*Joint KINS-IAEA-ANNuR/ANSN/FNRBA
BPTC Course on Nuclear Safety,
19 ~ 30 September 2022, KINS, Korea*

Safety Analysis:
Deterministic safety analysis

Manwoong KIM

m.kim@kins.re.kr

Korea Institute of Nuclear Safety

CONTENTS

1. Needs for Safety Analysis
2. Introduction of Safety Analysis: DSA
   (1) Purpose
   (2) Requirements
   (3) Analysis in the Plat Sates
3. Safety analysis approaches
   (1) Classification of Initiating Events
   (2) Overview of Deterministic Analysis
   (3) Typical Safety Criteria for DBAs
   (4) Safety Analysis Codes
   (5) Verification and Validation of Codes
   (6) LOCA and Non-LOCA Analysis
   (7) Regulatory Auditing Calculation
4. Application of deterministic safety analysis
5. Summary

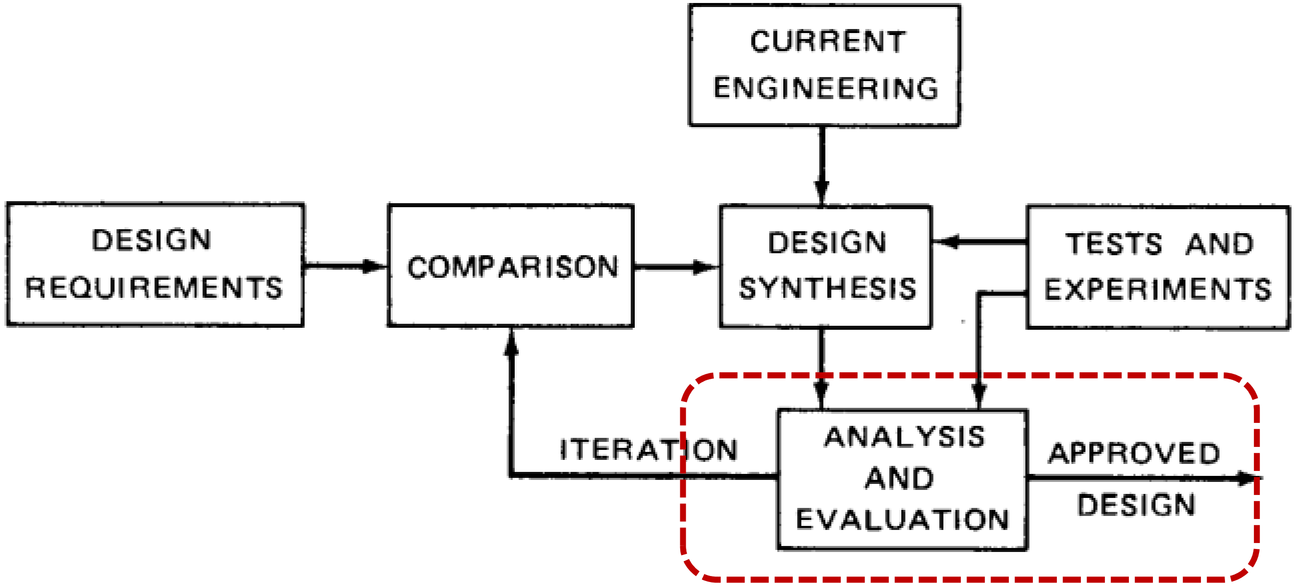
1. Needs for Safety Analysis

1. Needs for Safety Analysis

TID-26241 Nuclear Power Plant Design Analysis

- Two other types of effects are of major importance to the designer:
  - The power distribution may vary with time as the fuel is depleted and also as the result of different fuel reloading strategies.
  - The thermal consequences of start-up, shutdown, and inadvertent operating situations must be considered in the safety analysis as well as the detailed effects of various postulated accidents.

Design feedback and iteration process



1. Needs for Safety Analysis (cont'd)

- **Safety analyses** are analytical studies aimed at demonstrating that safety requirements are met.
  - The address all possible operating conditions of a nuclear power plant, for various postulated initiating events.
- **In the design process,** safety analyses are used to:
  - confirm that the design meets all design and safety requirements,
  - derive operational limits and conditions,
  - establish and validate possible accident conditions and
  - confirm that safety criteria which have been established to limit the risks posed by the nuclear power plant are met.
- The results of the safety analysis ensure that, with a high level of confidence, the plant will perform as designed and that it will meet all the design acceptance criteria at commissioning and throughout the life of the plant

1. Needs for Safety Analysis (cont'd)

- The **IAEA Safety Glossary** acknowledges the interchangeable use of both terms but specifies that "when the distinction is important, safety analysis should be used for the study of safety, and safety assessment for the evaluation of safety".
- We will refer to these types of analyses as Deterministic Safety Analysis or Deterministic Safety assessment (DSA) interchangeably.
- They are an essential element of a plant design as well as of the licensing process.

Safety Assessment for Facilities

Safety Assessment

Safety Analysis

Two complementary methods

Deterministic Safety Analysis (DSA)

Predicts the response to postulated events with predetermined assumptions; checks fulfilment of acceptance criteria

Probabilistic Safety Analysis (PSA)

Combines the likelihood of initiating events, potential scenarios and their consequences into estimation of CDF, source term or overall risk

Safety Approach

- Defence in depth
- Safety Margin
- Multiple barriers

Safety Features

- Site characteristics
- Engineering aspects
- Safety function
- Human factors
- Long-term safety
- Radiation protection

1. Needs for Safety Analysis (cont'd)

- It is an international requirement that **both deterministic and probabilistic safety analysis** shall be used in a safety analysis of the design of nuclear power plants.
- This is to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.
- Thus requirement s adopted in almost all national legislations.
- Such analyses are an integral part of any licensing process and are part of the Final Safety Analysis Report (FSAR) for every nuclear power plant.

1. Needs for Safety Analysis (cont'd)

- Both types of safety analysis support **the safe operation of the plant** by serving as an important tool in developing and confirming
  - plant protection,
  - control system set points,
  - control parameters.
- They are also used to establish and validate:
  - the plant's operating specifications and limits (technical specifications),
  - normal operating procedures,
  - maintenance and inspection requirements,
  - emergency operating procedures (EOPs), and
  - severe accident management guidelines (SAMGs).

2. Introduction of Safety Analysis: DSA

- Purpose
- Requirements
- Analysis in the plant states

(2-1) Purpose of safety analyses

- The Safety Fundamentals publication, **Fundamental Safety Principles**, establishes the principles for ensuring the protection of workers, the public and the environment, now and in the future, from harmful effects of ionizing radiation.
- Safety analyses are undertaken as a means of evaluating compliance with safety principles and safety requirements for all nuclear facilities.
- They are to be carried out and documented by the organization responsible for operating the facility, are to be independently verified and are to be submitted to the regulatory body as part of the licensing or authorization process.

What deterministic safety analyses provide

- **Deterministic safety analysis** mainly provides:
  - Establishment and confirmation of the deign basis for all items important to safety;
  - Characterization of the postulated initiating events that are appropriate for the site and the design of the plant;
  - Analysis and evaluation of event sequences that result from postulated initiating events;
  - Comparison of the results of the analysis with dose limits and acceptance limits, and with design limits;
  - Demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by automatic actuation of safety systems;
  - Demonstration that the management of design extension conditions is possible by actuation of plant systems in combination with prescribed operator actions.

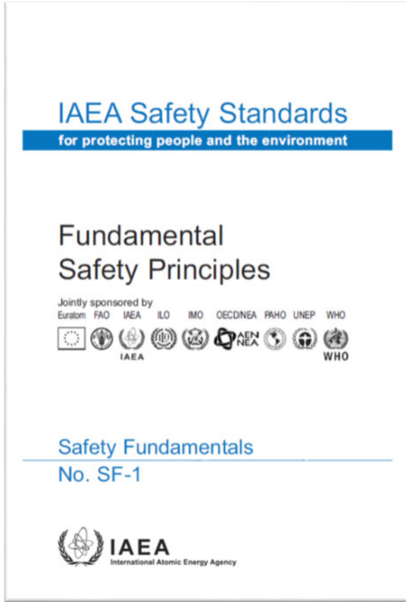
(2-2) Requirements

1. Safety Assessment for Facilities and Activities, GSR Part 4
2. Safety of Nuclear Power Plants: Design, SSR-2/1
3. Deterministic Safety Analysis for Nuclear Power Plants, SSG-2
4. Development and Application of Level 1 PSA for NPPs, SSG-3
5. Development and Application of Level 2 PSA for NPPs, SSG-4

(2-2) Requirements

SF1 Fundamental Safety Principles

- The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation.
- To ensure that facilities are operated and activities conducted so as to achieve the highest standards of safety that can reasonably be achieved, measures have to be taken:
  - To restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation;
  - To mitigate the consequences of such events if they were to occur;
  - To control the radiation exposure of people and the release of radioactive material to the environment.



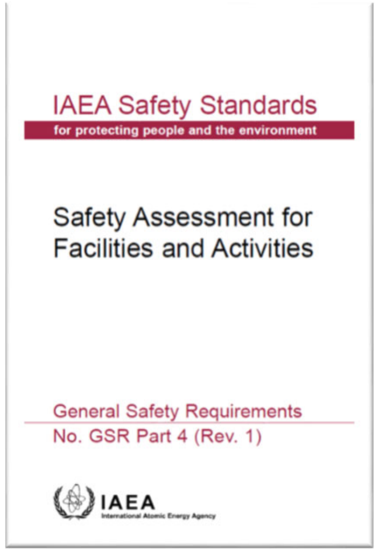
Ref. : IAEA Safety Standard Series No. SF-1

(2-2) Requirements (cont'd)

GSR Part 4 Safety Assessment for Facilities and Activities

Requirement 4: Purpose of the safety assessment

- The primary purposes of the safety assessment shall be to determine whether an adequate level of safety has been achieved for a facility or activity and whether the basic safety objectives and safety criteria established by the designer, the operating organization and the regulatory body, in compliance with the requirements for protection and safety as established in Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, have been fulfilled.



(2-2) Requirements (cont'd)

GSR Part 4 Safety Assessment

Requirement 3: Responsibility for the safety assessment

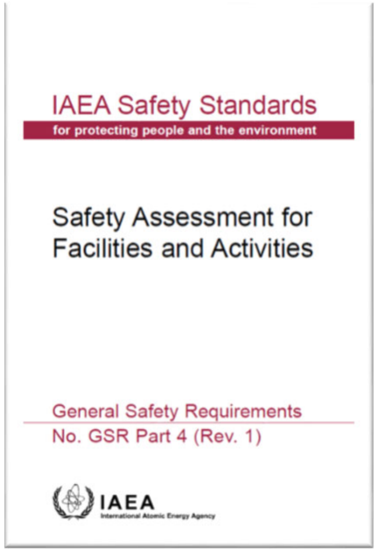
The responsibility for carrying out the safety assessment shall rest with the responsible legal person; that is, the person or organization responsible for the facility or activity.

- Generally, the person or organization authorized (licensed) to operate the facility.
- The operating organization shall be responsible for the safety assessment.

(2-2) Requirements (cont'd)

GSR Part 4 Safety Assessment

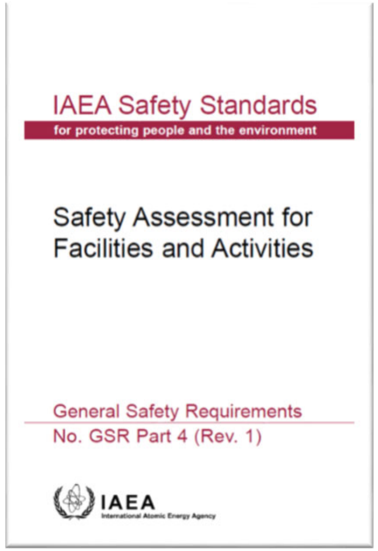
- the deterministic safety analysis shall include:
  - Confirmation that operational limits and conditions are in compliance with the design assumptions and intent for the normal operation of the plant;
  - Characterization of the PIEs that are appropriate for the plant design and its location;
  - Analysis and evaluation of event sequences that result from PIEs;
  - Comparison of the results of the analysis with radiological acceptance criteria and design limits;
  - Establishment and confirmation of the design basis;
  - Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by automatic safety system response in combination with prescribed operator actions.



(2-2) Requirements (cont'd)

GSR Part 4 Safety Assessment

- The applicability of the analytical assumptions, methods and degree of conservatism used shall be verified
- The safety analysis of the plant design shall be
  - updated in the light of
    - significant changes in plant configuration,
    - operational experience,
    - improvements in technical knowledge or
    - understanding of physical phenomena
    - consistent with the current or "as-built



(2-2) Requirements (cont’d)

SSR 2/1 Design of NPPs

Safety Analysis Definitions in SSR-2/1

- “A safety analysis of the plant design, applying methods of Deterministic and Probabilistic analysis, shall be provided which establishes and confirms the design basis for the items important to safety and demonstrates that the overall plant design is capable of meeting the prescribed and acceptable limits for radiation doses and releases for each plant condition category, and that defense in depth has been achieved.”

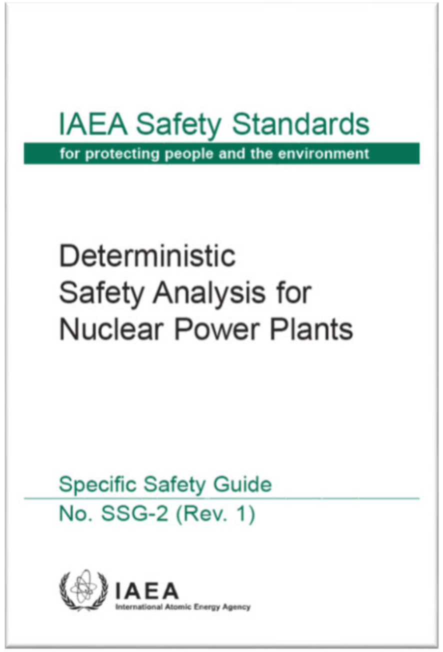
(2-2) Requirements (cont'd)

IAEA SSG-2 Deterministic Safety Analysis for NPPs

- The objective is to provide recommendations and guidance on performing deterministic safety analysis for designers, operators, regulators and technical support organizations. It also provides recommendations on the use of deterministic safety analysis in:

  (a) Demonstrating or assessing compliance with regulatory requirements;

  (b) Identifying possible enhancements of safety and reliability;



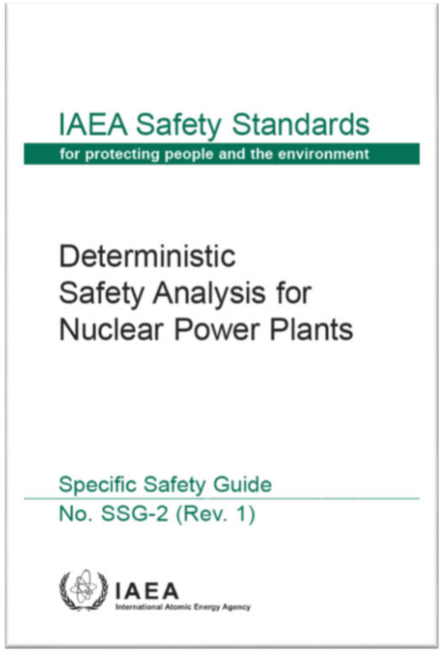
(2-2) Requirements (cont'd)

IAEA SSG-2 Deterministic Safety Analysis for NPPs

- The objective is to provide recommendations and guidance on performing deterministic safety analysis for designers, operators, regulators and technical support organizations. It also provides recommendations on the use of deterministic safety analysis in:

  (a) Demonstrating or assessing compliance with regulatory requirements;

  (b) Identifying possible enhancements of safety and reliability;



(2-3) Analysis in the Plat Sates

- **Plant states** for nuclear power plants are specified in SSR 2/1.
- They are divided into operational states and accident conditions.
- **Operational states** include normal operation as well as anticipated operational occurrences.
- **Accident conditions** include accidents that are within the design basis and design extension conditions.
- In the past, design extension conditions were termed the Beyond design basis accident conditions.
- Design extension conditions include severe accident conditions, which are characterized as states with significant core degradation.

(2-3) Analysis in the Plat Sates (cont'd)

Table 2.1: Plant states.

Operational states		Accident conditions	
Normal operation	Anticipated operational occurrences	Design basis accidents	Design extension conditions

(2-3) Analysis in the Plat Sates (cont'd)

Normal operation is defined as operation within specified operational limits and conditions.

- Deterministic analysis is applied to normal operation with the aim of showing that normal operation can be carried out safely including;
  - acceptable doses to workers and
  - the public, and
  - acceptable planned releases of radioactive material.
- The analysis should demonstrate that, during normal operation, plant parameters remain within acceptable limits.
  - to establish the necessary settings for the safety and control systems,
  - writing the operating procedures for the staff and
  - defining the constraints that must not be exceeded when the plant is operating.

(2-3) Analysis in the Plat Sates (cont'd)

An **anticipated operational occurrence (AOO)** is an operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility.

- Because of appropriate design provisions, it does not cause any significant damage to items that are important to safety or lead to accident conditions.
- Such events have the potential to challenge the safety of the plant but, because of appropriate design provisions, they do not lead to any significant fuel damage, and, therefore, no offsite consequences.

(2-3) Analysis in the Plat Sates (cont'd)

- Deterministic analysis is carried out to assess the **response of the control and safety systems** and to show the robust nature of the design.
- Generally, the analysis should consider uncertainties in modelling and data to demonstrate that there are **margins to safety limits**, even with conservative assumptions.

Anticipated operational occurrences typically include loss of normal off-sit e power, turbine trip, failure of control equipment and loss of power to the main coolant pump.

(2-3) Analysis in the Plat Sates (cont'd)

Design basis accidents (DBAs) are accident conditions against which a facility is designed according to established design criteria.

- In DBAs, the damage to the fuel and the release of radioactive material are kept within authorized limits.
- DBAs are not expected to occur in the life of the plant, but are of sufficiently high probability that they are reasonably considered as tests of the safety design of the plant.
- A chance of their appearance is judged to be greater than 1 % over the lifetime of the plant, even though modern designs have reduced their frequency below this value.

(2-3) Analysis in the Plat Sates (cont'd)

DECs are defined as accident conditions that are not considered for design basis accidents, but are considered in the design process of the facility in accordance with best estimate methodology.

- For DECs, releases of radioactive material are kept within acceptable limits.
- Such accidents are of extremely low frequency, so they have not historically been considered to be within the design basis.
- **Some recent designs** have included features to mitigate the consequences of severe accidents.
- The intention is to minimise or practically eliminate the need to apply counter measures to protect members of the public outside the site.

(2-3) Analysis in the Plat Sates (cont'd)

- The analysis of DECs is conducted using best estimate codes and data with an analysis of the uncertainties, which can be considerable.
- In contrast to the analyses of normal operation, AOOs and DBAs, where well-defined acceptance criteria are available, **no such generally accepted deterministic criteria** are available for severe accidents (SAs).
- **The principal role** of the deterministic analysis of DECs and SAs is to define those scenarios that will progress to SAs, and to support the probabilistic analyses of the risk associated with SAs.

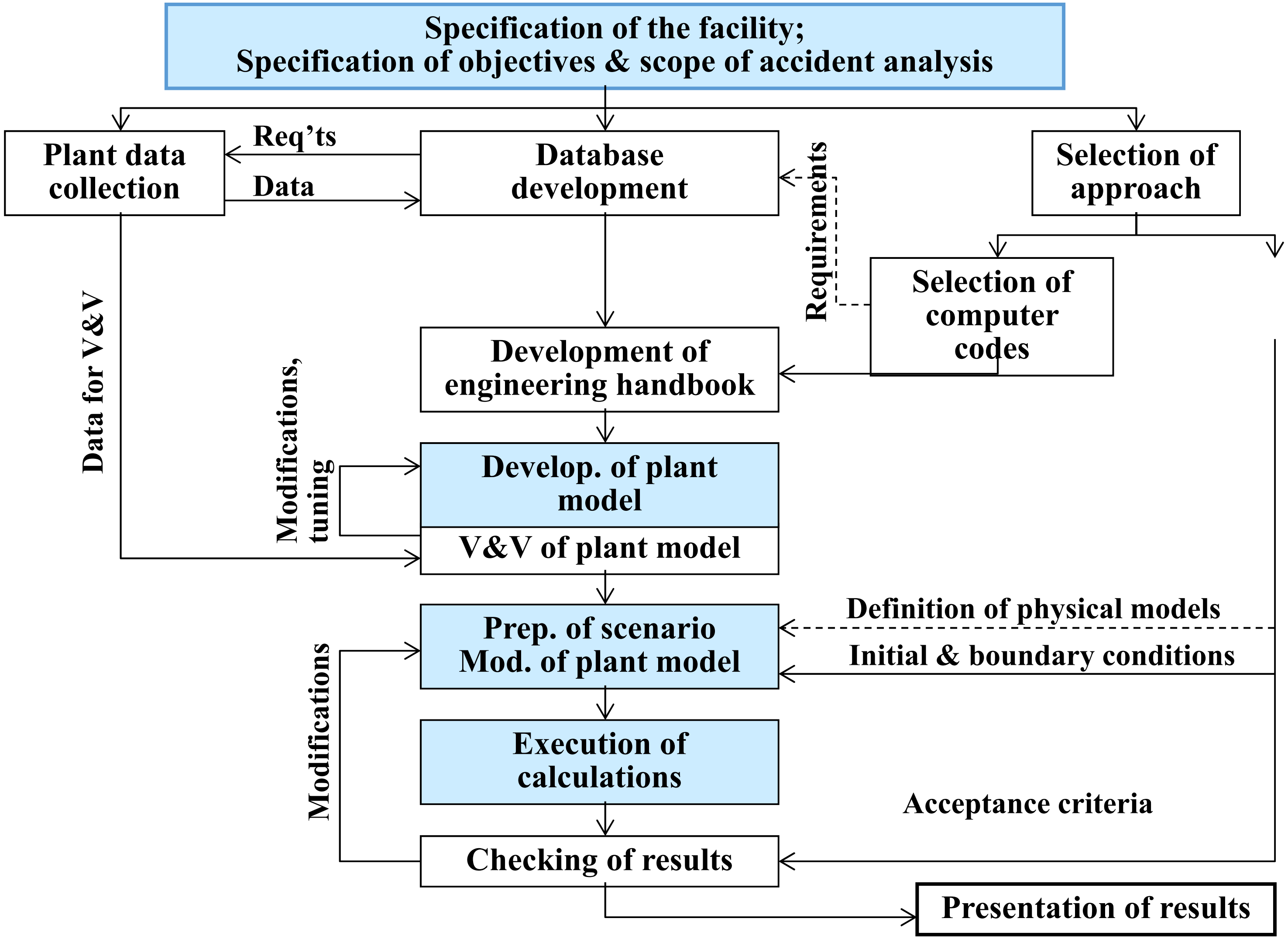
3. Safety analysis approaches

- Classification of Initiating Events
- Overview of Deterministic Analysis
- Typical Safety Criteria for DBAs
- Accident Analysis Codes
- LOCA and Non-LOCA Analysis

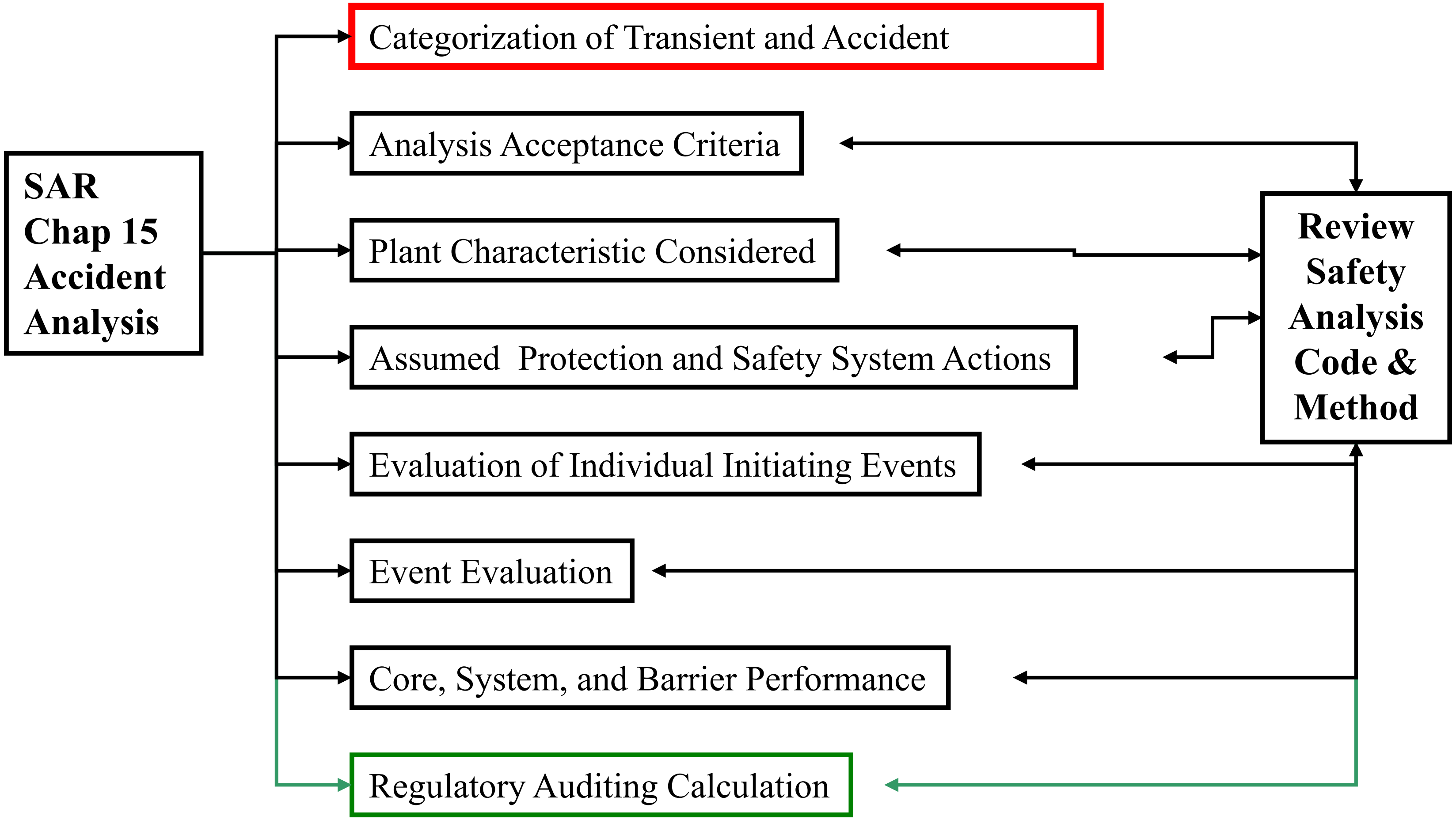
Procedure for Safety Analysis

- Identify & categorize initiating events
- Establish acceptance criteria
- Establish analysis methods & codes
- Perform analysis
- Compare results with relevant acceptance criteria

Basic Steps in the Safety Analysis Procedure



Regulatory Review Process



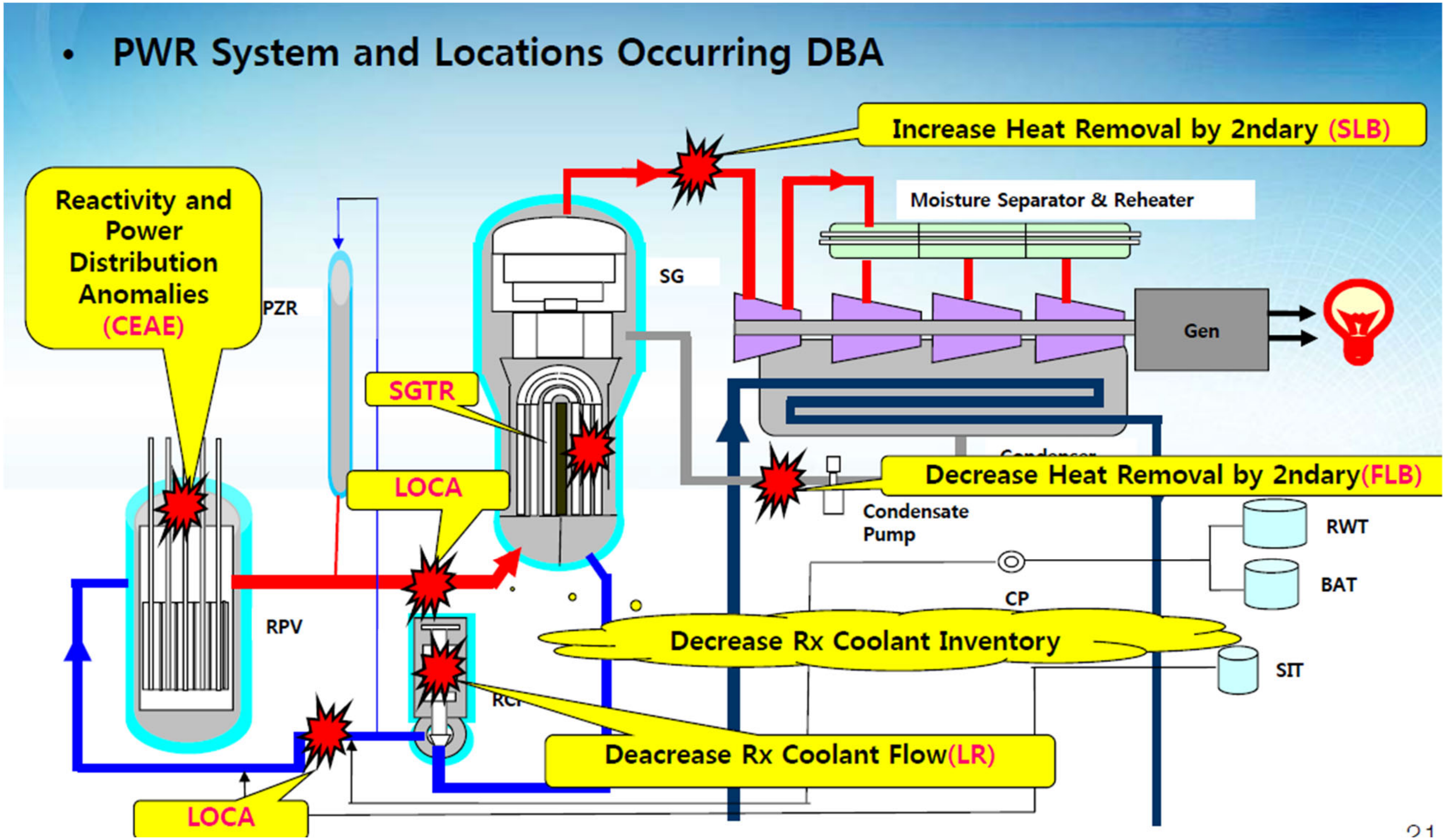
(3-1) Classification of Initiating Events

- Increase in heat removal by the secondary side
- Decrease in heat removal by the secondary side
- Decrease in flow rate in the reactor coolant system
- Increase in flow rate in the reactor coolant system
- Anomalies in distribution of reactivity and power
- Increase in reactor coolant inventory
- Decrease in reactor coolant inventory
- Radioactive release from a subsystem or

Fundamental Safety Functions

- Control of Reactivity
- Removal of heat from the nuclear fuel
- Confinement of radioactive materials

(3-1) Classification of Initiating Events (cont'd)



Examples of Initiating Events

- **Increase in heat removal by the secondary side**
  - Decrease in feedwater temperature
  - Increase in feedwater flow
  - Increase in steam flow
  - Inadvertent opening of a steam generator relief or safety valve
  - Steam system piping failure inside and outside the containment
- **Decrease in heat removal by the secondary side**
  - Loss of external load
  - Turbine trip
  - Loss of condenser vacuum (LOCV)
  - Closure of main steam isolation valve
  - Loss of nonemergency ac power to the station auxiliaries
  - Loss of normal feedwater flow
  - Feedwater system pipe break inside and outside the containment

Examples of Initiating Events (cont'd)

- **Reactivity and Power Distribution Anom**alies
  - Uncontrolled Control Element Assembly Withdrawal from a Subcritical or Low-Power Startup Condition
  - Uncontrolled Control Element Assembly Withdrawal at Power
  - Control Element Assembly Misoperation
  - Startup of an Inactive Reactor Coolant Pump
  - Inadvertent Decrease in Boron Concentration in the Reactor Coolant System
  - Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position
  - Spectrum of CEA Ejection Accidents

Examples of Initiating Events (cont'd)

- **Decrease in Reactor Coolant Inventory**
  - Inadvertent opening of a pressurizer pressure relief valve
  - Failure of small lines carrying primary coolant outside the containment
  - Steam generator tube failure
  - Loss-of-coolant accidents (LOCAs) resulting from a spectrum of postulated piping breaks within the reactor coolant pressure boundary (RCPB)

Grouping by Frequency of Occurrences (IAEA)

Occurrence (per RY)	Characteristics		Terminology	Acceptance Criteria
$10^{-2} \sim 1$ (Expected during plant life)	Expected	Anticipated operational occurrences	Anticipated transients; transients; frequent faults; incident of moderate freq.; upset/ abnormal cond.	No additional fuel damage
$10^{-4} \sim 10^{-2}$ (Chance greater than 1% over the plant life)	Possible	Design Basis Accidents (DBAs)	Infrequent incidents; infrequent faults; limiting faults; emergency conditions	No radiological impact at all or no radiological impact outside the exclusion area
$10^{-6} \sim 10^{-4}$ (Chance less than 1% over the plant life)	Unlikely	Beyond Design Basis Accidents (BDBAs)	Faulted conditions	Radiological consequences outside exclusion area within limits
$< 10^{-6}$ (Very unlikely to occur during plant life)	Remote	Severe Accidents	Faulted conditions	Emergency response needed

Event Classification in USA/KOREA

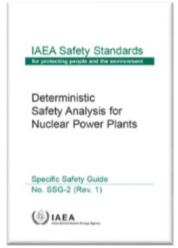
<table>
<tr><th colspan="3">ANS</th><th colspan="2">USNRC</th></tr>
<tr><th>Freq. per RY</th><th>ANSI/ANS-51.1 (1983)</th><th>ANS N18.2 (1973)</th><th>GR 1.70 (Rev. 2)</th><th>10 CFR</th></tr>
<tr><td>Normal Operation</td><td>Plant Condition 1 (PC-1)</td><td>Condition I</td><td>Normal operation & operational transients</td><td>Normal operation</td></tr>
<tr><td>> 10^{-1}</td><td>Plant Condition 2 (PC-2)</td><td>Condition II</td><td>Incidents of moderate frequency</td><td rowspan="2">Anticipated operational occurrences (AOOs)</td></tr>
<tr><td>$10^{-2} \sim 10^{-1}$</td><td>Plant Condition 3 (PC-3)</td><td>Condition III</td><td>Infrequent incidents</td></tr>
<tr><td>$10^{-4} \sim 10^{-2}$</td><td>Plant Condition 4 (PC-4)</td><td rowspan="3">Condition IV</td><td rowspan="3">Limiting faults</td><td rowspan="3">Accidents</td></tr>
<tr><td>$10^{-6} \sim 10^{-4}$</td><td>Plant Condition 5 (PC-5)</td></tr>
<tr><td>< 10^{-6}</td><td>Not considered</td></tr>
</table>

(3-2) Overview of Deterministic Analysis

- **Major Steps in Deterministic Analysis**
  - Identification & categorization of events considered in the design basis
  - Analysis of enveloping scenarios
  - Evaluation of consequences and comparison with acceptance criteria
- **Approaches**
  - Conservative Analysis
    - Direct comparison of analysis results with acceptance criteria

    (eg.) PCTallowable > PCTconservative > PCTactual
  - Best-Estimate analysis + Uncertainty
    - Comparison of analysis results plus uncertainty with acceptance criteria

    (eg.) PCTallowable > PCTBE + PCTuncert. > PCTactual > PCTBE - PCTuncert.



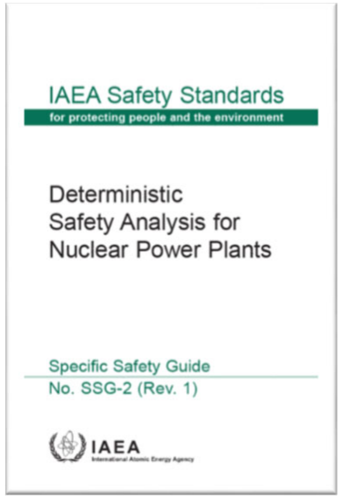
Terminology [IAEA]

- **Conservative model:** a model that provides a pessimistic estimate for a physical process in relation to a specific acceptance criterion
- **Conservative code:** a combination of all the models necessary to provide a pessimistic bound to the processes relating to the specified acceptance criteria
- Best estimate model: a model that provides a realistic estimate for a physical process to the degree nsistent with the currently available data and knowledge of the phenomena concerned
- Best estimate code: a combination of the best estimate models necessary to provide a realistic estimate of the overall response of the plant during an accident. The BE code is free of deliberate pessimism and contains sufficiently detailed models and correlations to describe the relevant processes for the transients that the code is designed to model
- Conservative data: plant parameters, initial plant conditions and assumptions about availability of equipment and accident sequences chosen to give a pessimistic result, when used in a safety analysis code, in relation to a specified acceptance criteria
- Realistic data: plant parameters, initial plant conditions and assumptions about availability of equipment and accident sequences chosen to give a realistic (also ‘as designed’, ‘as built’, ‘as operated’) result
- Bounding data: data to provide conservative results, usually used for nuclear data that change from cycle to cycle or within a cycle

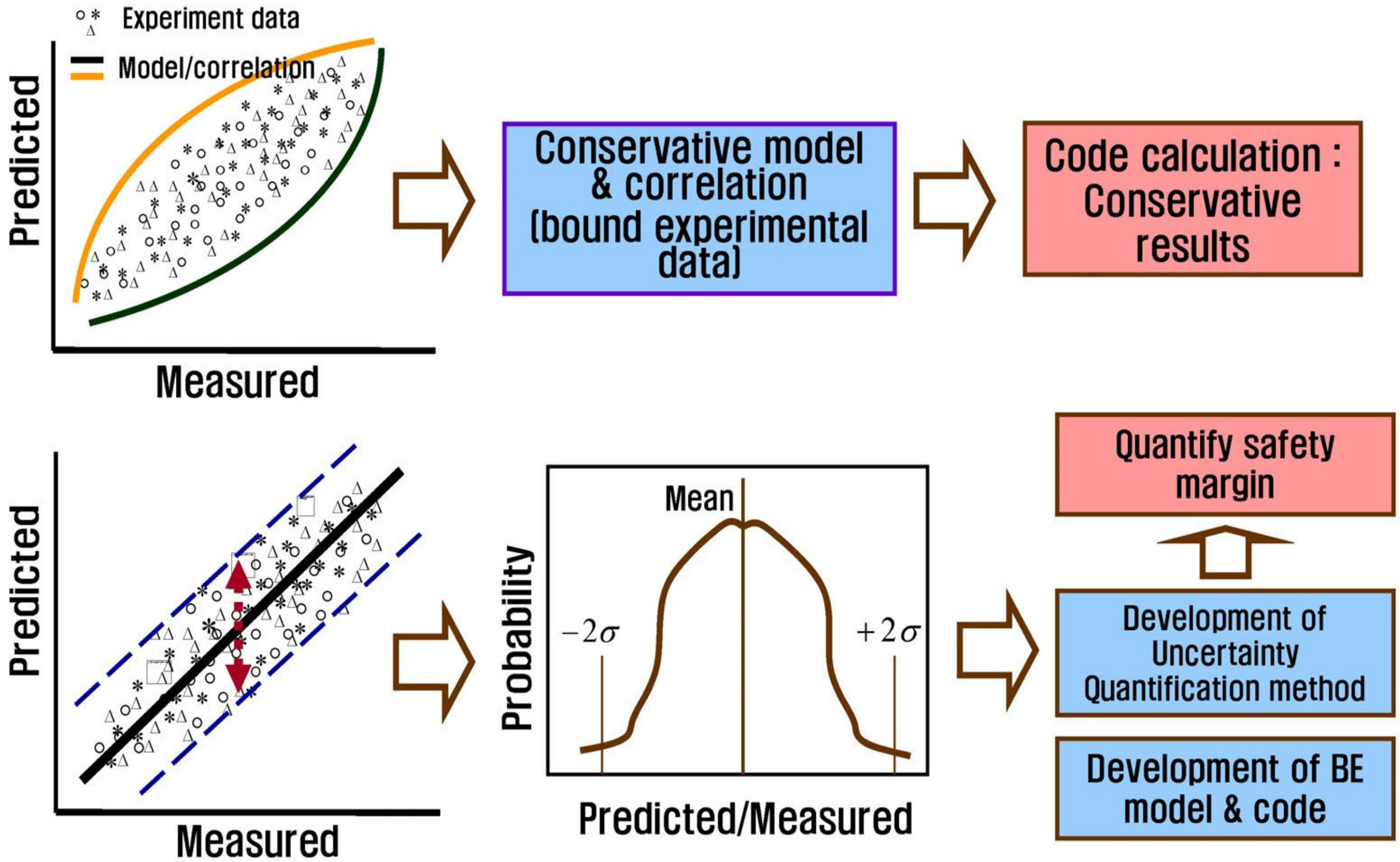
Options for performing deterministic safety analysis

Option	Computer code type	Assumptions about systems availability	Type of initial and boundary conditions
1. Conservative	Conservative	Conservative	Conservative
2. Combined	Best estimate	Conservative	Conservative
3. Best estimate plus uncertainty	Best estimate	Conservative	Best estimate Partly most unfavourable conditions
4. Realistic*	Best estimate	Best estimate	Best estimate

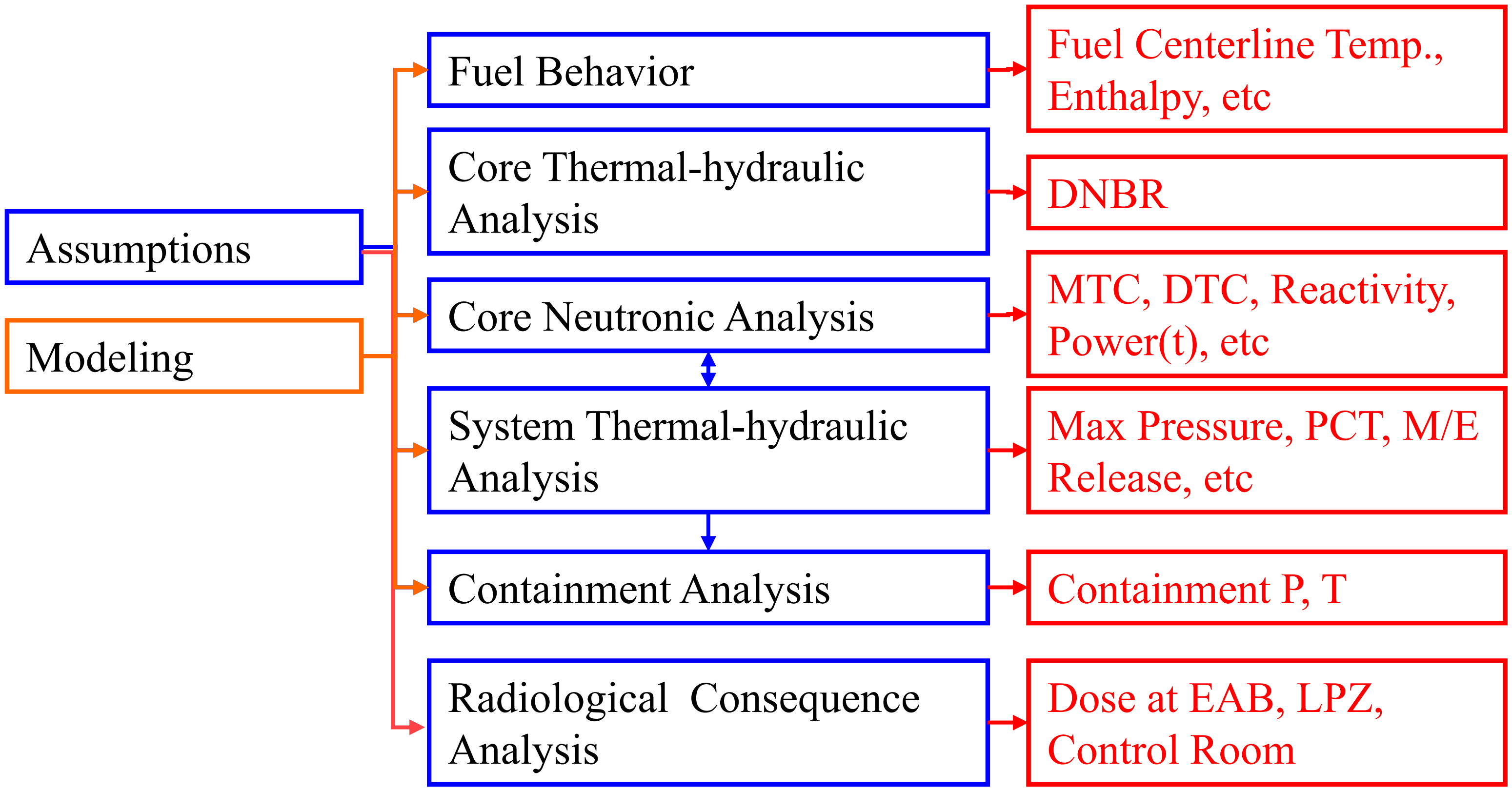
* For simplicity, the terms 'realistic approach' or 'realistic analysis' are used in this Safety Guide to mean best estimate analysis without quantification of uncertainties.



Conservative ~ Best-estimate Approach



Systematic Evaluation



(3-2) Systematic Evaluation

- **Initiating Events**
  - Limiting initial events and comparison with non-limiting one
  - (e.g.) Increase in heat removal by the secondary side
    - Decrease in feedwater temperature,
    - Increase in feedwater flow
    - Increase in steam flow (Limiting)
    - Inadvertent opening of a steam generator relief or safety valve

Systematic Evaluation

- **Event Evaluation**
  - Identification of Causes and Frequency Classification
  - Sequence of Events and Systems Operation
    - Step-by-step from initiation to finalized condition (e.g. occurrence, sensor trip, insertion of control rods, attainment of safety valve setpoint, opening/closing of safety valve, generation of containment isolation signal, containment isolation, operator action credited, etc.)
    - Extent to which normal operating plant I&C assumed and reactor protection system required
    - Credited operation of engineered safety systems
    - Use only safety-related system

Parameters

Nuclear design

- control rod worth, rod insertion time, shutdown margin
- control temperature feedback coefficients (fuel, moderator)
- power distribution (radial, axial)
- decay heat
- fission product inventory
- delayed neutron fraction

Fuel

- thermal conductivity (pellet, gap, cladding)
- gap fraction of fission product
- fuel and cladding dimension

Core thermal-hydraulics

- fuel rod heat flux
- heat transfer coefficient between cladding and coolant
- coolant flow rate
- core bypass flow rate

Parameters

- **RCS**
  - coolant pressure/temperature
  - coolant inventory (Pressurizer level, charging flow, letdown flow)
  - pressurizer safety valve open/close setpoints
  - RCP coastdown curve
  - ESF actuation delay time
- **Main steam system**
  - coolant inventory (SG water level, feedwater flow rate)
  - steam pressure/temperature
  - main steam safety valve open/close setpoints
- **Instrumentation and control system**
  - process time including delay in instrumentation and actuation

Mitigating Systems

- Reactor protection system
- Safety injection system
- Auxiliary feedwater system
- Overpressure protection system
- Main steam/feedwater isolation system
- Emergency diesel generators
- Reactor containment system

Mitigating Systems

- **Protective Actions and Safety Systems Actions**
  - Inclusion of the most limiting single failure
  - Limiting delay time for protection safety system function used (calibration error, drift, instrumentation error, etc)
- **Single Failure Criterion**
  - **A failure which results in the loss of capability of a component to perform its intended safety function(s), and any consequential failure(s) which result from it.**
  - Redundancy in safety system is essential to minimize the possibility of loss of the safety function
  - Single Failure is assumed in accident analysis
  - One control rod with maximum worth is assumed to be stuck out of the reactor core, in spite of reactor trip signal

Mitigating Systems

- **Subsequent loss of offsite power**
  - Results from a electrical grid failure, due to electrical perturbation given to the grid following trip of generator
  - Reactor trip → turbine/generator trip → instability in electric grid → loss of electric grid → loss of offsite power → RCP stops
  - Flow rate through reactor core drops down to natural circulation mode
  - Reactor coolant pumps coasts down with the help of flywheel
  - Delay time between trip of generator and loss of offsite power is a crucial factor
  - Additional margin to fuel rod integrity and peak RCS pressure

Mitigating Systems

- **Operator action**
  - Operators shall be well trained, however, shall not be considered to be perfect, due to **human error**
  - Operator action can be credited **mostly after 30 minutes** after the initiation of event
  - To apply earlier action time, justification is required by analyzing operator responses
    - **15 minutes** for boron dilution event(easy to recognize in MCR)

(3-3) Typical Safety Criteria for DBAs

- **Acceptance Criteria**
  - Defined as **limits and conditions set by a regulatory body to achieve an adequate level of safety**
  - The **individual/collective doses to workers and the public** are required to be within prescribed limits and as low as reasonably achievable in all operational states by mitigating the radiological consequences of any accident
  - The **integrity of barriers** against the release of radioactive material (fuel itself, fuel cladding, primary/secondary reactor coolant system, containment) should be maintained, depending on the plant states
  - **The capabilities of systems and operators** intended to perform a safety function, directly or indirectly, should be ensured for the accidents for which safety function is required.
  - In some designs, it is required that early large releases of radioactive material be practically excluded

(3-3) Typical Safety Criteria for DBAs (cont'd)

- Acceptance criteria should be established for the entire range of operational states and accident conditions.
- Acceptance criteria may **be related to the frequency of the event.** Events that occur frequently, such as anticipated operational occurrences, should have acceptance criteria that are more restrictive than those for less frequent events such as design basis accidents.
- Acceptance criteria should be set in terms of the variable or variables that directly govern the physical processes that challenge the integrity of a barrier. Surrogate variables can also be used as acceptance criterion that, if not exceeded, will ensure the integrity of the barrier (PCT, DNBR, Pellet Enthalpy Rise, etc.)
- Compliance with the single failure criterion should be evaluated for each safety system in the plant

Plant Conditions & Acceptance Criteria (USA, Korea)

Category	Condition I	Condition II	Condition III	Condition IV
Name	Normal operation & operational transients	Incidents of moderate frequency	Infrequent incidents	Limiting faults
Expected Frequency	Expected	Once per reactor year	Less than once during plant life	Not expected during plant life
Typical Acceptance Criteria	● Prevention of fuel failure (by avoiding CHF ● $P_{max} < 1.1\ P_{design}$		● Prevention of severe core damage ● Continuous cooling ● Radioactive release < 10% of 10CFR100 ● $P_{max} < 1.1\ P_{design}$	● Continuous cooling ● Radioactive release < 10CFR100 ● Separate criteria for LOCA
Example for PWRs	· Normal power operation · Start-up · Shutdown · Refueling	· Decrease in feedwater flow · Loss of offsite power · Turbine trip · Partial loss of coolant flow	· Total loss of coolant flow · Very small loss of coolant · Small break in steam line	· LOCA · MSLB · MFLB

(3-4) Accident Analysis Codes

- **Computer Codes for Deterministic DBA Analysis**
  - Reactor physics codes
  - Fuel behavior codes
  - Thermal-hydraulic codes
    - System codes
    - Subchannel codes
    - Computational fluid dynamics codes
  - Containment analysis codes
  - Structural analysis codes

Thermal-Hydraulic System Codes (1)

- Mainly developed for analysis of loss-of-coolant accidents
- Conservative vs. Best-Estimate Codes
  - **Conservative code:** conservative models & assumptions based on Evaluation Models (e.g. Appendix K of 10 CFR 50), fast/simple calculation
  - **BE code:** realistic & detailed modeling, uncertainty quantification
- Characteristics of Best-Estimate T/H System Codes
  - Mixed hyperbolic-elliptic system of 6 conservation equations (mass, energy and momentum for the vapor & liquid phases)
  - Constitutive laws to describe the needed boundary conditions for each of the phases, e.g. friction between the phases and the wall
  - Typically 1-D modeling; partial implementation of 3-D modeling
  - Code validation with SET and IET data bases

Thermal-Hydraulic System Codes (2)

Name	Developer	Governing Eq.	Numerical Methods	T/H Dimension
TRAC-PF1	USNRC	2C, 2M, 2E(*)	SETs	1D, 2D, 3D Catesian, Cylinder
TRAC-M	USNRC	2C, 2M, 2E	SETs, Semi-implicit	1D, 2D, 3D Catesian, Cylinder
RELAP5/MOD 3	USNRC	2C, 2M, 2E	Semi-impicit	1D
RELAP5-3D	USDOE, INEEL	2C, 2M, 2E	Semi-implicit Two-step nearly implicit	1D, 2D, 3D Catesian, Cylinder
COBRA-TF	PNL, USA	3C, 3M, 2E	Semi-implicit	3D Component Subchannel
RETRAN-03	EPRI, USA	2C, 1M, 2E	fully implicit	1D
CATHARE	CEA, France	2C, 2M, 2E	fully implicit(0D,1D) semi-implicit(3D)	0D,1D,2D,3D
ATHLET	GRS, Germany	2C, 1M, 2E 2M for DC	fully implicit semi-implicit	1D, 2D, 3D (FLUBOX)
MARS	KAERI	2C, 2M, 2E	fully implicit semi-implicit	1D, 2D, 3D

Thermal-Hydraulic System Codes (3)

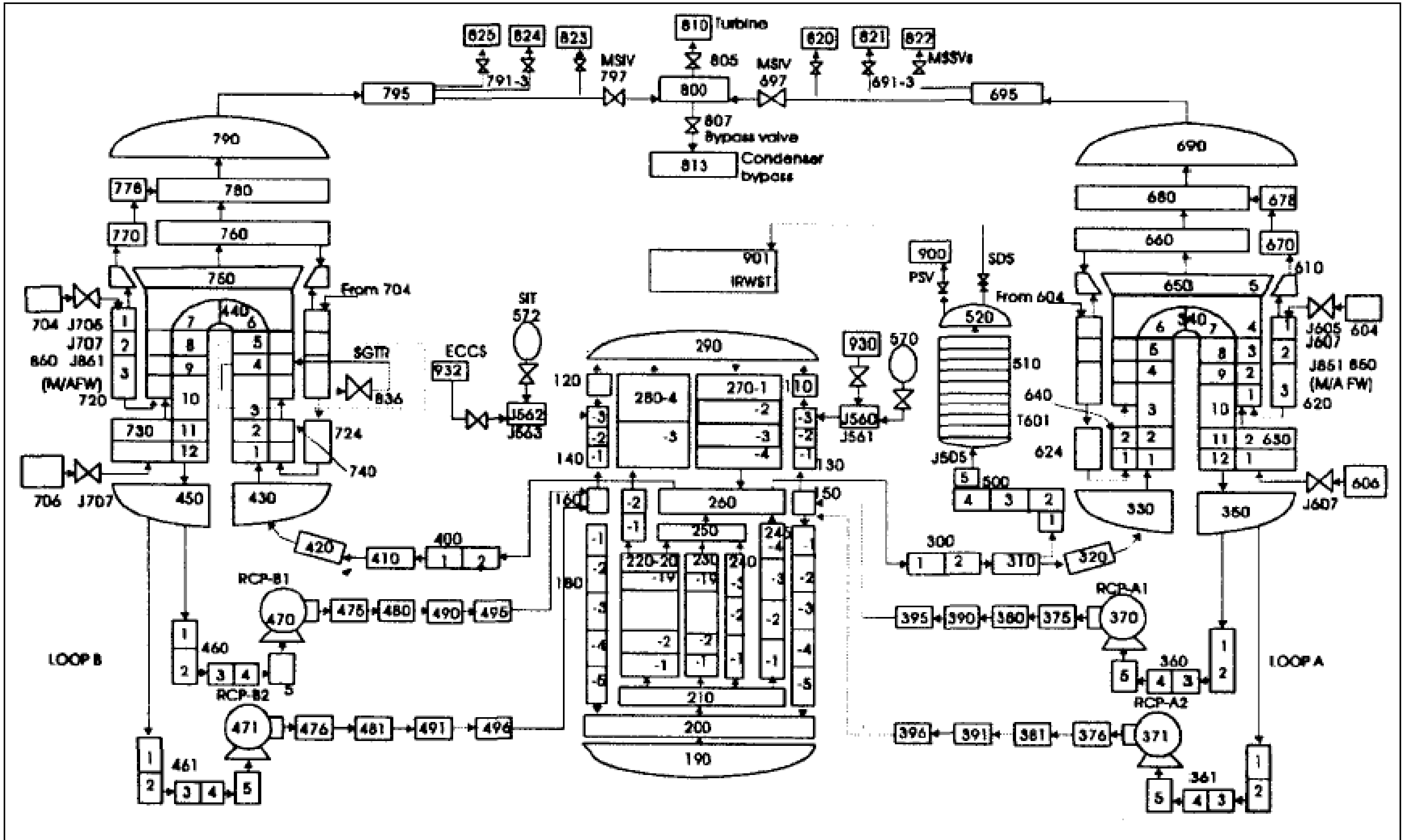


Fig. 1. Schematic Diagram of APR1400 Nodalization

(2) Containment Analysis Codes

Code	Country	Type	T/H Dimension
CONTAIN	USA	Lumped parameter	Thermal hydraulics, Hydrogen burning, Aerosol models
COCOSYS	Germany	Lumped parameter	Thermal hydraulics, Hydrogen burning, Aerosol models
GOTHIC	USA/ Germany	Lumped parameter	Thermal hydraulics, Hydrogen distribution & reduction
WAVCO	Germany	Lumped parameter & 3D CFD versions	Thermal hydraulics, Pressure differences
CONTEMPT-LT	USA	Lumped parameter	Thermal hydraulics

Other Codes

- Reactor Physics Codes: WIMS, CASMO, HELIOS, DYN3D, KIKO 3D, HEXTRAN, COCCINELLE, MASTER, . . .
- Fuel Behavior Codes: FRAPCON, FRAPT-T6, TRANSURANUS, . . .
- Structural Analysis Codes: ABAQUS, ANSYS, NASTRAN, COSMOS/M, . . .
- Mechanistic Severe Accident Codes: SCDAP/RELAP5, CATHARE/ICARE, ATHELET-CD, RELAP/SCDAPSIM, IMPACT
- Parametric Severe Accident Codes: MAAP, MELCOR, ESCADRE, THALES, MIDAS, . . .
- Subchannel Analysis Codes: COBRA-3, COBRA-IV, THINC, VIPER, MATRA, . . .

(3-5) Verification and Validation of Codes

- **1) Code verification**

  To ensure that the code design confirms to and are appropriately implemented in accordance with the design requirements

  - the numerical methods
  - transformation of the equations into a numerical scheme
  - user options are appropriately implemented in accordance with the design requirements

  To include a review of the design concept, basic logic, flow diagrams, numerical methods, algorithms and computational environment

  Checklists to be provided for review and inspection

  To demonstrate that it confirms to programming and language standards, and its logic is consistent with design specification

(3-5) Verification and Validation of Codes (cont'd)

- **2) Code Validation**
  - To provide confidence in the code ability to predict safety parameter
    - quantify the code accuracy
  - To be performed in two phases
    - development phase: by the code developer
    - independent assessment phase: independent of the developer
  - User should simulate validation tests without having any prior knowledge of the experimental results
  - The range of validity and the limitations of a code as a result of validation
  - The results of a validation to be used to determine the uncertainty of the code

(3-6) LOCA and Non-LOCA Analysis

1) Non-LOCA Analysis: Introduction

- Most Non-LOCA Scenarios Belong to Condition II (or III)
- Some Non-LOCA Scenarios Belong to Condition IV
- Acceptance Criteria Depend on Accident Frequencies
  - Max. pressure < 110% (120% for some case) of design pressure
  - Radioactive release < negligible, 10% or 100% of 10 CFR 100 limits
  - Prevention of CHF for Condition II events
  - Additional criteria according to PIEs
- Analysis Codes
  - Reactor physics (or neutronics) code for power calculation
  - System analysis code for calculation of pressure, temperature & flow
  - Subchannel analysis code for CHFR (DNBR) calculation
  - Other codes for radioactive releases, fuel behavior, etc.

(3-6) LOCA and Non-LOCA Analysis

- **Concept of CHFR Analysis**
  - Critical Heat Flux (CHF)
    - A sharp reduction of boiling heat transfer coefficient due to the replacement of liquid by vapor near the heat transfer surface
    - The CHF usually accompany a sharp increase of surface temperature → The CHF on fuel rod surface may result in fuel failure
- Critical Heat Flux Ratio (CHFR) or DNBR
  - CHFR (or DNBR) = [CHF]calculated / [Actual Heat Flux]estimated
  - Uncertainties in the estimation of both CHF and actual heat flux
  - Safety requirement: Minimum CHFR > CHFRlimit
  - CHFRlimit is determined to assure that the probability of CHF non-occurrence is above 95% at 95% confidence level (95/95 limit)
  - Assume the failure of fuel rods when Minimum CHFR > CHFR limit

(3-6) Analysis Methods for LOCA

- **Accident Scenarios**
  - Selection of conservative scenarios through sensitivity analysis
  - Large-break loss-of-coolant accident (LBLOCA) and Small-break loss-of-coolant accident (SBLOCA)
- **Conservative Analysis – Evaluation Model (EM)**
  - **10 CFR 50, Appendix K:** ECCS Evaluation Models
  - Simple but conservative analysis codes
  - Conservative assumptions (I.C., B.C., plant parameters, etc.)
- **Realistic Analysis – Best-Estimate**
  - **Regulatory Guide 1.157:** Best-Estimate Calculations of Emergency Core Cooling System Performance
  - BE codes with detailed models such as RELAP5, TRAC, CATHARE, . . .
  - Various uncertainty quantification methods

(3-6) ECCS Acceptance Criteria: 10 CFR 50.46

- **Peak Cladding Temperature (PCT).** The calculated maximum fuel element cladding temperature shall not exceed 2200ºF.
- **Maximum Cladding Oxidation**. The calculated total oxidation of the cladding shall nowhere exceed 0.17 times the total cladding thickness before oxidation.
- **Maximum Hydrogen Generation**. The calculated total amount of hydrogen generated from the chemical reaction of the cladding with water or steam shall not exceed 0.01 times the hypothetical amount that would be generated if all of the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.
- **Coolable Geometry**. Calculated changes in core geometry shall be such that the core remains amenable to cooling.
- **Long-term Cooling**. After any calculated successful initial operation of the ECCS, the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed for the extended period of time required by the long-lived radioactivity remaining in the core.

(3-6) LOCA Evaluation Model

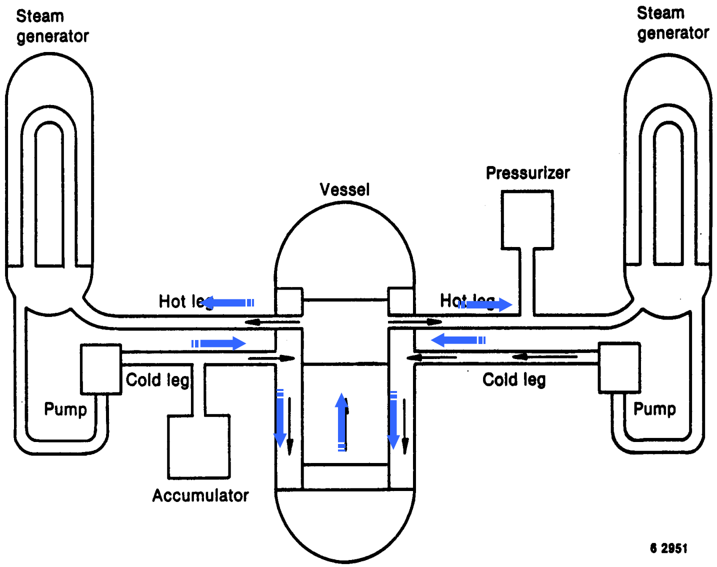
- **Conservative Evaluation Model**
  - Conformance with 10 CFR 50, Appendix K ECCS EM
  - Required Model Should Be Used
- **Best Estimate Model** (Reg. Guide 1.157)
  - BE analysis with uncertainty evaluation
  - Show the acceptance criteria are met considering the calculational uncertainty in **High level of probability**

(3-6) LB LOCA Sequence of Event

- **Blowdown Phase**
  - Discharge of Coolant through Break (0 ~ 25 ~ 30sec)
- **Refill Phase**
  - From End of Blowdown to the time the bottom of the core of reactor vessel core filled with ECCS water (EOB ~ EOB+7 ~8 sec)
- **Reflood Phase**
  - From the core bottom flooding to complete core quenching (End of Refill to ~ Quenching time)
- **Long-Term Cooling Phase**
  - After complete Quenching to secure state

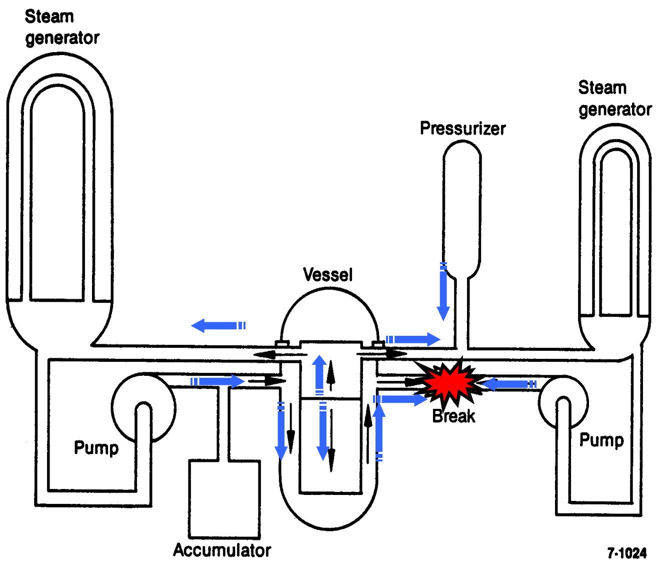
LOCA Phenomena

Normal Operation



Core → Hot Leg → SG → Cold Leg → Downcomer→ Core

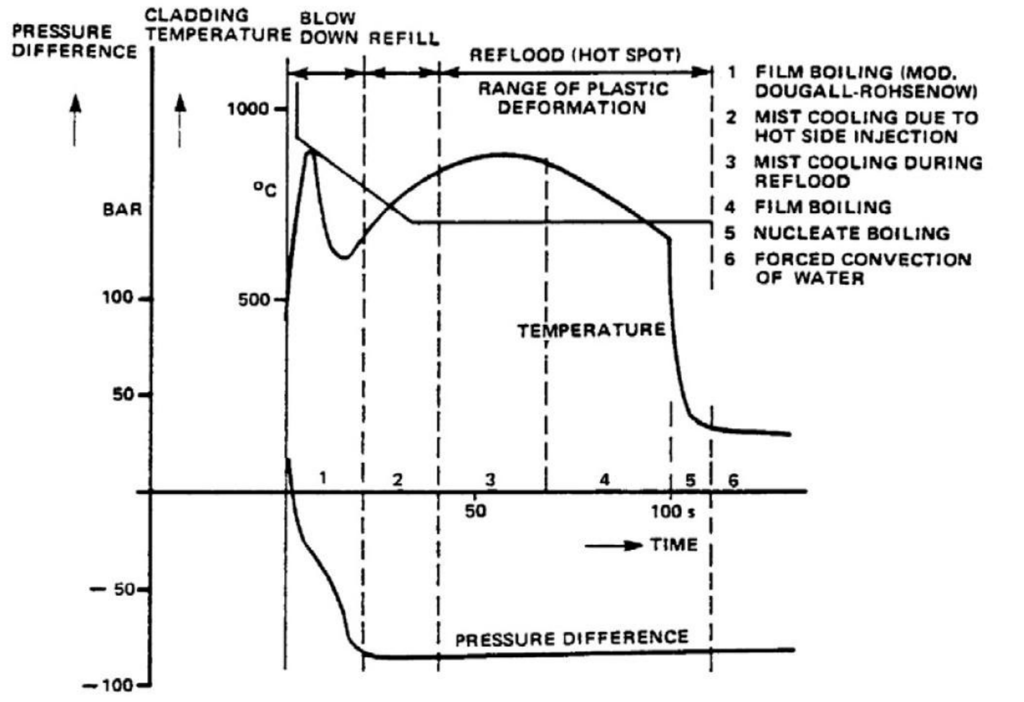
After LOCA



Core → Downcomer/Hot Leg → Cold Leg/Hot Leg → Break

(3-6) LB LOCA Sequence of Event

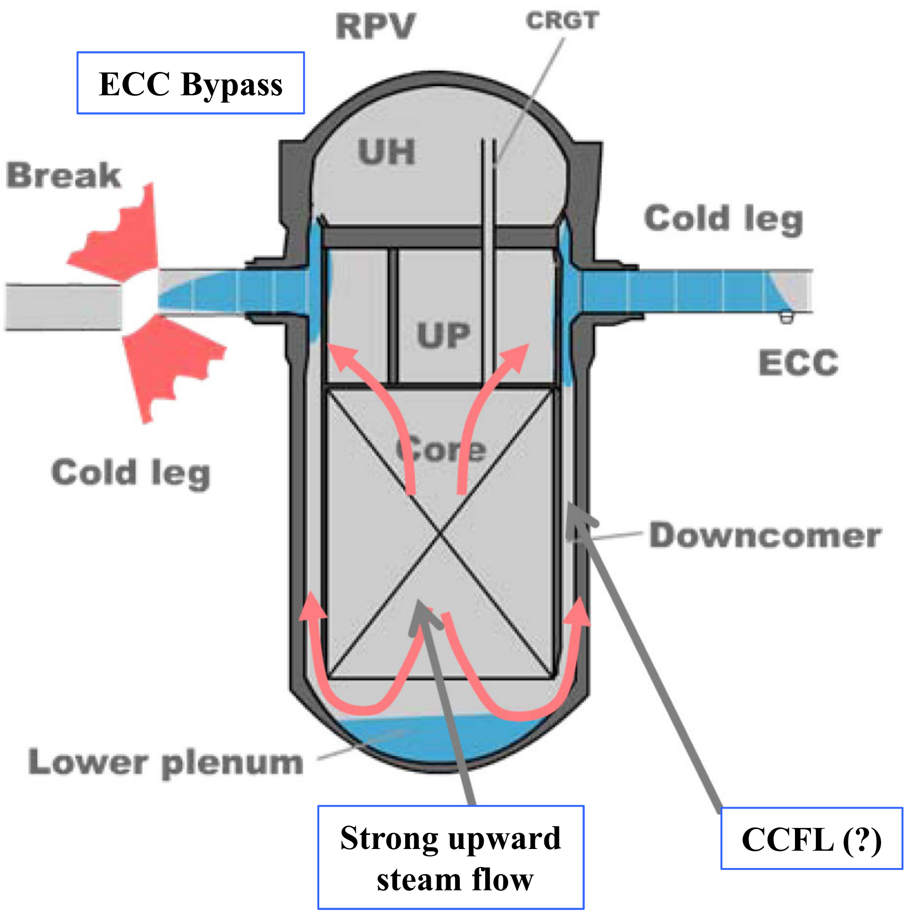
Double ended cold leg break, pressure difference across the cladding and cladding temperature at the hot spot

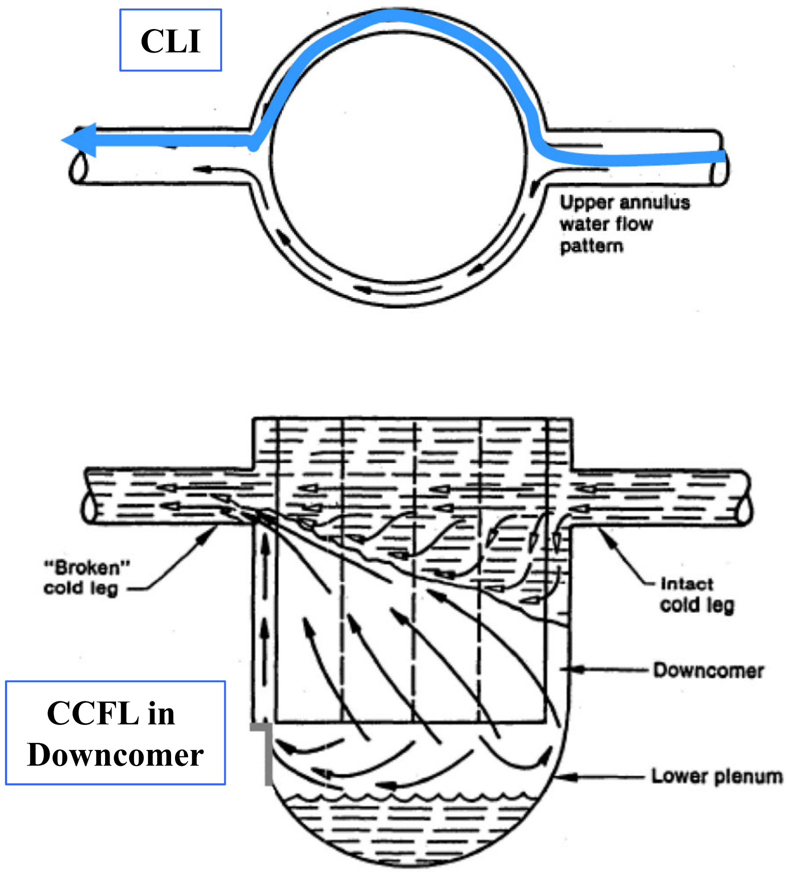


PWR Large Break LOCA

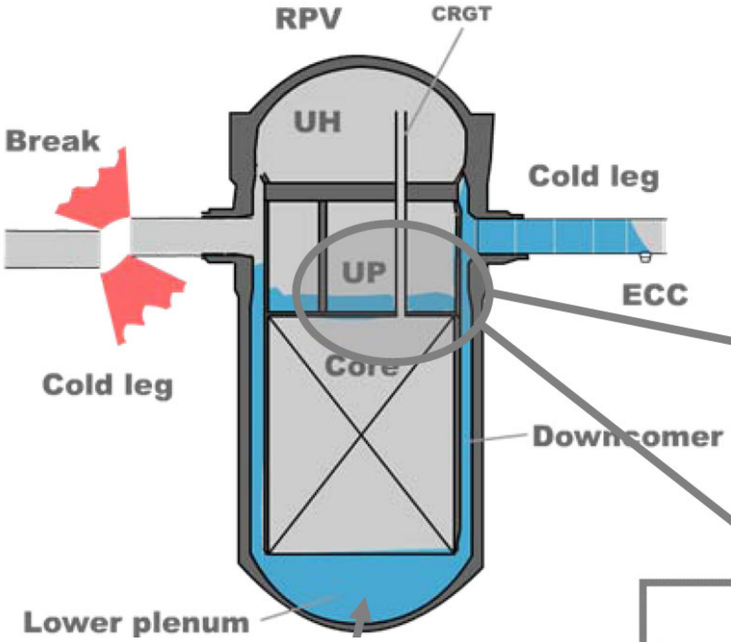
Cladding Temperature and Pressure Difference

LBLOCA- Blowdown Phase





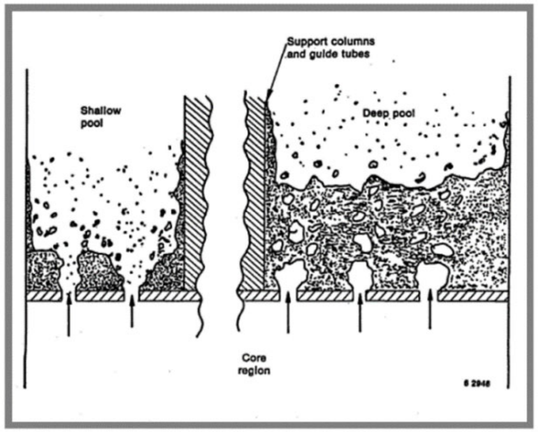
LOCA-Reflood Phase

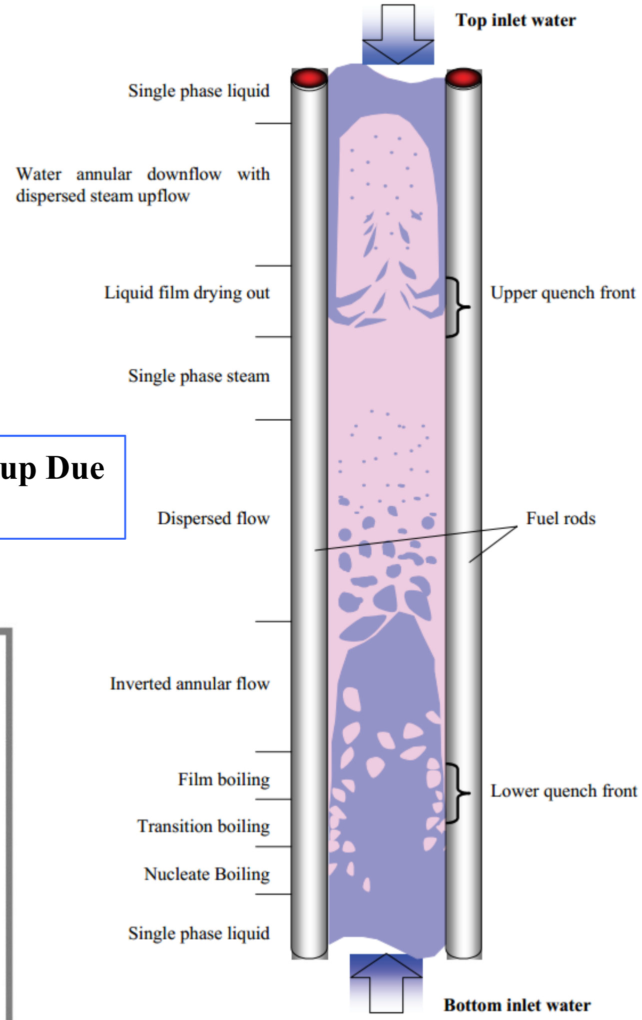


Upper plenum starts to fill up Due to condensation

Lower plenum has been replenished

Top quenching
or
top flooding





Important Phenomena during <u>Blowdown Phase</u>

- ECCS Bypass to Break (Large portion of SIT water bypassed)
- Lower Plenum and part of Downcomer Flooded by ECCS Water
- Bottom of Core Recovered
- Beginning of Reflood

Important Phenomena during <u>Refill Phase</u>

- Break Flow (Chocked Flow)
- Core Nucleate Boiling, Flashing dye to rapid depressurization
- Void Formation, Negative reactivity, Critical Heat Flux
- Reactor Trip, RCP Trip by loss of offsite power, Safety Injection Signal
- Cladding Temperature Peak by depletion of coolant after CHF (Bolwdown-PCT)

Important Phenomena during <u>Reflood Phase</u>

- Core flooded by the continuous SIT injection
- **Complex Flow Regimes and Heat Transfer phenomena** in the core due to interaction of the coolant with hot fuel clad
- Entrainment/De-entrainment by two-phase flow in core and upper plenum
- Two-phase flow at hot leg, heated and vaporized by the heat from the SG secondary side and Steam Binding to increase pressure at the core and to suppress the core quenching, flow oscillation
- PCT (Reflood-PCT) occurrence and quenching by the continuous SIP injection (SIT exhaust)

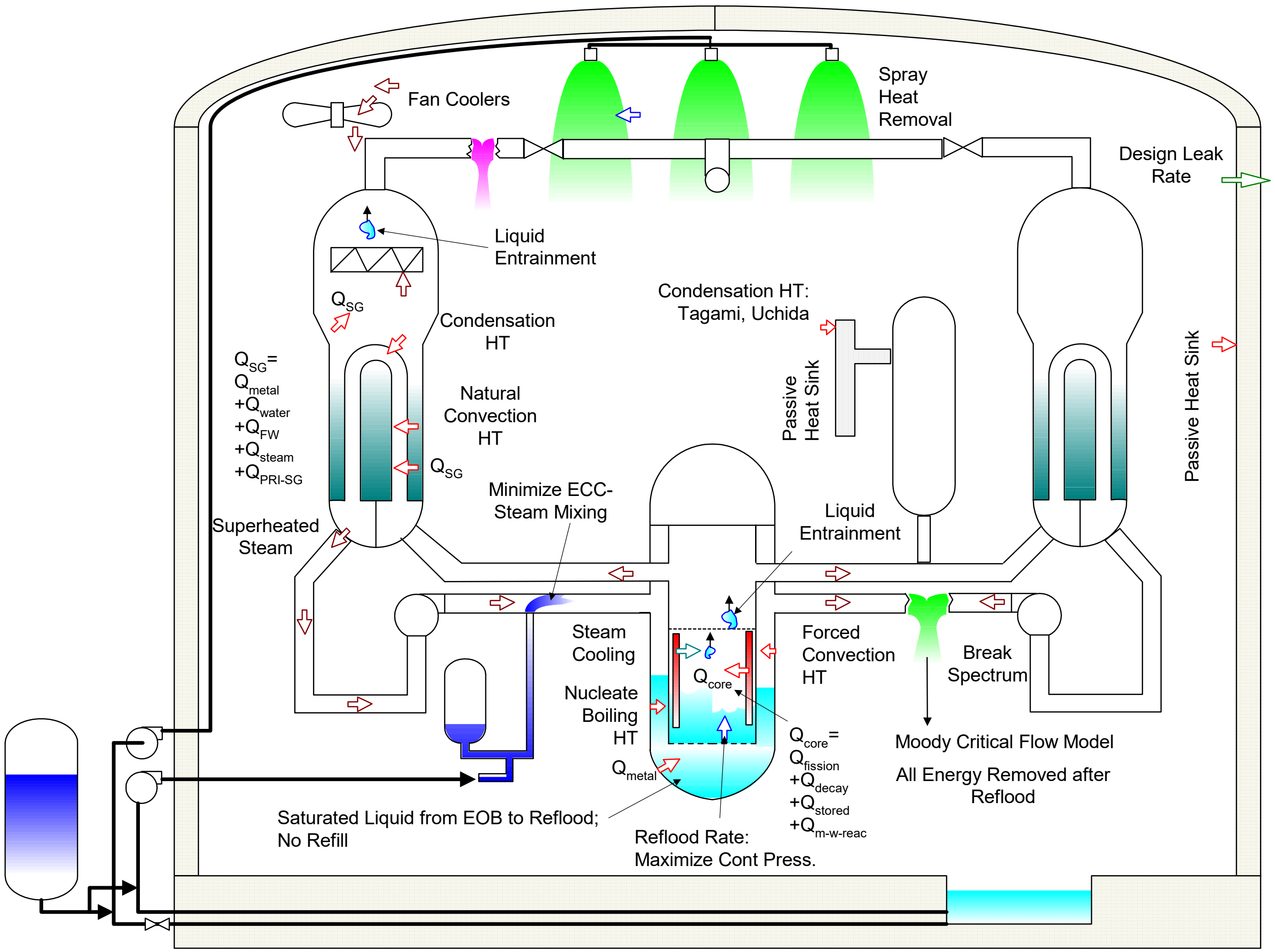
Summary of LOCA

- LOCA is an accident in which reactor coolant is lost by the rupture of primary coolant system pressure boundary
- Loss of coolant results in decreased heat removal from the reactor and overheating of the fuel leads to fuel failure
- Radioactive fission product can be released from fuel to coolant and then into the containment through the broken pipe
- Radioactive material can be leaked out from containment to the outside of reactor resulting radiation exposure to the public

Long-Term Cooling Phase

- After Core Quenching, to remove the core decay heat and maintain the core at low temperature, water continuously provided by SIP
  - Borated water of high concentration may be precipitated at the core Simultaneous injection to hot leg and cold leg to prevent boron precipitation
- Switchover of water source from RWT to Containment recirculation sump
- Long term cooling via Heat Exchangers of Shutdown Cooling System or Containment Spray System

Containment Analysis



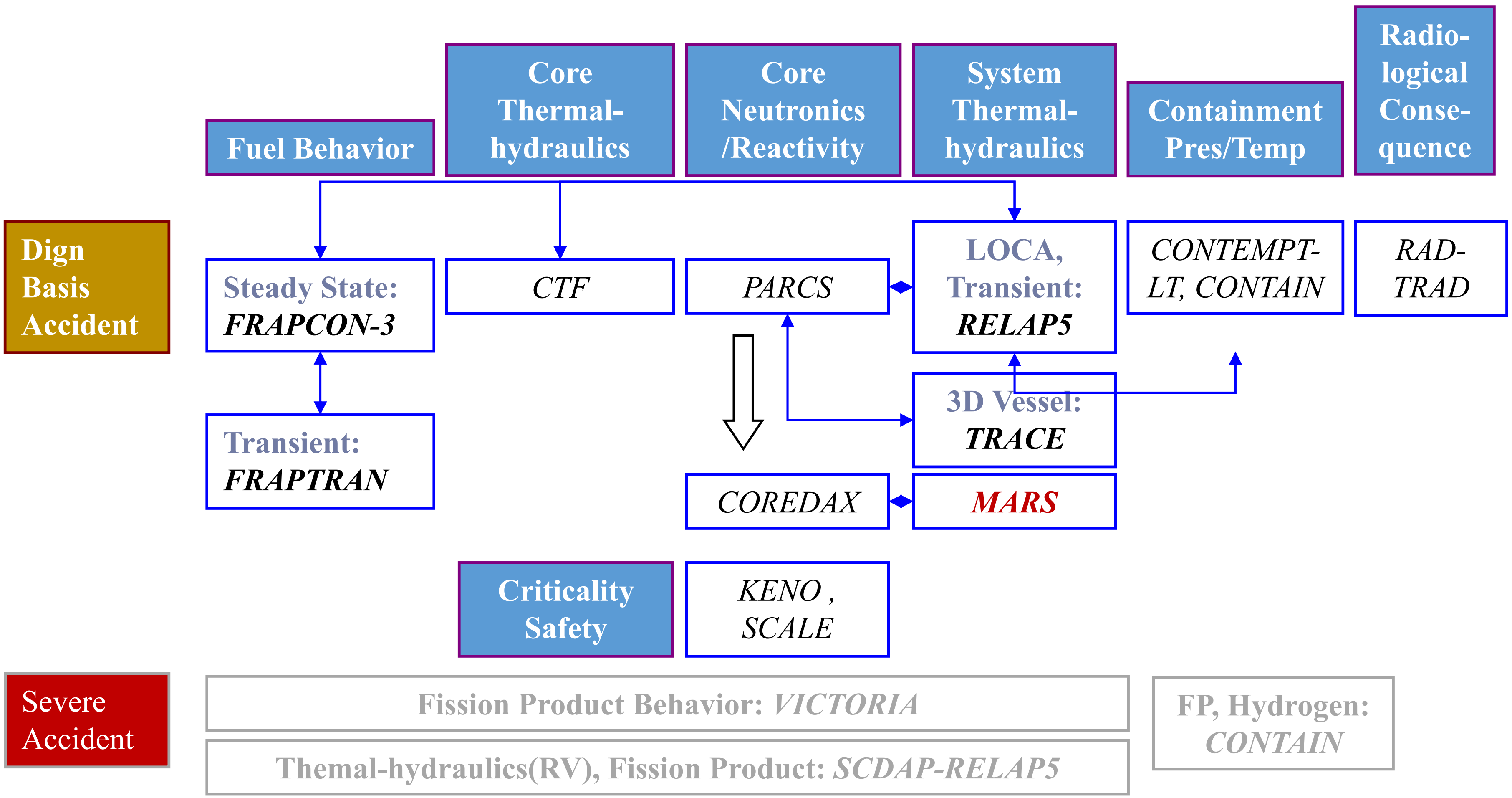
Radiological Consequence Analysis

- **Radiological consequences of DBA**
  - Final safety goal
  - Required by Defense-in-depth concept and regulatory requirements
  - Quantity of the radioactive material that escapes to the environment or enters the control room.
  - Credit for several natural and engineered removal mechanisms. (sprays, natural deposition, leakage, natural and forced convection, filters)

(3-7) Regulatory Auditing Calculation

- What is **Auditing Calculation** ?
  - One of the regulatory activities taken for evaluating safety of NPP in review process
  - Specified at chapter 15.0 , 5, 6, and 4 of Safety Review Guide (Standard Review Plan, USNRC NUREG-0800)
  - An independent analysis for confirming validity and conservatism of Licensee's Safety analysis method and results
  - State-of-the-art Computer Codes used for simulating the complex thermal-hydraulic and mechanical behavior of reactor system
  - Information and basic data (e.g, geometric data, design and operational data) should be provided from Licensee
  - Validity and Reliability of computer codes and method of auditing calculation should be established

(3-7) Regulatory Auditing Calculation



4. Application of deterministic safety analysis

Areas of application

- **Deterministic safety analyses** should be carried out for the **following areas**:
  - Design of nuclear power plants.
    - Such analyses require either a conservative approach or a best estimate analysis together with an evaluation of uncertainties.
  - Production of new or revised safety analysis reports for licensing purposes, including obtaining the approval of the regulatory body for modifications to a plant and to plant operation.
    - For such applications, in many countries, but not all, conservative approaches and best estimate plus uncertainty methods may be used.
  - The assessment by the regulatory body of safety analysis reports.
    - For such applications, in many countries, but not all, conservative approaches and best estimate plus uncertainty methods may be used.

Areas of application

- The analysis of incidents that have occurred or of combinations of such incidents with other hypothetical faults.
  - Such analyses would normally require best estimate methods, in particular for complex occurrences that require a realistic simulation.
- The development and maintenance of emergency operating procedures and accident management procedures.
  - Best estimate codes together with realistic assumptions should be used in these cases.
- The refinement of previous safety analyses in the context of a periodic safety review to provide assurance that the original assessments and conclusions are still valid.
  - As for the original analyses, both, conservative approaches and best estimate plus uncertainty methods may be used.
- By the Regulatory Body to provide independent oversight of licensee activities.

(4-1) The design of nuclear power plants

- The **design basis** for items that are important to safety is required to be established and confirmed by means of a comprehensive safety assessment.
- The design basis comprises the **design requirements** for structures, systems and components that must be met for the safe operation of a nuclear power plant, and for preventing or mitigating the consequences of events that could jeopardise safety.
- For example, deterministic analyses are carried out to determine what pressure and temperature the components of the primary coolant system must be able to withstand.

(4-2) The licensing of nuclear power plants

- The use of deterministic safety analyses to develop the design, and to **license a nuclear power plant,** are closely related.
- The plant must be designed so that it complies with **all the applicable regulations and standards** and this must be demonstrated in safety analysis reports in order to obtain licenses to construct and operate the plant.
- The analyses that are presented in the safety analyses reports should represent the current state of the design and should be presented in a way that demonstrates to the **regulatory body** that its **requirements** have been **met.**

(4-3) The assessment of safety analysis reports

- The **operating organisation** shall ensure that an **independent verification of the safety assessment** is performed by individuals or groups separate from those carrying out the design, before the design is submitted to the regulatory body.
- **Additional independent analyses** of selected aspects may also be carried out by or on behalf of the **regulatory body.**

(4-4) Application in plant modifications

- The **modification** of **existing** nuclear power **plants** is normally undertaken
  - to counteract the ageing of the plant,
  - to justify its continued operation,
  - to take advantage of developments in technology or
  - to comply with changes to the applicable rules and regulations.

(4-4) Application in plant modifications

- To comply with the **regulatory requirements**, a **revision of the safety analysis** of the plant design should be made
  - when major modifications or modernization programmes are implemented,
  - when advances in technical knowledge and understanding of physical phenomena are made,
  - when changes in the described plant configuration are implemented or
  - when changes are made in operating procedures owing to operational experience.

(4-4) Application in plant modifications

- Other **important applications** of deterministic safety analysis are aimed at the more **economical utilization** of the reactor and the nuclear fuel.
- Such applications encompass
  - up-rating of the reactor power,
  - the use of improved types of fuel and
  - the use of innovative methods for core reloads.
- Such applications often imply that the **safety margins** to operating limits are **reduced** and **special care** should be taken to ensure that the limits are not exceeded.

(4-5) Analysis of operational events

- The analysis of **actual events** that have occurred on operating nuclear power plants are a very important way of establishing the extent to which the deterministic analysis that has been performed **accurately represents** the **behaviour of the plant.**
- Such analyses should form an integral part of the **feedback** from operational experience.

(4-5) Application to the analysis of operational events

- **Operational events** may be analysed with the **following objectives:**
  - To check the adequacy of the selection of postulated initiating events;
  - To determine whether the transients that have been analysed in the safety analysis report bound the event;
  - To provide additional information on the time dependence of the values of parameters that are not directly observable using the plant instrumentation;
  - To check whether the plant operators and plant systems performed as intended;

(4-5) Analysis of operational events

- **Operational events** may also be analysed with the **following objectives:**
  - To check and review emergency operating procedures;
  - To identify any new safety issues and questions arising from the analyses;
  - To support the resolution of potential safety issues that are identified in the analysis of an event;
  - To analyse the severity of possible consequences in the event of additional failures (such as severe accident precursors);
  - To validate and adjust the models in the computer codes that are used for analyses and in training simulators.
- The analysis of operational events requires the use of a **best estimate approach**. **Actual plant data** should be used. If there is a lack of detailed information on the plant status, **sensitivity studies**, with the variation of certain parameters, should be performed.

(4-6) Development and validation of emergency operating procedures (EOPs)

- Best estimate deterministic safety analyses should be performed to confirm the **strategies** that have been developed to restore normal operational conditions at the plant following transients due to **anticipated operational occurrences and design basis accidents.**
- These strategies are reflected in the **emergency operating procedures** that define the actions that should be taken during such events.
- After the emergency operating procedures have been developed, a **validation analysis** should be performed.
- This analysis is usually performed by using a **qualified simulator**.

(4-6) Development of severe accidents management guidelines (SAMGs)

- Deterministic safety analyses should also be performed to assist the development of the **strategy** that an operator should follow if the emergency operating procedures fail to prevent a **severe accident** from occurring.
- The analyses should be carried out by using one or more of the **specialized computer codes** that are available to model relevant physical phenomena.

(4-6) Development of severe accidents management guidelines (SAMGs)

- For **light water reactors**, these include
  - thermo-hydraulic effects,
  - heating and melting of the reactor core,
  - the retention of the molten core in the lower plenum,
  - molten-core–concrete interactions,
  - steam explosions,
  - hydrogen generation and combustion, and
  - fission product behaviour.

(4-7) Periodic safety reviews

- New deterministic analyses may be required to refine previous safety analyses in the context of a **periodic safety review** to provide assurance that the original assessments and conclusions are still valid.
- In such analyses, account should be taken of any **margins** that may have become **reduced** and continue to be reduced owing to ageing over the period under consideration.
- **Best estimate analyses** together with an **evaluation of the uncertainties** may be appropriate to demonstrate that the remaining margins are adequate.

5. Summary

Summary (Recapping)

1. Needs for Safety Analysis
2. Introduction of Safety Analysis: DSA
   (1) Purpose
   (2) Requirements
   (3) Analysis in the Plat Sates
3. Safety analysis approaches
   (1) Classification of Initiating Events
   (2) Overview of Deterministic Analysis
   (3) Typical Safety Criteria for DBAs
   (4) Accident Analysis Codes
   (5) LOCA and Non-LOCA Analysis
4. Application of deterministic safety analysis
5. Summary