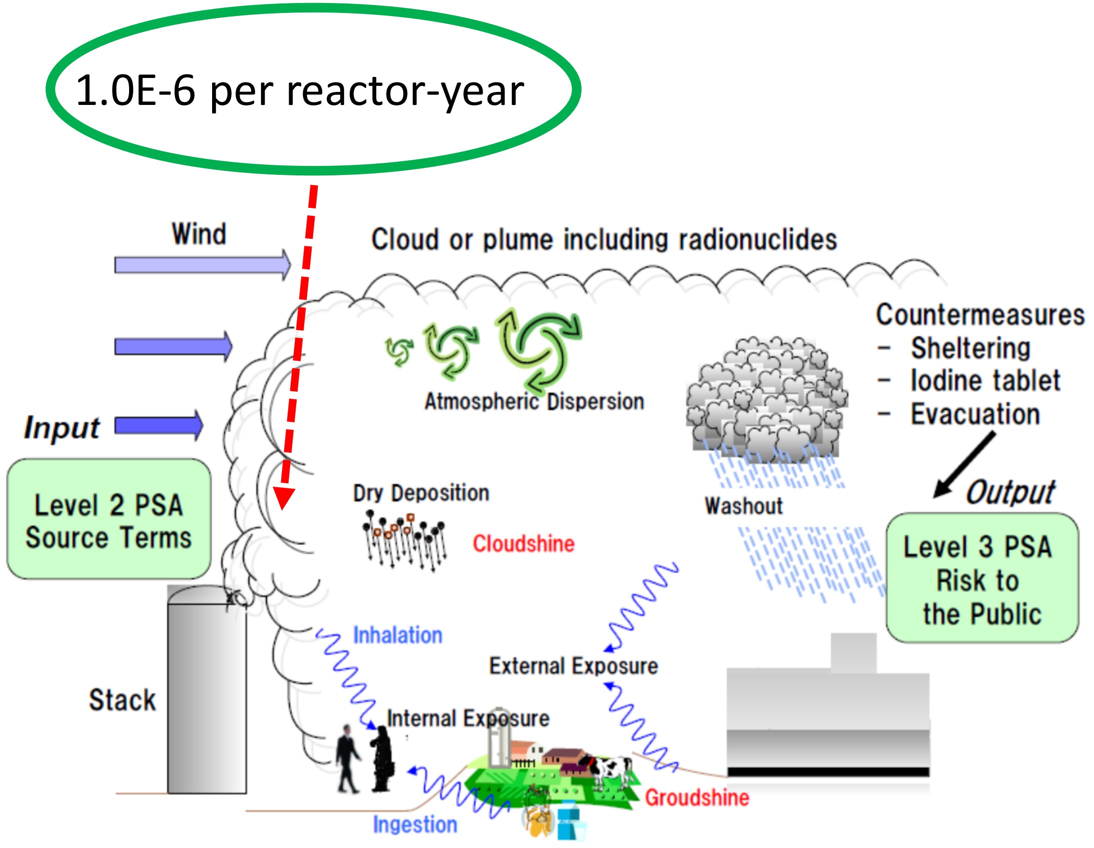
Level 2 PSA

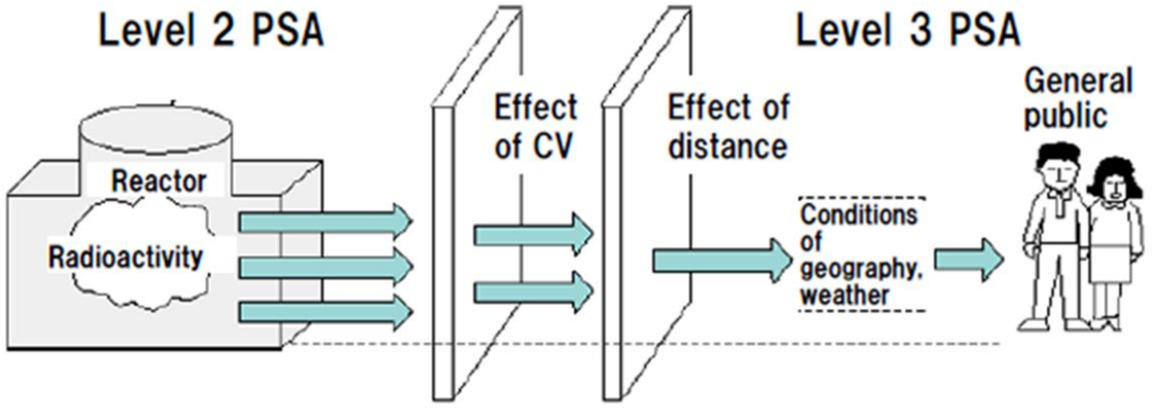


Source term :
The amount and isotopic composition of radionuclides released from facility

LERF (Large Early Releaase Frequency) is the probability per reactor-year of large early release of radioactive materials from the containment after core damage

Level 3 PSA


1.0E-6 per reactor-year
Wind
Cloud or plume including radionuclides
Atmospheric Dispersion
Countermeasures
– Sheltering
– Iodine tablet
– Evacuation
Input
Level 2 PSA Source Terms
Dry Deposition
Cloudshine
Washout
Output
Level 3 PSA Risk to the Public
Inhalation
External Exposure
Stack
Internal Exposure
Groudshine
Ingestion


Level 2 PSA
Level 3 PSA
Effect of CV
Effect of distance
General public
Reactor
Radioactivity
Conditions of geography, weather

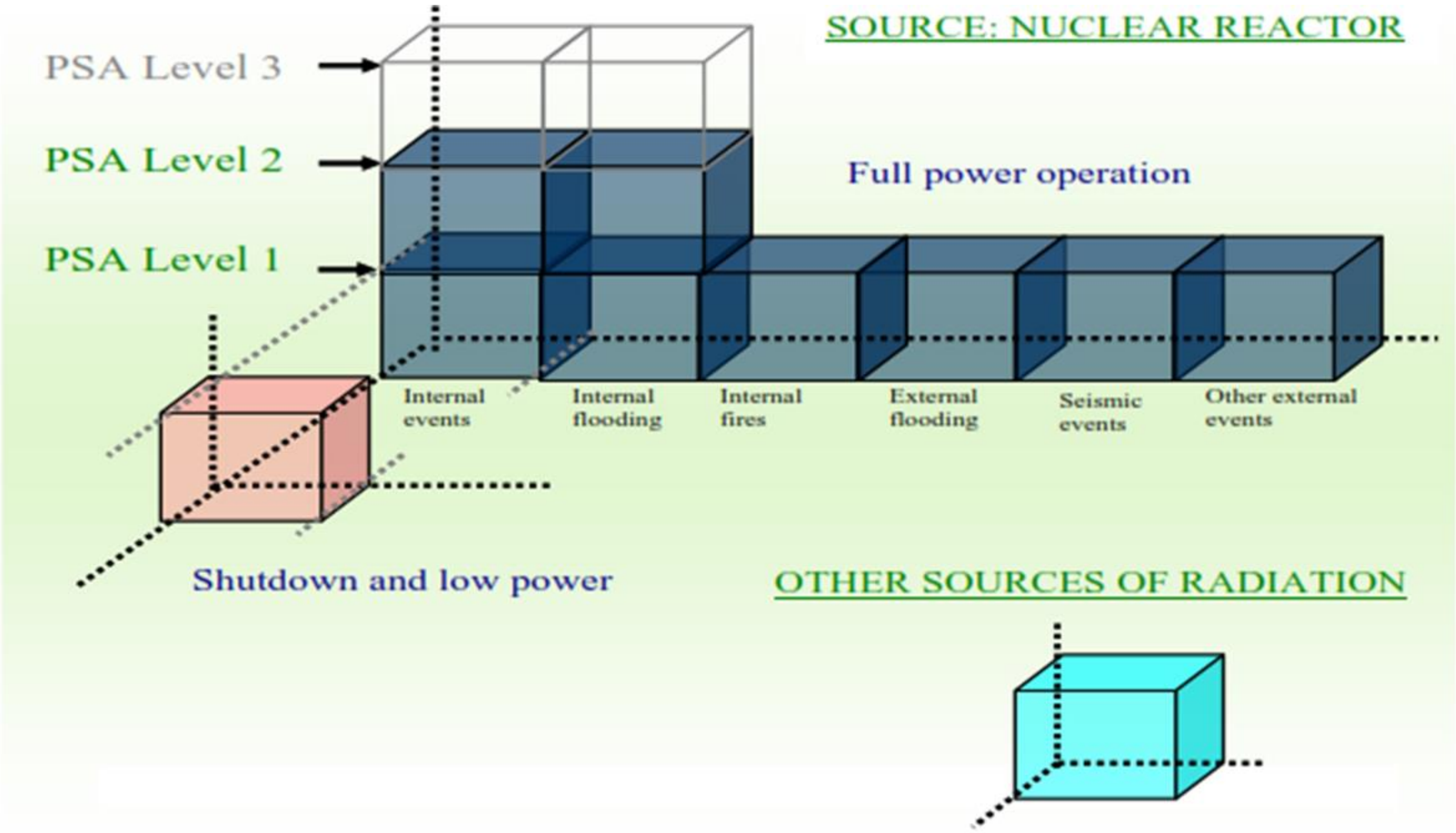
PSA Scope

- **End states (Consequences)**
  - Level 1 (Core Damage)
  - Level 2 (Containment Integrity)
  - Level 3 (Effect on public/environment)

- **Power level**
  - Full power PSA (100%)
  - Low power/shutdown PSA (LPSD)
    - ✓ Less than 20% power and refueling period
    - ✓ Need a separate model because possible initiating events and system configurations are significantly different from those during full power operation

- **Internal events and Hazard**
  - Internal (initiating) event PSA
    - ✓ Initiated by system/components failure internal to NPP
    - ✓ Example of internal events: LOCA, transients, loss of offsite power, SGTR
  - Internal Hazard
    - ✓ Example of internal events: internal fire, internal flooding, turbine missiles, internal explosion, etc
  - External Hazard
    - ✓ Example of external events: earthquake, fire, flooding, tsunami and human induced, etc

PSA Scope



SOURCE: NUCLEAR REACTOR
PSA Level 3
PSA Level 2
PSA Level 1
Full power operation
Internal events
Internal flooding
Internal fires
External flooding
Seismic events
Other external events
Shutdown and low power
OTHER SOURCES OF RADIATION

Risk During LPSD Operation

Potential Risk During Shutdown State

- Potential core damage is announced during mid-loop operation is shutdown state
  - ✓Loss of RHR (Residual Heat Removal)
- Most of accident could still occur
  - ✓SBO, LOCA,LOOP, PORV stuck, etc

Degraded Safety During Shutdown State

- Degraded defence in depth by maintenance
- Open containment
- Configuration of safety system is changed
- Increase human error possibility
- Lack of risk assessment and emergency procedure

Risk During LPSD Operation

LPSD Risk and PSA

- Core damage frequency from PSA is comparable with that from full power operation
- Loss of shutdown cooling during mid-loop operation is the most important initiating event
- Plant configuration changes and human error are the dominant contributors
- Challenges in LPSD PSA
  - ✓ Lack of data
  - ✓ A number of shutdown states, configuration changes, etc
  - ✓ Lack of procedures for emergency/abnormal events

LPSD PSA

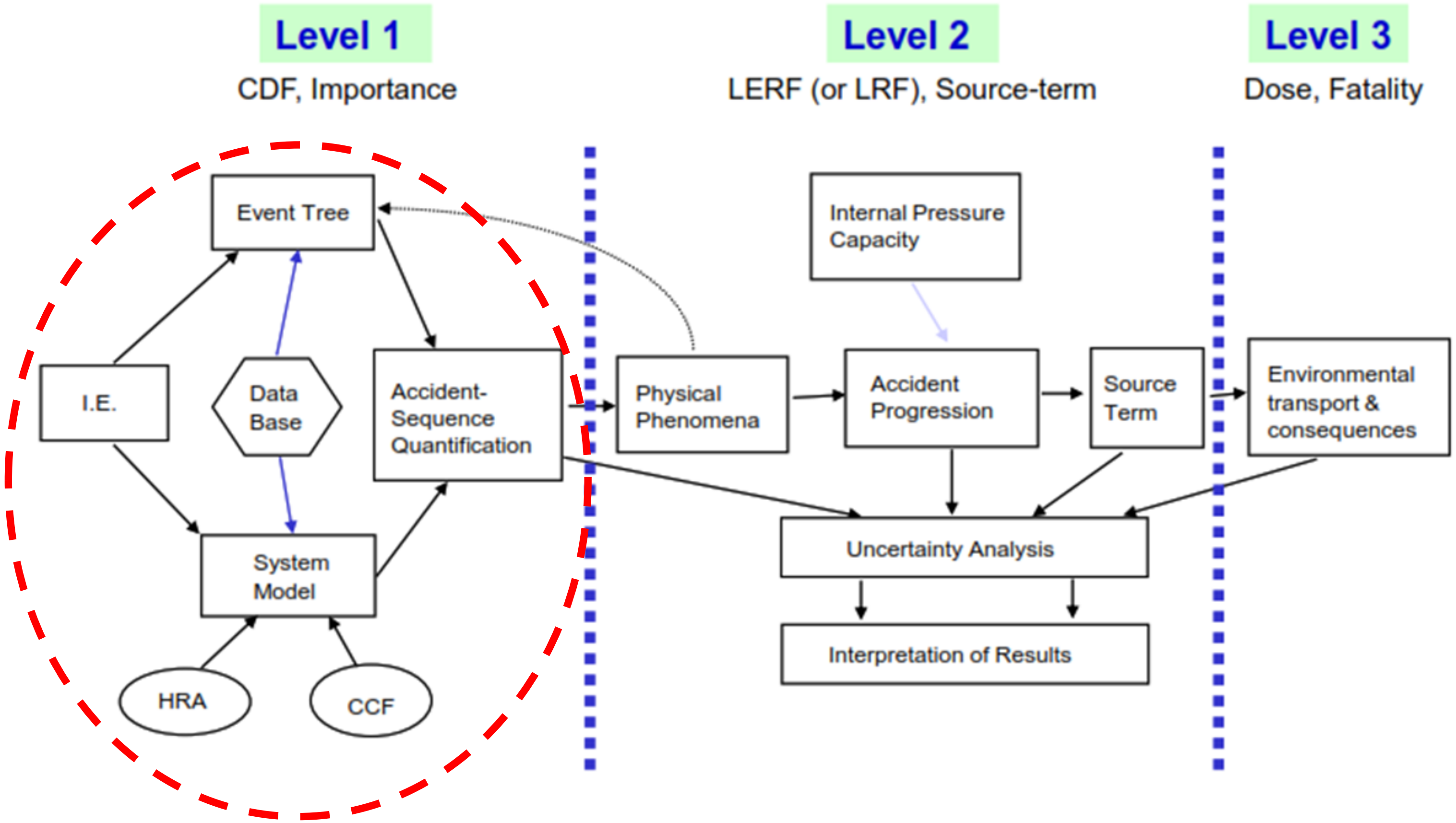
Objectives

- Estimate CDF during LPSD operation mode and its contribution to total plant CDF
- Identify insight and relative importance of SCCs (Structure, System and Components) and operator actions.

Overall process

- The LPSD operation mode is divide into a number of POSs (Plant Operation States) depending on:
  - ➢ Reactor power, RCS (Reactor Cooling System) level/temperature, plant configuration, etc
- For each POS, PSA model is developed and CDF is calculated based on:
  - ➢ possible initiating events, accident sequences, plant configuration and database
- Total CDF during LPSD operation mode is calculated by aggregating the CDFs of all POSs

Level 1 PSA



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

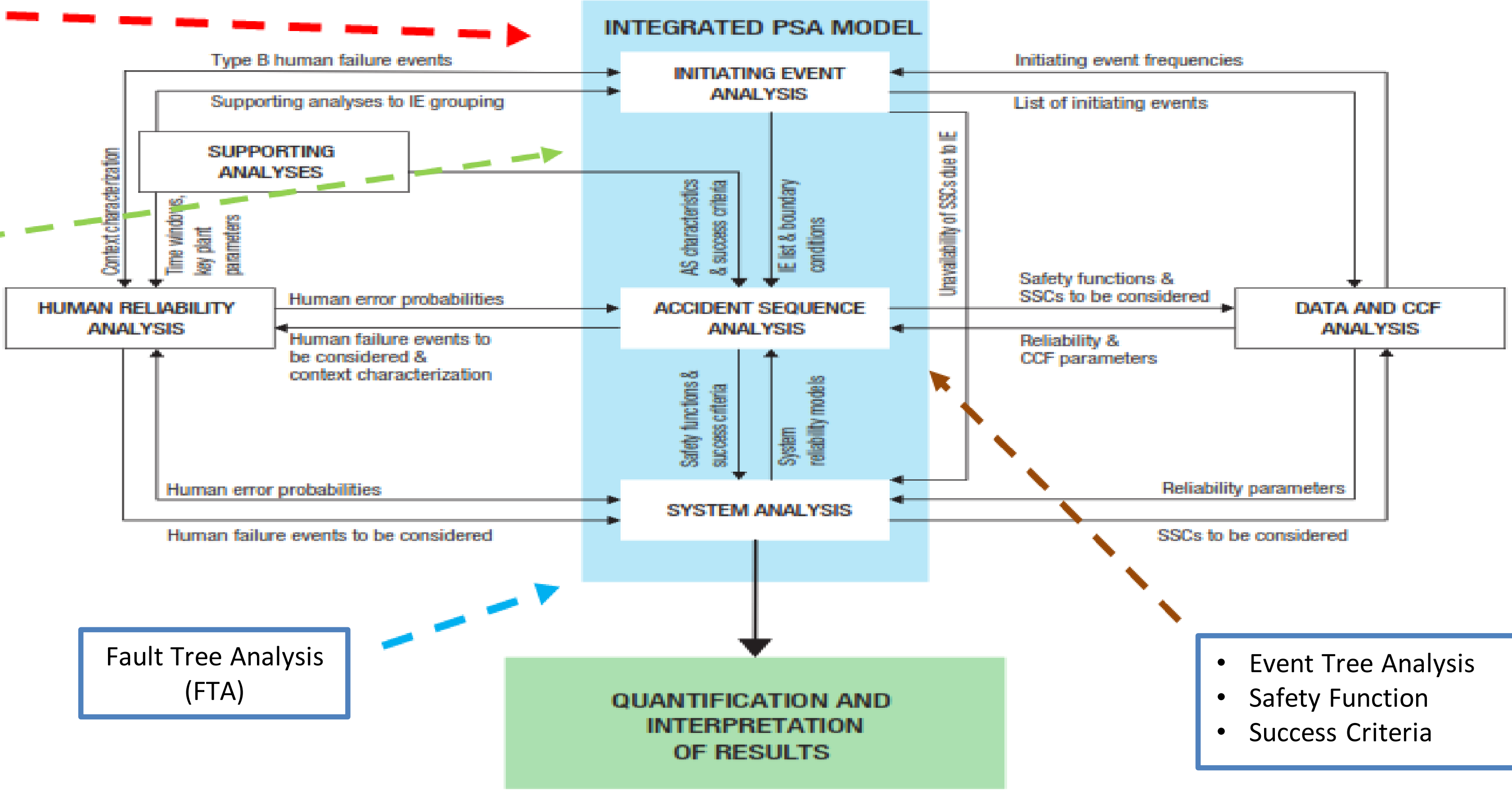
Tasks of Level 1 PSA: Internal Initiating Event

Initiating Event:
- Grouping
- Quantification

Failure:
- Type A
- Type B
- Type C

Quantification of Human Error

Common Cause Failure for System and Component

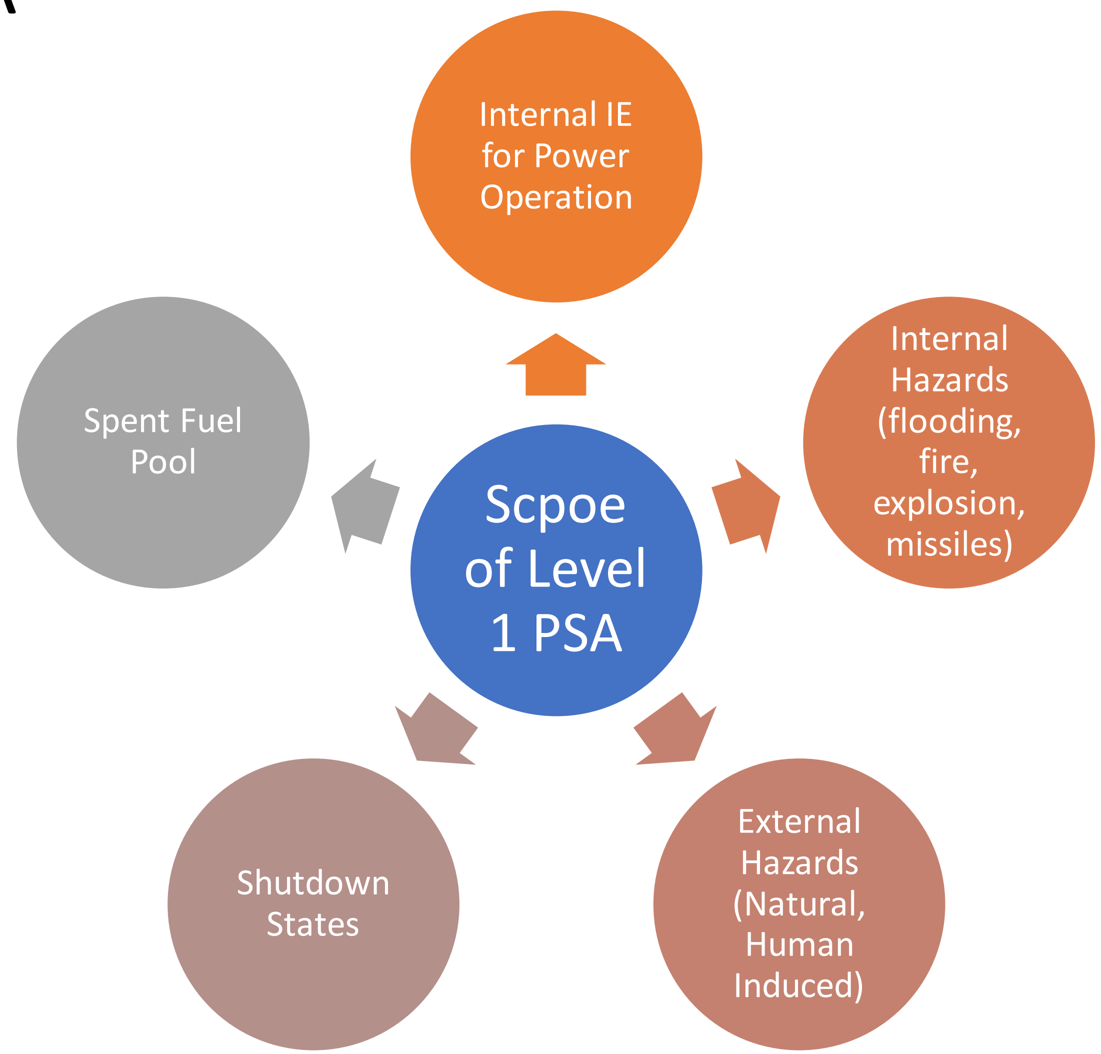


Fault Tree Analysis (FTA)

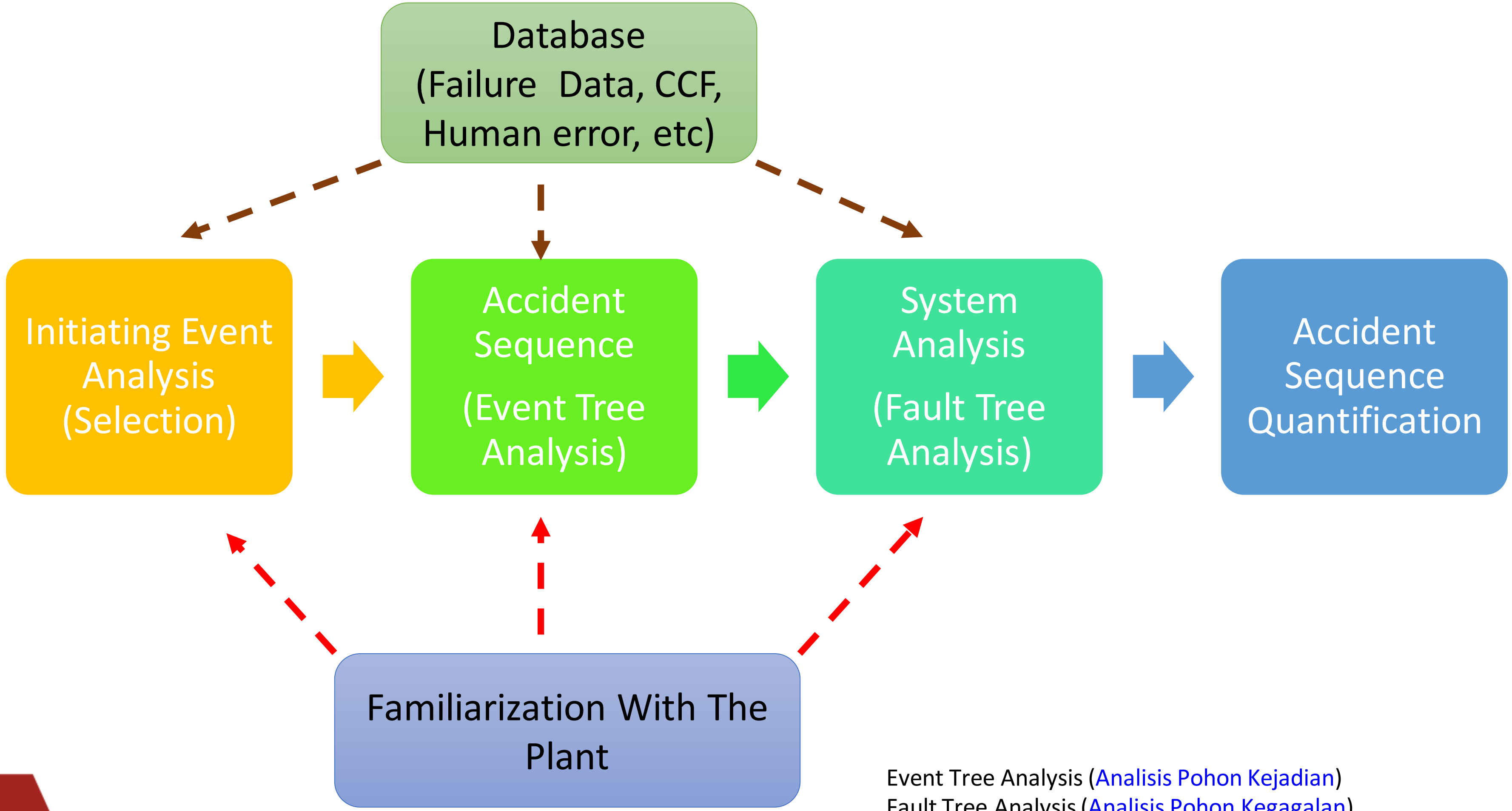
- Event Tree Analysis
- Safety Function
- Success Criteria

Source: SSG-3 Rev.1

Level 1 PSA


Internal IE for Power Operation
Internal Hazards (flooding, fire, explosion, missiles)
External Hazards (Natural, Human Induced)
Shutdown States
Spent Fuel Pool
Scpoe of Level 1 PSA

Simplified Process of Level 1 PSA



Event Tree Analysis (Analisis Pohon Kejadian)
Fault Tree Analysis (Analisis Pohon Kegagalan)

Level 1 PSA

FAMILIARIZATION WITH THE PLANT AND COLLECTION OF INFORMATION

- Safety analysis report
- Technical specifications
- Descriptions of systems
- As built (as is) system drawings
- Electrical line drawings
- Control and actuation circuit drawings
- Procedures (Normal operating, Emergency, Maintenance, etc}

- Success criteria of systems
- Operating experience
- Operators' logs
- Discussions with operating personnel
- Plant operational records and reports of shutdowns
- Plant databases

- Plant layout drawings
- Drawings of piping location and routing
- Drawings of cable location and routing
- Plant walkdown reports
- Regulatory requirements
- Other relevant plant documents

Initiating Event

Initiating Event

- An event which creates a disturbance in the plant and has the potential of leading to core damage

Transient

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

LOCA

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

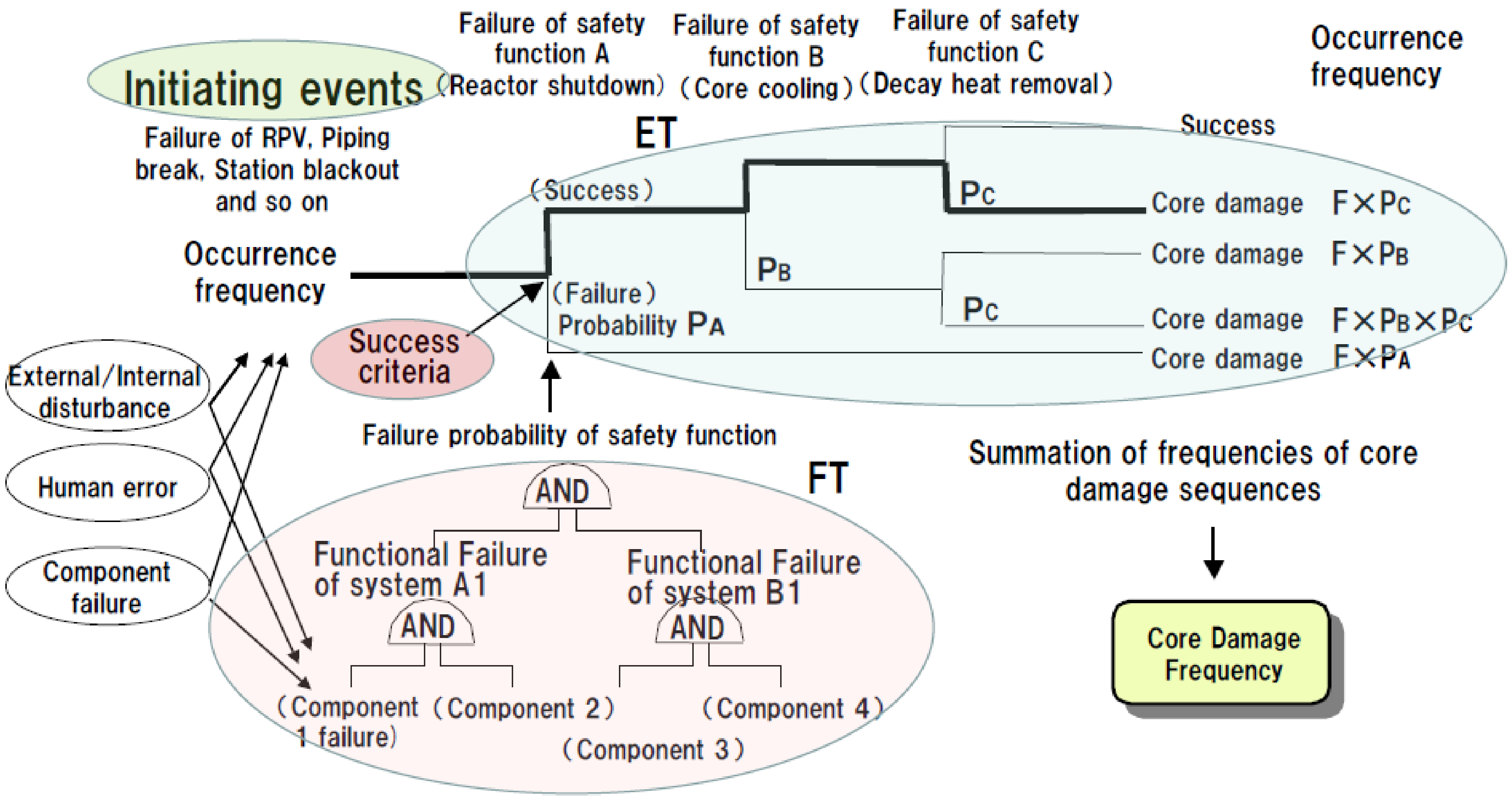
Initiating Event Analysis

- Identify and get raw data from plant operational experiences (EPRI, NUREG, etc)
- Analyze using master logic diagrams
- IE frequency using FMEA

❑ ***Initiating event frequencies*** *(example)*

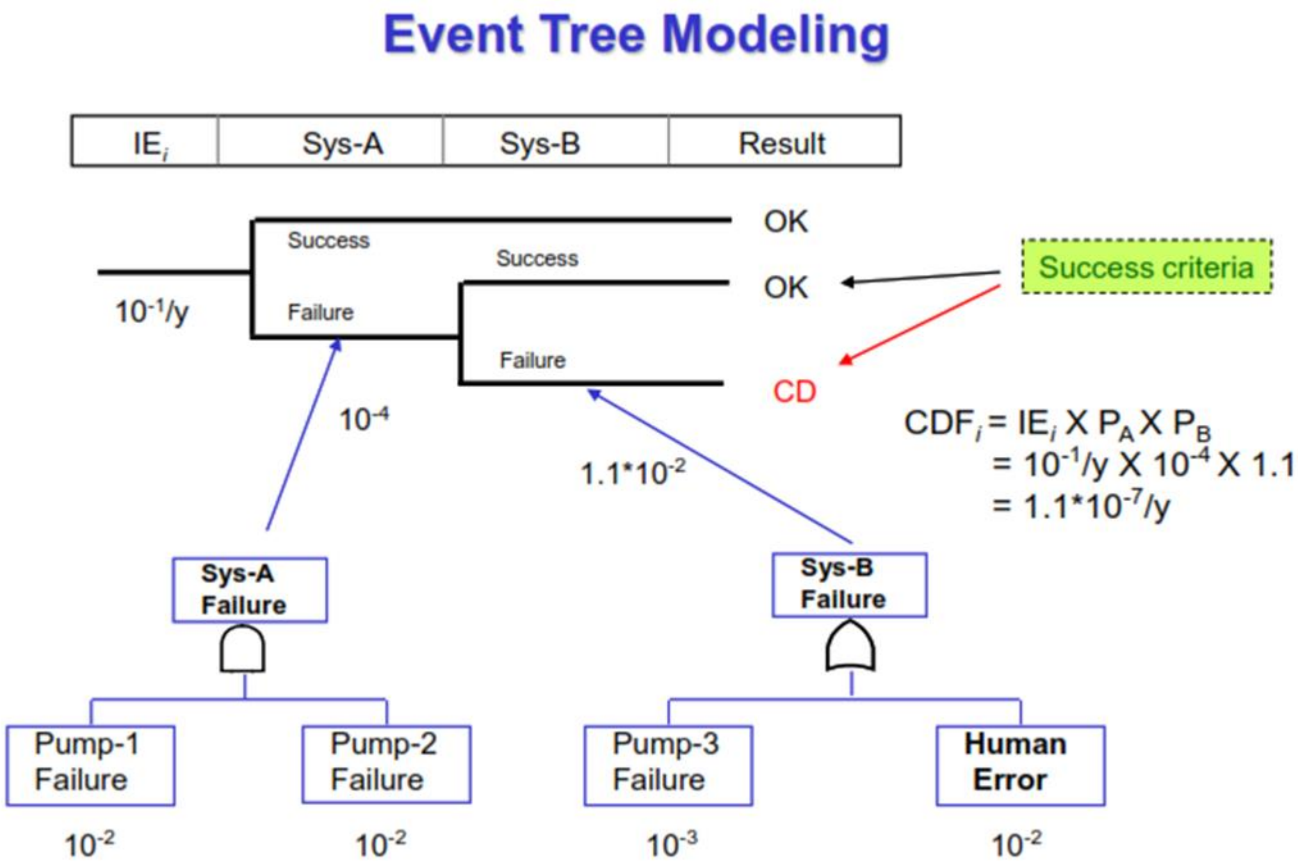
No.	Initiating Event	OPR-1000	NUREG/CR-5750
1	Large Loss of Coolant Accident	5.00E-06	5.00E-06
2	Medium Loss of Coolant Accident	4.00E-05	4.00E-05
3	Small Loss of Coolant Accident	4.80E-04	5.00E-04
4	Steam Generator Tube Rupture	7.10E-03	7.00E-03
5	Interfacing Systems LOCA	5.35E-08	2.00E-06
6	Reactor Vessel Rupture	2.66E-07	N/A
7	Large Secondary Side Break	1.10E-02	1.30E-02
8	Loss of Main Feedwater	8.40E-02	6.50E-02
9	Loss of Condenser Vacuum	4.90E-02	2.80E-02
10	Loss of a CCW Train	5.13E-01	9.70E-04
11	Loss of a 4.16KV AC bus	2.40E-02	1.40E-02
12	Loss of a 125V DC bus	1.70E-03	6.90E-04
13	Loss of Offsite Power	3.00E-02	2.40E-02
14	Station Blackout	3.66E-05	N/A
15	General Transients	9.46E-01	1.20E+00
16	Anticipated Transient Without Scram	9.00E-06	N/A
17	Loss of a 120V AC bus	1.30E-02	2.10E-03
18	RCP Seal LOCA	2.17E-03	2.50E-03

Simplified Structure of Level 1 PSA Calculation



- Core Damage is defined as failure of fuel cladding or pellets, not as melting of fuel
- Core Damage Frequency (CDF) is the probability per year of reactor operation (reactor year) of experiencing core damage accident
- Performance Target:
  - 1.0E-04 per reactor-year for existing plants
  - 1.0E-05 per reactor-year for future plant
  - < 1.0E-05 per reactor-year for Gen-III/III+

Simplified Structure of Level 1 PSA Calculation



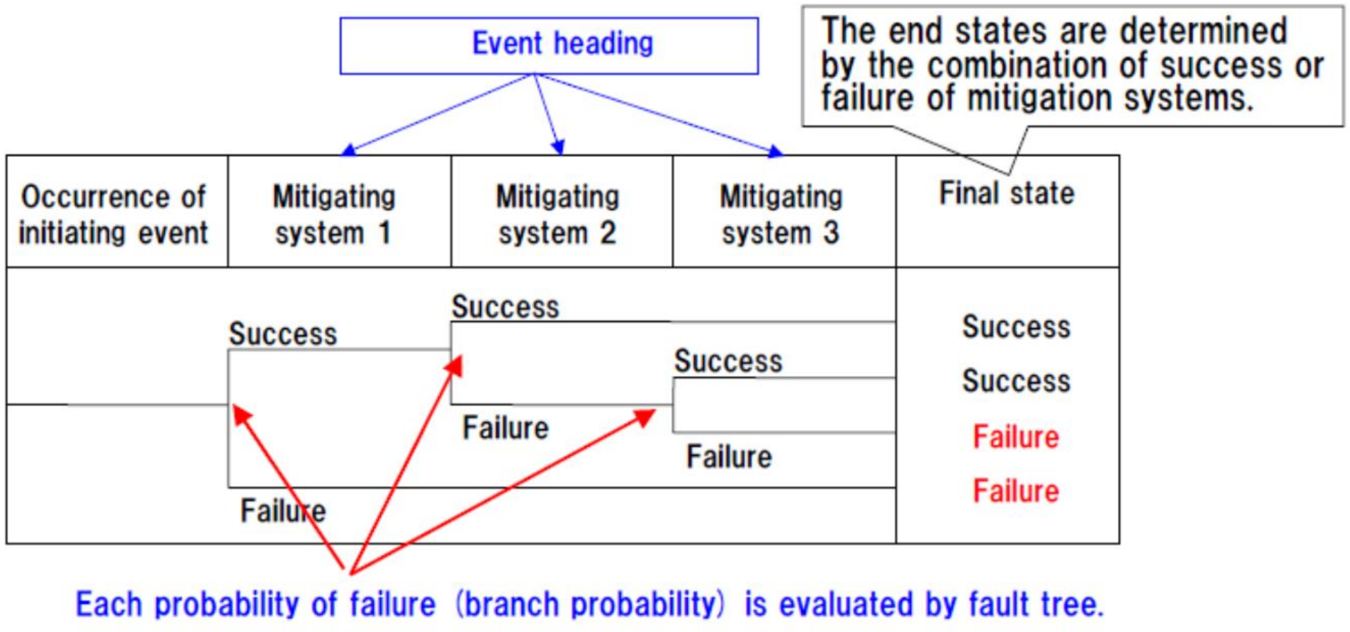
$$CDF_i = IE_i \times P_A \times P_B = 10^{-1}/y \times 10^{-4} \times 1.1*10^{-2} = 1.1*10^{-7}/y$$

Core Damage Frequency:

- Expected frequency (number of occurrences per unit time)
- Of accident sequences leading to core damage:
  - Core damage criteria: **Uncovery and heatup** of reactor core
- For all initiating events
- **Core damage or not**:
  - Determined whether the combination safety function against each accident sequence is enough or not to meet above core damage criteria
    - ➢ **Success criteria**

Accident Sequence (Event Tree Analysis)

- It is a tool to analyze processes from a starting incident (**group of initiating event**) to final state, by preceding the process into branches (like tree). Usually, a two-branch tree is used.
- The upper and lower branches express success and failure, respectively.
- Probabilities for reaching the final state are analyzed by inputting the occurrence probability of the initiating event and branch probabilities (success and failure probabilities) of events (called "Event Headings").
- Deternine accident sequences by which lead to core damage.



Accident Sequence (Sekuensi Kecelakaan, Rentetan Kecelakaan)

Accident Sequence (Event Tree Analysis)

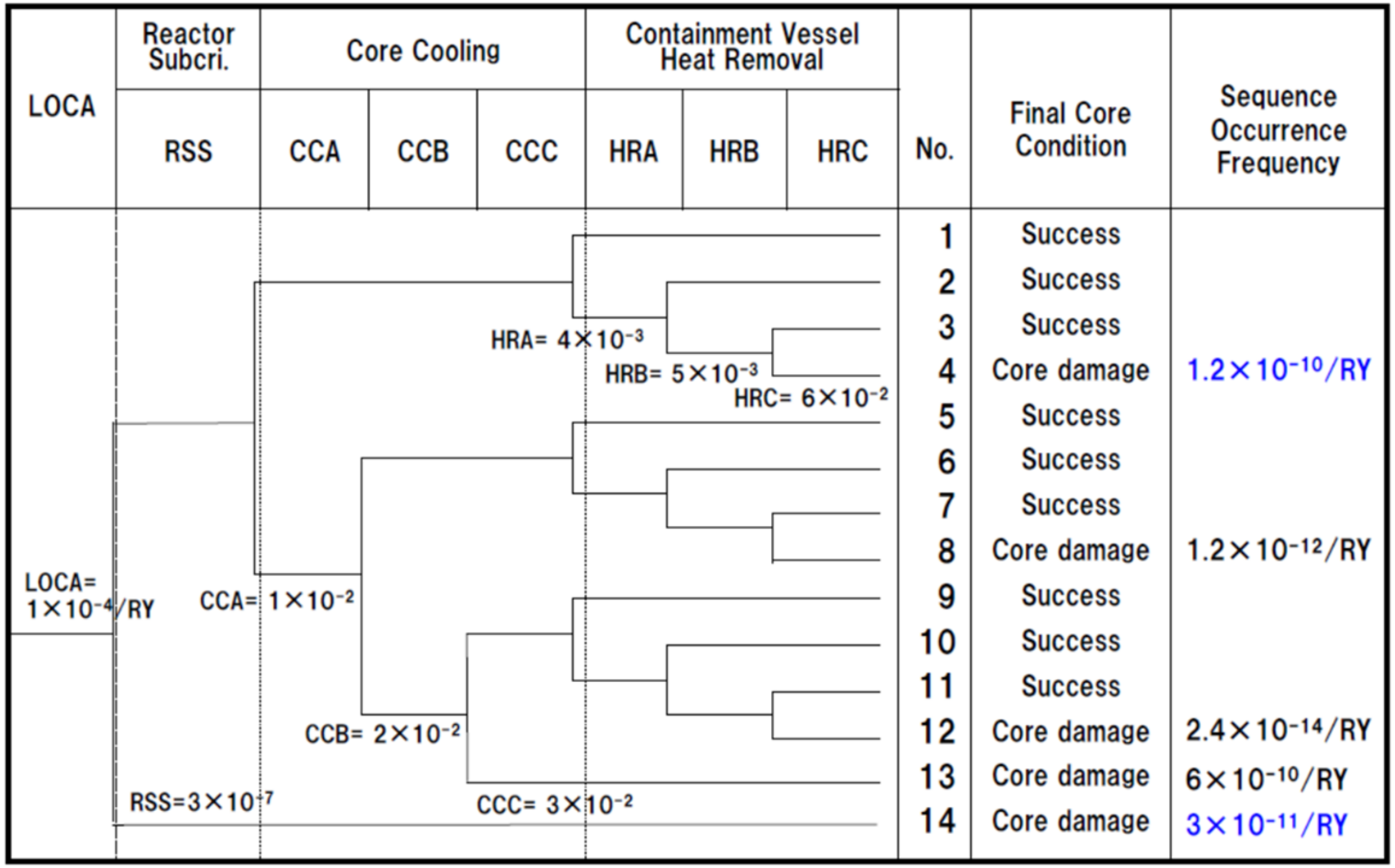
- Success Criteria:
  - Determined as the **minimum level of performance** required from the safety system.
  - Specify the **mission time** for the safety system based on the transient analysis carried out.
  - Also specify the requirements for the **support systems** based on the success criteria of the (frontline) safety system.
  - Need to identify the **operator actions** required to bring the plant to a safe, stable shutdown state.

Accident Sequence (Event Tree Analysis)

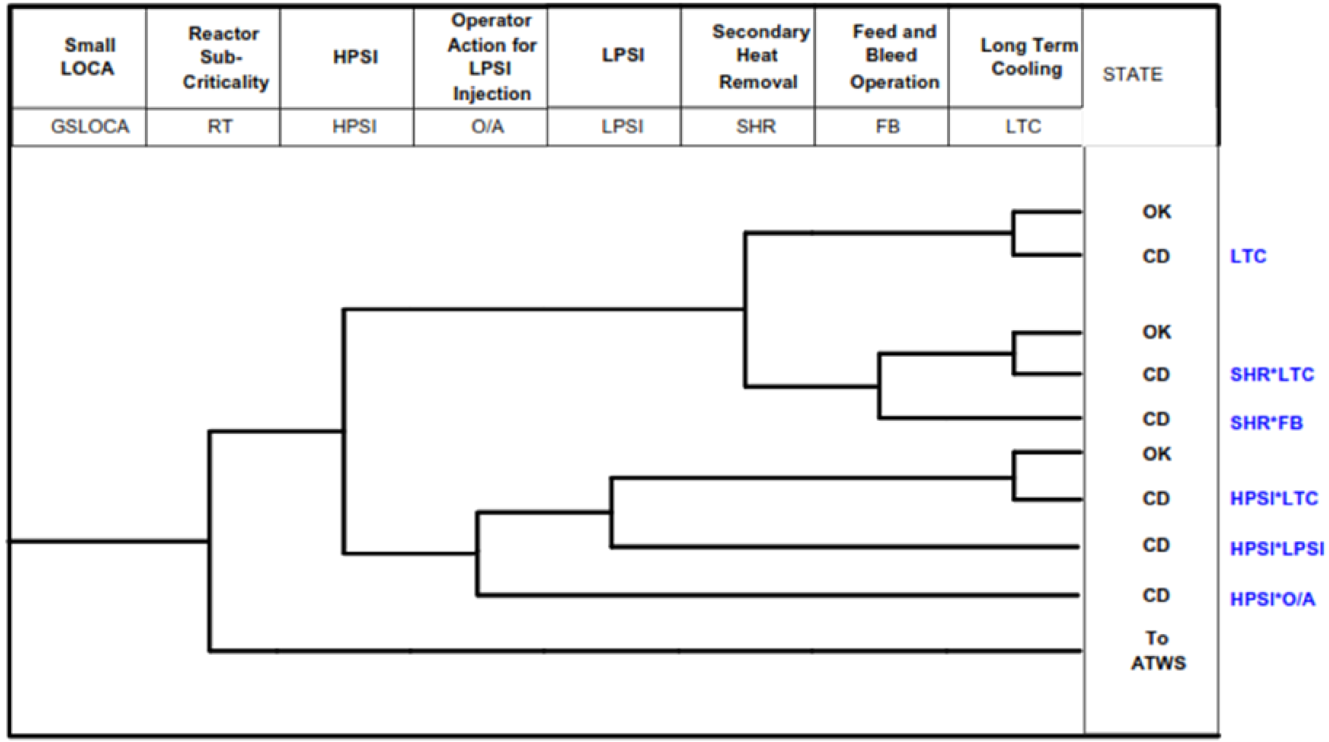
For the simple calculation, Table 1 is a success criteria of LOCA (Loss of Coolant Accident) for NPP. LOCA occurrence frequency is assumed to be 1E-04/RY (Reactor-Year).

Table 1. Success Criteria of LOCA for NPP

Mitigating function	Minimum required system	System unavailability
Reactor sub-criticality	RSS	$RSS=3\times10^{-7}$
Core cooling	CCA or CCB or CCC	$CCA=1\times10^{-2}$ $CCB=2\times10^{-2}$ $CCC=3\times10^{-2}$
Containment Vessel Heat Removal	HRA or HRB or HRC	$HRA=4\times10^{-3}$ $HRB=5\times10^{-3}$ $HRC=6\times10^{-2}$



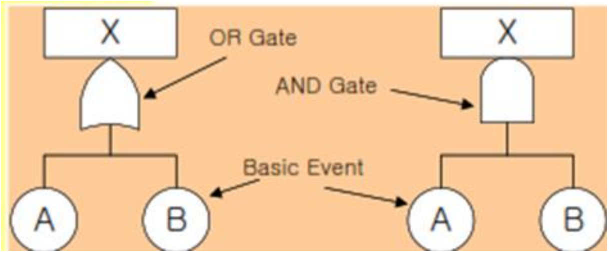
Accident Sequence (Event Tree Analysis)



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

System Analysis (Fault Tree Analysis)

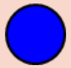
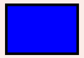
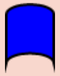
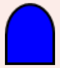
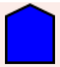
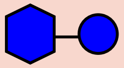
- Identify and model the possibilities in which a system may fail its function.
  - ✓ System weaknesses is identified.
  - ✓ in general, fault tree analysis technique is used.
  - ✓ CCF analysis & HRA are incorporated



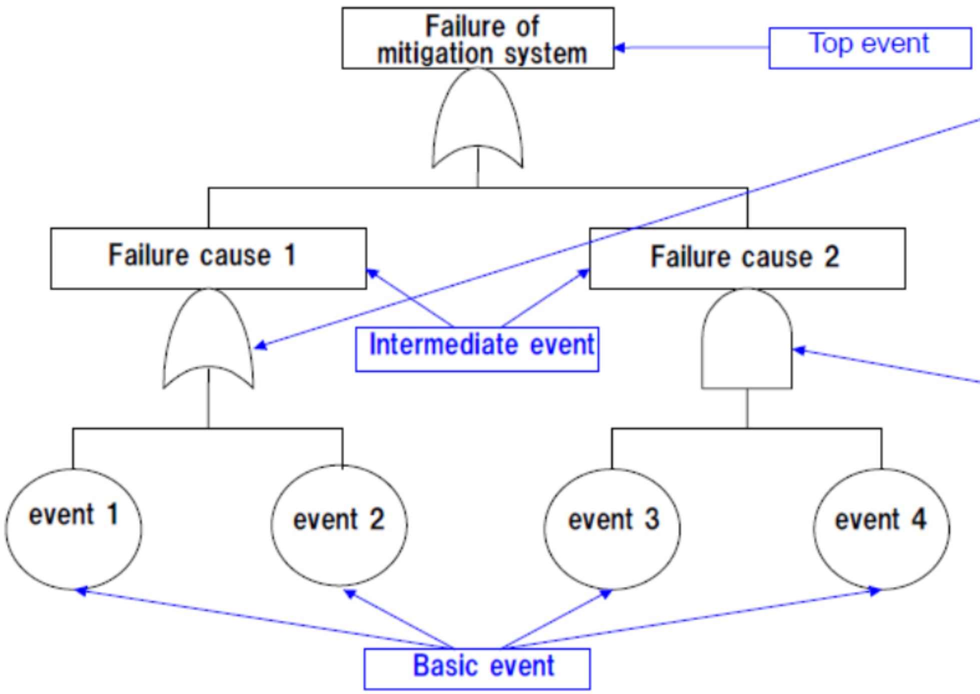
System Analysis (Fault Tree Analysis)

- Fault Tree Analysis (FTA) is used to identify how a system, component, function or operation may fail
- Minimal Cut Set (MCS) is the minimum combination of events, which causes a system to fail.
- Use Laws of boolean algebra and logical

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

Symbol	Name of the Symbol	Description
	Basic Event	A lower most event that can not be further developed
	An Event/Fault	This can be a intermediate event (or) a top event. They are a result logical combination of lower level events.
	OR Gate	Either one of the bottom event results in occurrence of the top event.
	AND Gate	For the top event to occur all the bottom events should occur.
	Undeveloped Event	An event which has scope for further development but not done usually because of insufficient data.
	External Event	An event external to the system which can cause failure.
	Inhibit Gate	The top event occurs only if the bottom event occurs and the inhibit condition is true.

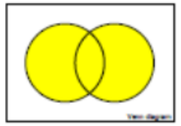
System Analysis (Fault Tree Analysis)



OR gate

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

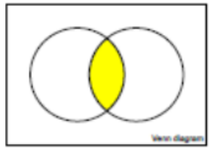
It means logical addition of two events:
(occurrence probability of event 1) +
(occurrence probability of event 2).



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).



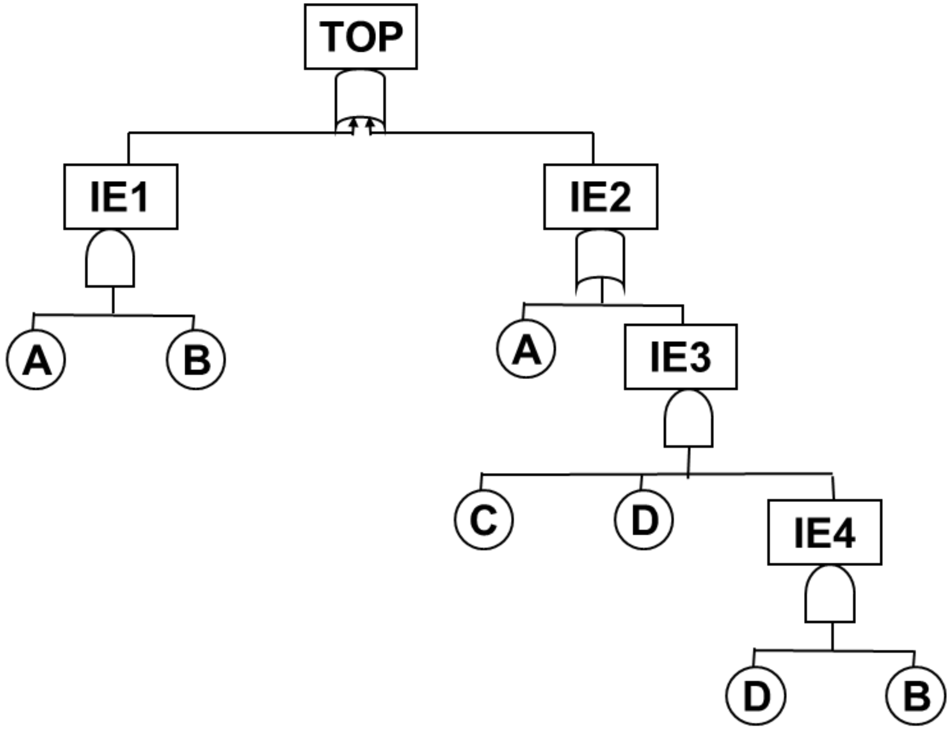
This fault tree is expressed in a formula as follows:

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

System Analysis (Fault Tree Analysis)

Boolean Algebra Reduction Example:

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



So the minimal cut sets are:
CS1 = A
CS2 = B.C.D
meaning TOP event occurs if
either A occurs OR (B.C.D) occurs.

System Analysis (Fault Tree Analysis)

Calculate the unavailability of simplified core injection system shown in Fig. 1 and Table 1:

- The system takes water from infinitely large tank with two parallel motor operated pumps (MOPs) and injects water into the reactor.
- One out of two motor operated pumps (MOPs) is sufficient to cool the core.
- Mission time: 24 hours.

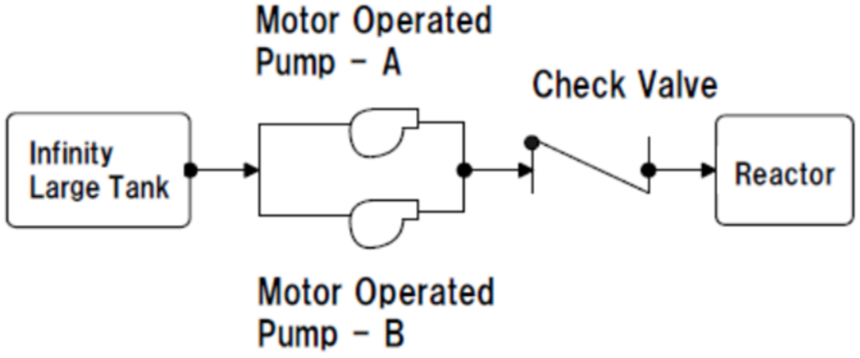


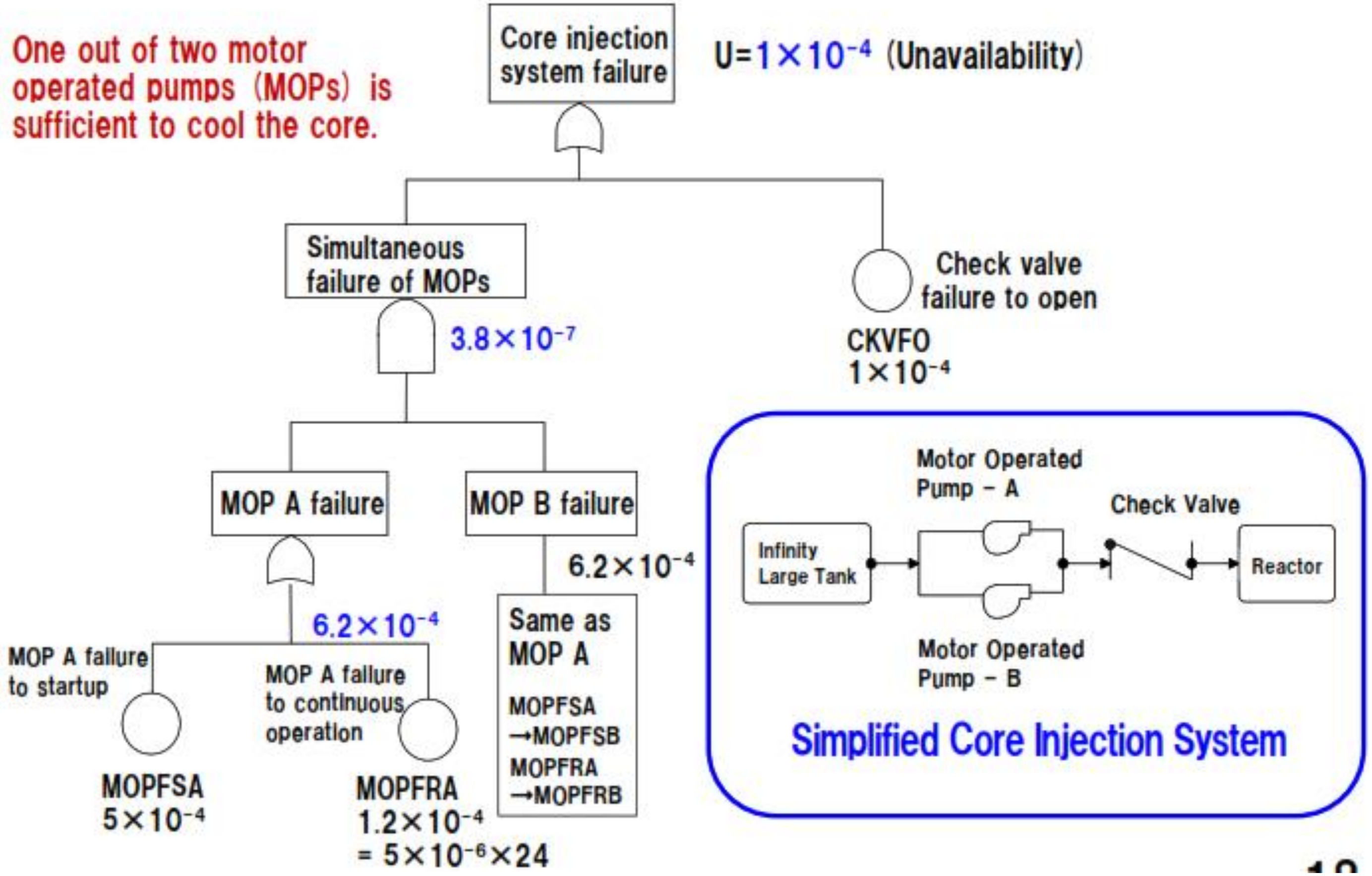
Fig. 1. simplified Core Injection System

Table 1. Component Failure Data

Component	Failure Mode	Failure data (mean)
Motor Operated Pump (MOP)	Failure to startup (MOPFS) Failure to continuous operation (MOPFR)	5E-4/d 5E-6/h
Check Valve	Failure to open (CKVFO)	1E-4/d

Total component unavailability during mission time for MOPs is
UMOP= Failure to startup + (Failure to continuous operation x Mission time)

System Analysis (Fault Tree Analysis)



Database

- Data used in PSA
  - ✓ Initiating event frequencies
  - ✓ Component failure probabilities
  - ✓ Component outage frequencies and durations
  - ✓ Human error probabilities
  - ✓ CCF (Common Cause Failure) parameters
- Generic data & Plant-Specific data
  - ✓ Generic data: existing database world
  - ✓ Plant-specific data: data from operating experiences of specific plant
  - ✓ In general, generic data are compensated by plant-specific data using Bayesian inference technique
- Reliability data of component
  - ✓ Failure rate to run
  - ✓ Failure upon demand or failure to start
  - ✓ Failure rate during stand-by
  - ✓ Repair rate or repair time
  - ✓ Unavailability for maintenance or testing

Quantification

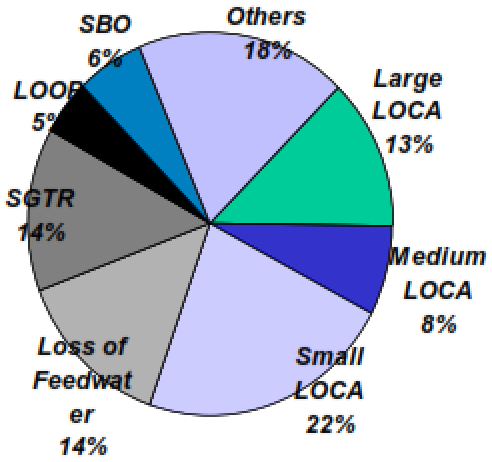
- CDF (point estimate & uncertainty)
- Contributions to the CDF (each group of initiating events)
- Minimal cutsets, minimal cutset frequencies, scenario frequencies
- Results of sensitivity and uncertainty analysis
- Importance measures
- Frequencies of plant damage states (interface between level 1 PSA and level 2 PSA)

Quantification of the Level 1 PSA

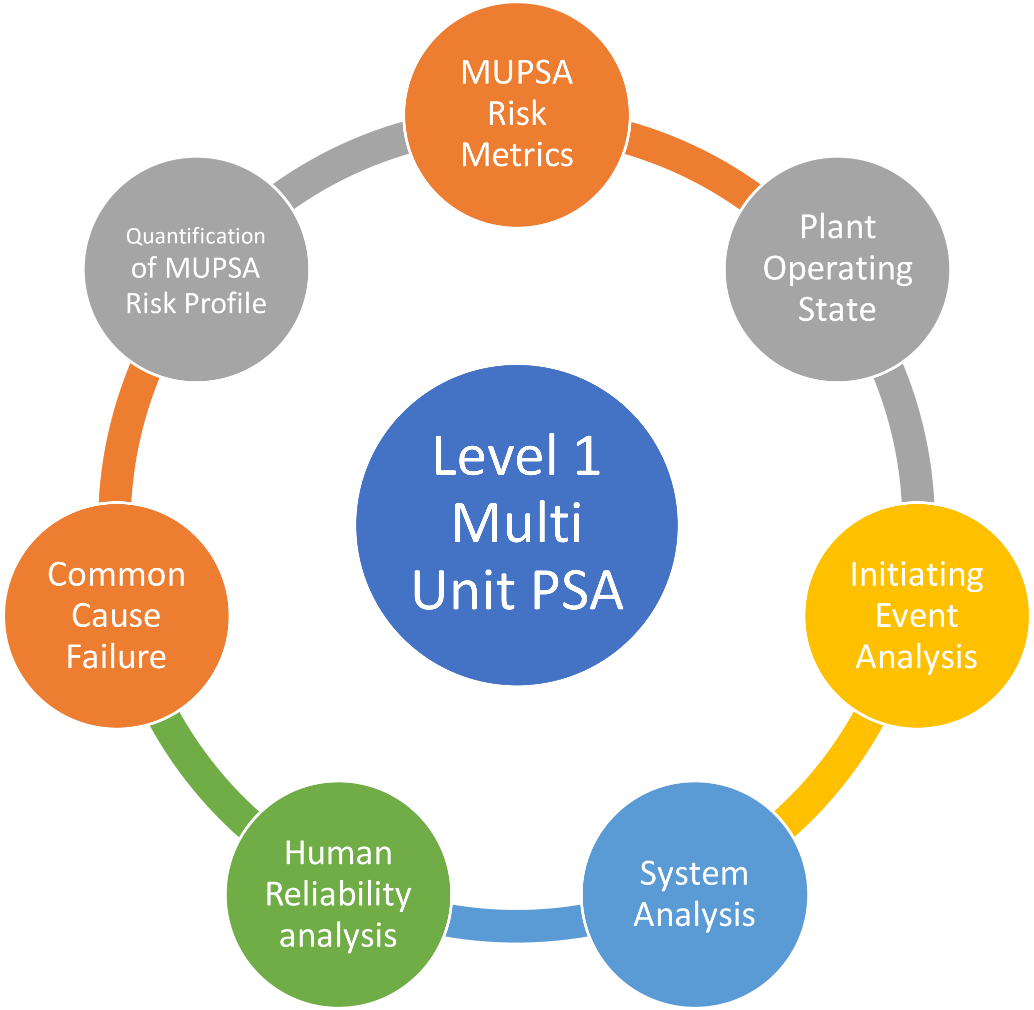
Level 1 PSA Result

Contribution to CDF

Initiating Events	CDF	
	/yr	%
Large LOCA	1.05E-06	12.7
Medium LOCA	6.33E-07	7.7
Small LOCA	1.86E-06	22.5
Steam Generator Tube Rupture	1.14E-06	13.8
Large Secondary Side Break	1.46E-07	1.8
Loss of Feedwater	1.14E-06	13.8
Loss of Condenser Vacuum	2.53E-08	0.3
Loss of a CCW Train	1.25E-07	1.5
Loss of a 4.16KV Bus	5.48E-10	<0.1
Loss of a 125V DC Bus	3.17E-07	3.8
Loss of Off-site Power	4.00E-07	4.8
Station Blackout	4.80E-07	5.8
General Transients	3.59E-07	4.4
Anticipated Transient Without Sc	3.15E-07	3.8
Interfacing Systems LOCA	1.77E-09	<0.1
Reactor Vessel Rupture	2.66E-07	3.2
TOTAL	**8.25E-06**	**100**



Level 1 Multi Unit PSA (MUPSA)



Multi-unit PSA

MUPSA Risk Metrics

(Frequency per site-year of an accident)

- Single Unit CDF → Core damage to only one reactor on a multi-unit site
- Multi Unit CDF → core damage to two or more reactor on a multi-unit site
- Site CDF → core damage to one or more reactors on a multi-unit site
- Multi-Source Fuel Damage Frequency → fuel damage in two or more sources (e.g reactor core, spent fuel pool) on a multi-unit site


Thank
You