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

Design of Nuclear Reactor

Key Yong SUNG

(k109sky@kins.re.kr)

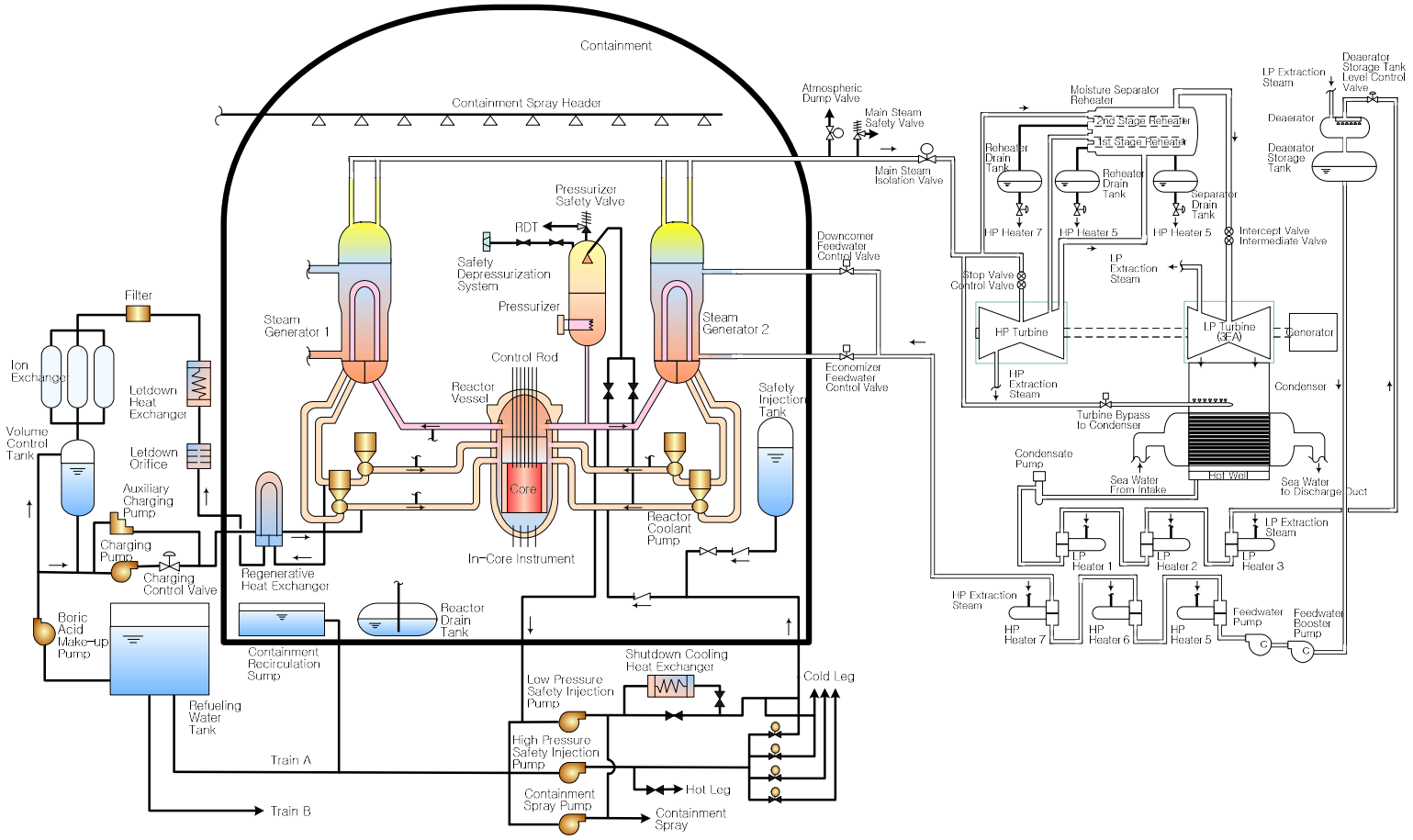
Korea Institute of Nuclear Safety

Lecture Topics

- **Introduction**
  - Fundamental Safety Functions
  - Defense-in-Depth
- **Defense-in-Depth Design in Safety**
  - DID Concept
  - DID Implementation
- **Overview of Safety Assessment**
  - Safety Assessment Process
  - Main Elements for Safety Assessment

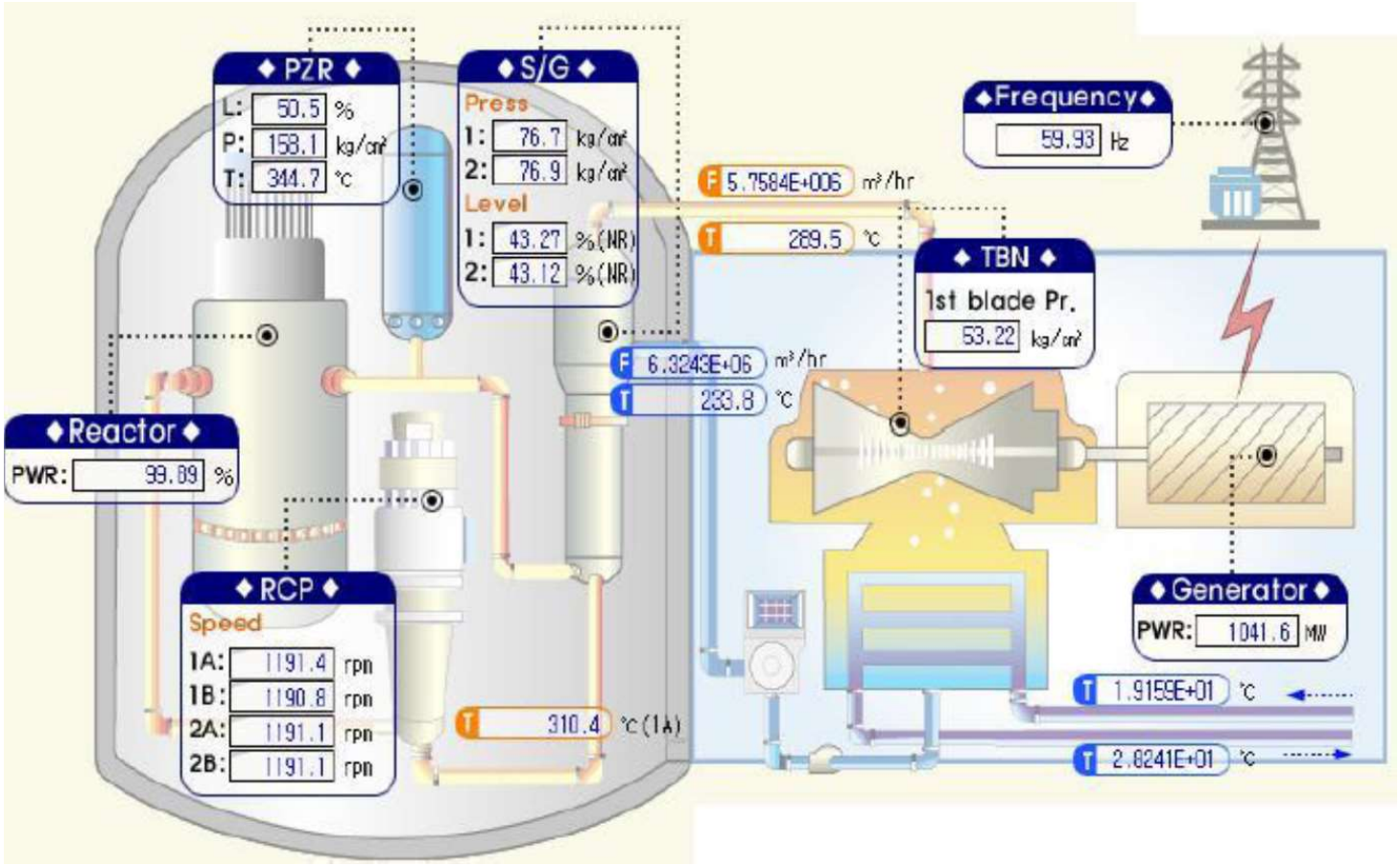
❖ *Most of the contents in this lecture are adopted from the IAEA publications and presentations (GSR-4, SSR-2/1)*

Plant Overall Configuration of OPR-1000



[Source : KINS-Saudi Training Material]

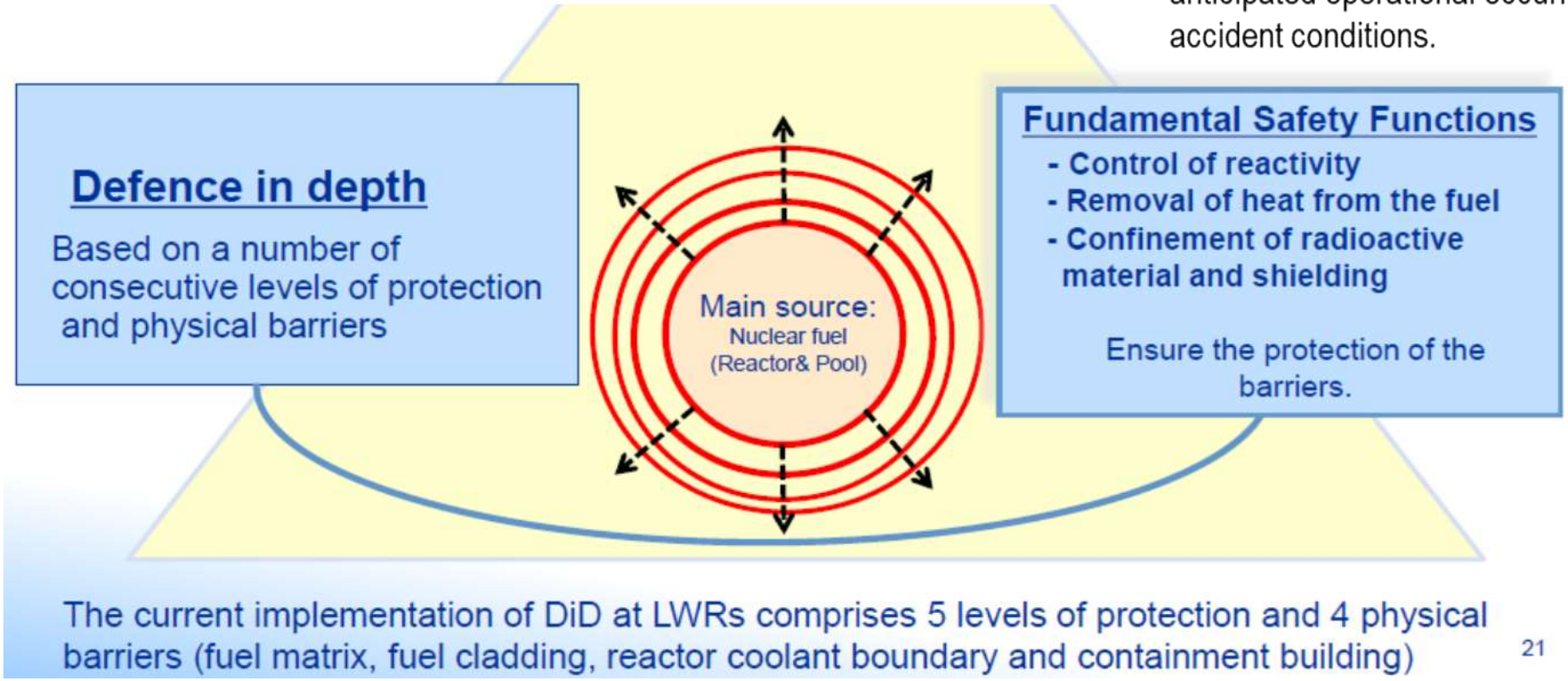
Operating Parameters of OPR-1000



[Source : KINS-Saudi Training Material]

Fundamental Safety Functions for NPPs

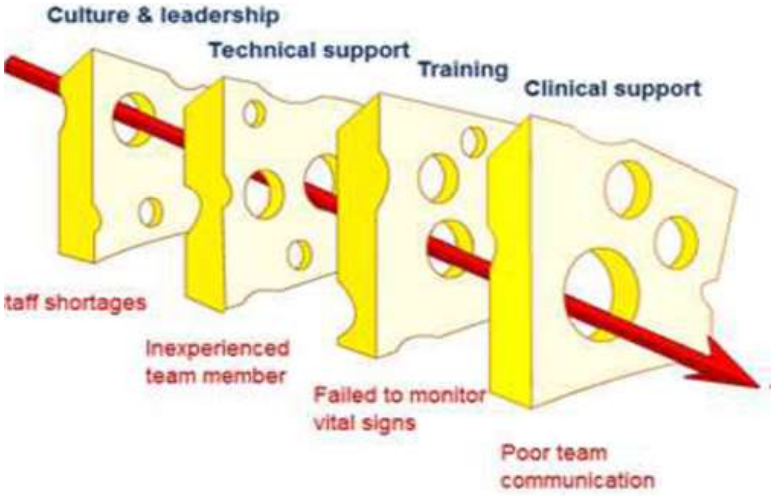
- Safety functions are functions that are necessary to be performed for the facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions.



[Source : Presentation at IAEA SSR-2/1 Workshop(2019)]

Basic DiD Concept

- **(Definition) by US NRC**
  - An approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials.
  - The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon.



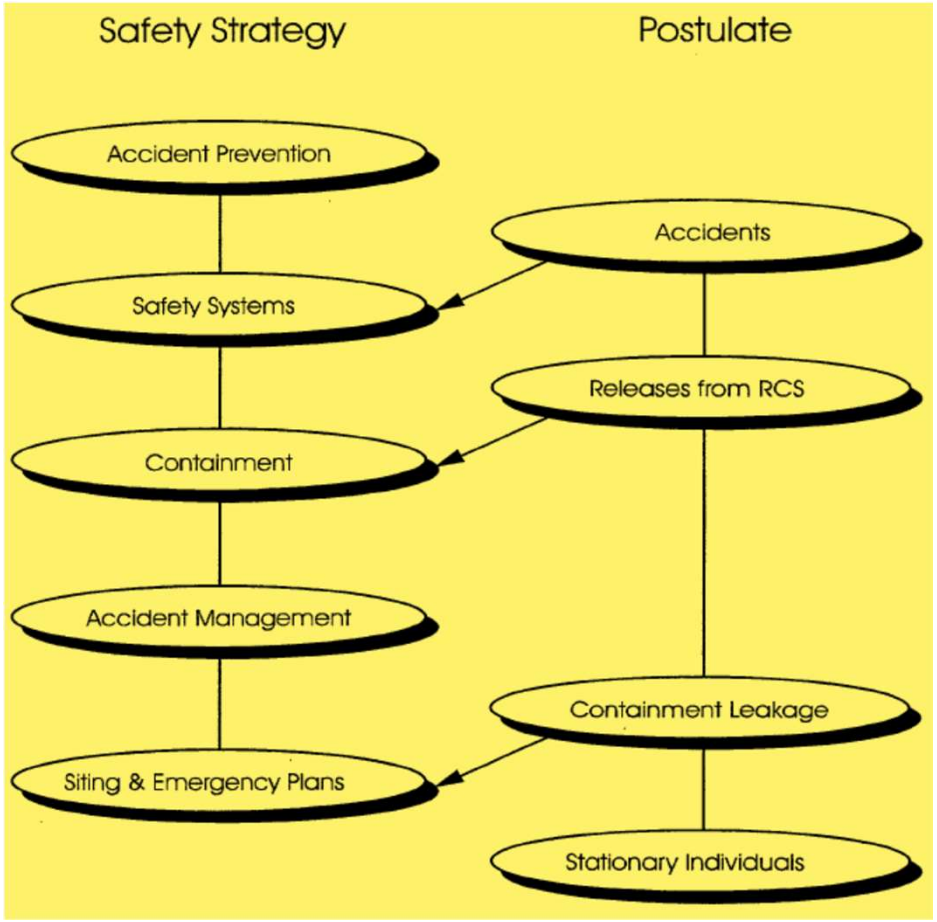
- Military Strategy
- Prison
- Chemical industry
- Information tech.
- Nuclear Industry
- Protection of building
- Home ….

Beginning of DiD in Nuclear Powered Warship

- **Nautilus- The first nuclear-powered submarine** (sea trials in 1955)
  - **Shipingport**, the first commercial NPP, began to produce electrical power in 1957
  - No avenue of escape for crew while the ship was at sea and major ports were generally large population centers(no remote siting)
  - Submarine hull provided a containment capability but to protect the crew
- **Navy relied on an accident-prevention strategy (Fig.)**
  - Conservative approach for design with considerable margin
  - Stringent procedures for operator training, Quality control & assurance, and System/component testing.
  - Redundant safety systems based on potential equipment malfunctions and failures
  - Four barriers : fuel itself(metal), Reactor primary system, Reactor compartment, Ship's hull
- **This strategy applied to commercial nuclear reactors in early 1960s**

Key Elements of Overall Safety Strategy in the early 1950s

Barrier or Layer	Function
1. Ceramic fuel pellets	Only a fraction of the gaseous and volatile fission products is released from the pellets.
2. Metal cladding	The cladding tubes contain the fission products released from the pellets. During the life of the fuel, less than 0.5 percent of the tubes may develop pinhole sized leaks through which some fission products escape.
3. Reactor vessel and piping	Thick steel vessels and pipes contain the reactor cooling water. A portion of the circulating water is continuously passed through filters to keep the radioactivity low.
4. Containment	The nuclear steam supply system is enclosed in a containment building strong enough to withstand the rupture of any pipe in the reactor coolant system.
5. Exclusion area	A designated area around each plant separates the plant from the public. Entrance is restricted.
6. Low population zone, evacuation plan	Residents in the low population zone are protected by emergency evacuation plans.
7. Population center distance	Plants are located at a distance from population centers.



Excerpted From NUREC/CR-6042(Rev,2)

Lecture Topics

- Introduction
  - Fundamental Safety Functions
  - Defense in depth (DID)
- **Defense-in-Depth Design in Safety**
  - DID Levels and Plant States of NPPs
  - DID Implementation into NPPs
- Overview of Safety Assessment
  - Safety Assessment Process
  - Main Elements for Safety Assessment

Hazard, Risk ?

Hazard :

Source of Risk

- Combustible material
- High Pressure piping
- Chemical solution
- Radionuclide inventory

Hazard

Protection

Risk

Protection :

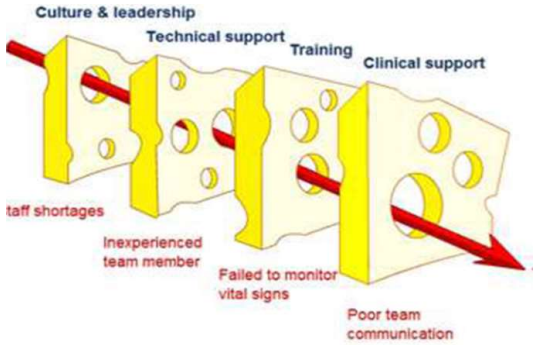
Prevent Loss or Damage

- Fire extinguisher
- Pipe restraints
- Protective clothing
- Emergency cooling system

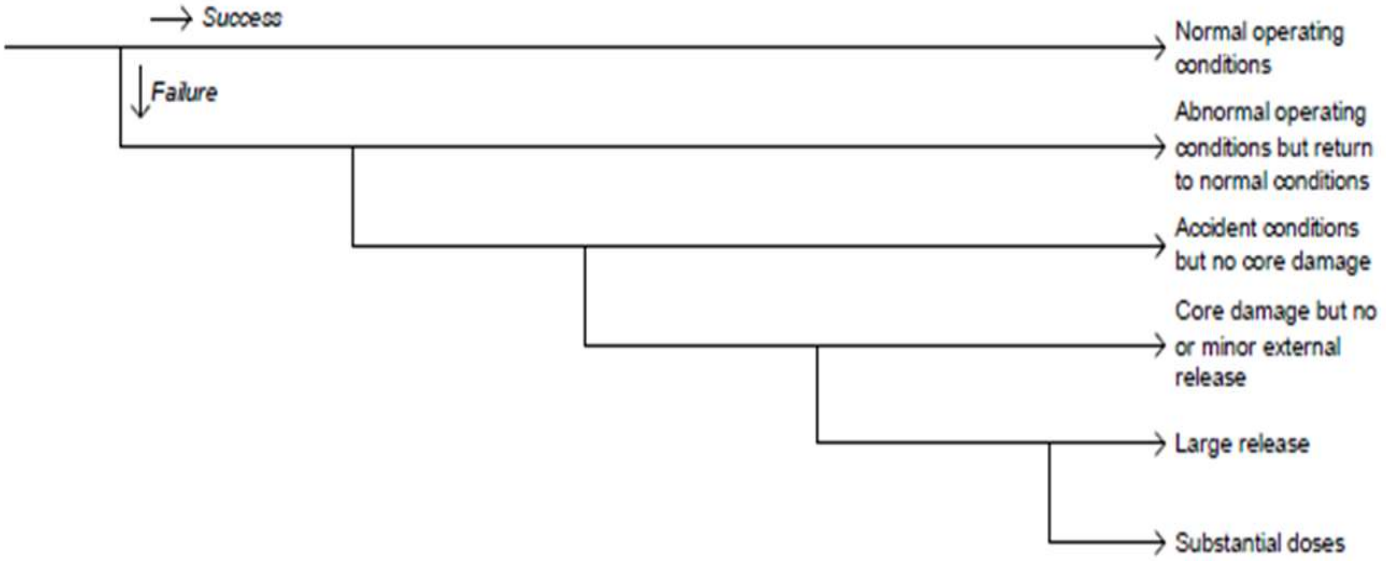
Risk :

Likelihood of Hazard causing Loss or Damage

DiD Levels and Relationship with Plant States



DID level 1 Prevention of abnormal operation and failures	DID level 2 Control of abnormal operation and detection of failures	DID level 3 Control of accidents within the design basis	DID level 4 Severe accident management (DEC)	DID level 5 Mitigation of the radiological consequences	Consequence



Plant States Definition

- **Normal Operation(NO)**
  - Includes all the phases of operation within specified operational limits and conditions both at power and shutdown.
- **Anticipated Operational Occurrences (AOOs)**
  - An operational process deviating from NO which is expected to occur at least once during the operating life time of the plant,
  - but in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions
- **Design Basis Accident (DBA)**
  - A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria, and for which releases of radioactive material are kept within acceptable limits. Postulated for the design bases of the safety systems.
- **Design Extension Conditions (DEC) : Beyond DBA?, Severe accident?**
  - Postulated accident conditions that are not considered as DBAs, but that are considered in the design process for the facility, and for which releases of radioactive material are kept within acceptable limits. DEC comprise conditions in events with core melting

Typical Initiating Events (Transients & Accident Symptoms)

- 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
- Increase in reactor coolant inventory
- Decrease in reactor coolant inventory
- Anomalies in distribution of reactivity and power
- Radioactive release from a subsystem or component

- **(Ex.) Decrease in Reactor Coolant Inventory**
  - **(AOO)** Very small LOCA due to an instrument line failure
  - **(DBA)** Loss of Coolant Accident(LOCA), Steam Generator Tube Rupture(SGTR)
  - **(DEC W/O Core Melting)**
    - Loss of core cooling due to Station BlackOut (SBO)
    - Multiple steam generator tube ruptures(MSGTR)
  - **(DEC W/ core melting)** Severe accident

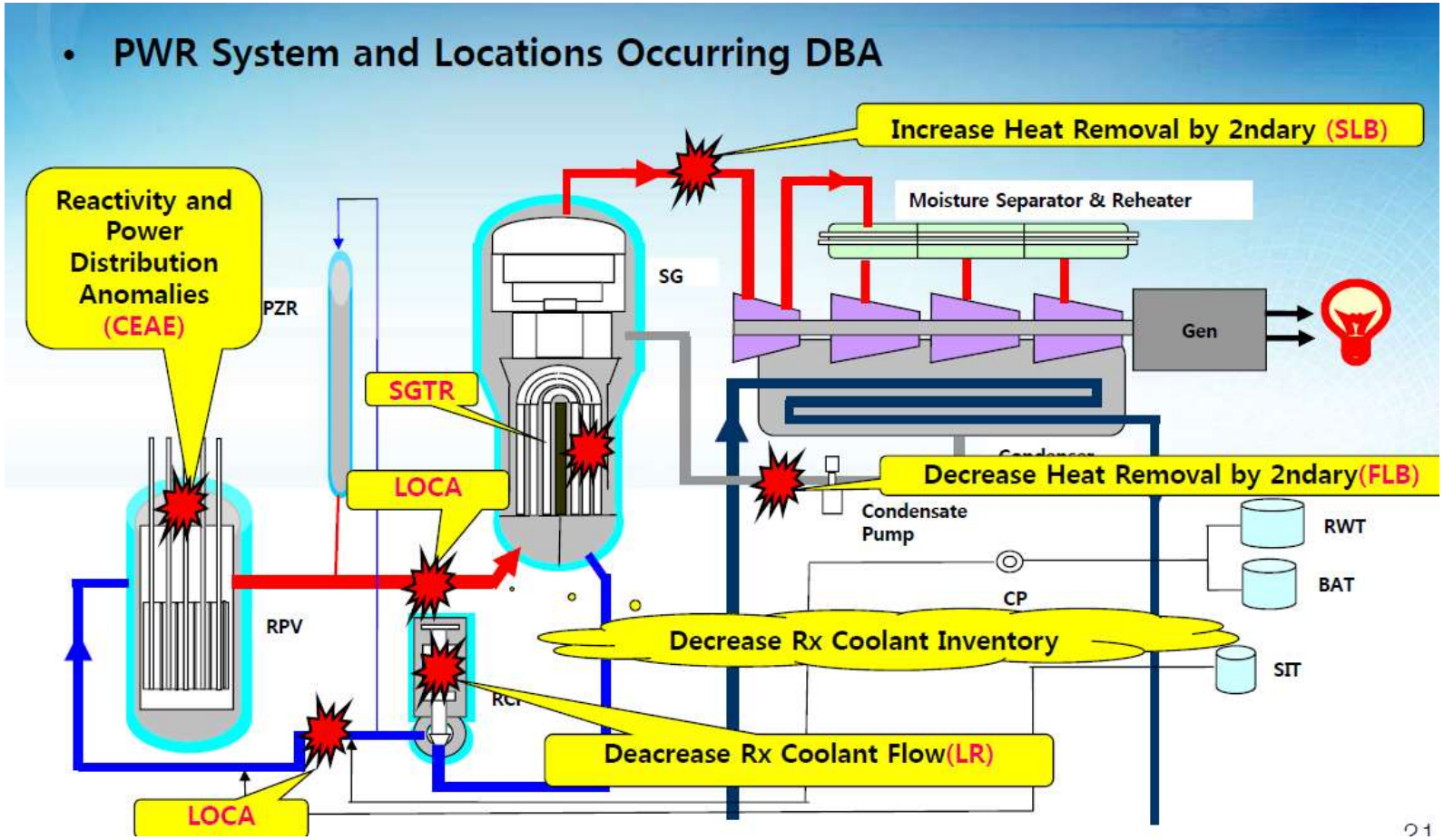
Plant States Definition and Example Conditions(1)

- **Normal Operation(NO)**
  - Includes all the phases of operation for which the plant was designed to operate both at power and shut down.
    - Normal reactor start-up from shutdown
    - Power operation and changes in the reactor power level,
    - Reactor shutdown from power operation including handling and storage of fresh and irradiated fuel
- **Anticipated Operational Occurrences (AOO)**
  - Increase in reactor heat removal (inadvertent opening of steam relief valve…)
  - Decrease in reactor heat removal (trip of one main feedwater pump…)
  - Decrease in reactor coolant system flow rate(Trip of one RCP…)
  - Reactivity and power distribution anomalies (inadvertent control rod withdrawal…)
  - Increase in reactor coolant inventory(malfunctions of reactor inventory control system..)
  - Decrease in reactor coolant inventory(very small LOCA due to an instrument line failure)
  - Loss of Offsite Power(LOOP)

Plant States : Example Conditions(2)

- **DBA (Design Basis Accident)**
  - A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits. Postulated for the design bases of the safety systems.
    - Increase in reactor heat removal (**MSLB** : Main Steam Line Break)
    - Decrease in reactor heat removal (**MFLB** : Main FeedLine Break)
    - Decrease in reactor coolant system flow rate **(Main Coolant Pump Seizure**)
    - Reactivity and power distribution anomalies **(Control Rod Ejection)**
    - Increase in reactor coolant inventory **(Inadvertent Operation of ECCS)**
    - Decrease in reactor coolant inventory (**LOCA**: Loss Of Coolant Accident, **SGTR** : Steam Generator Tube Rupture)

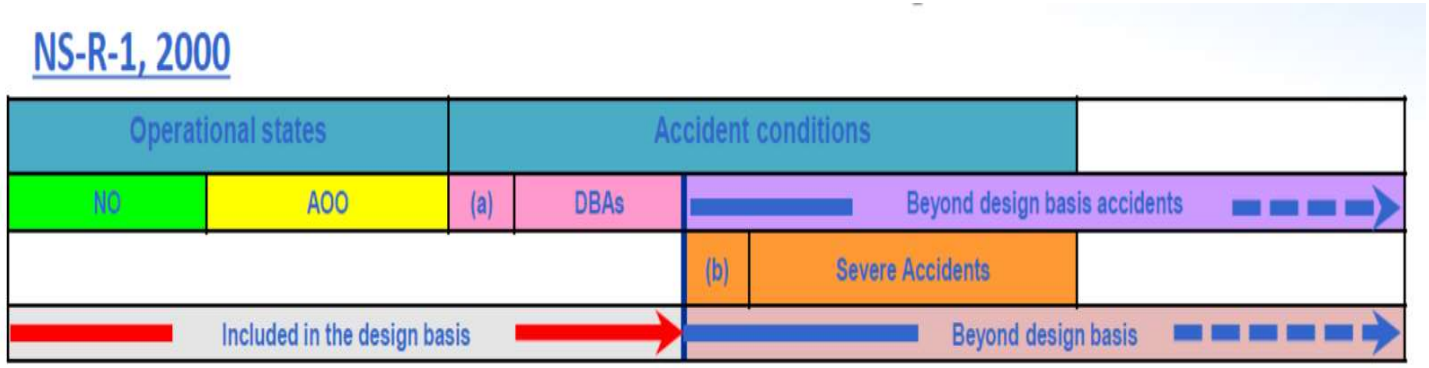
Various Initiating Events(DBA)

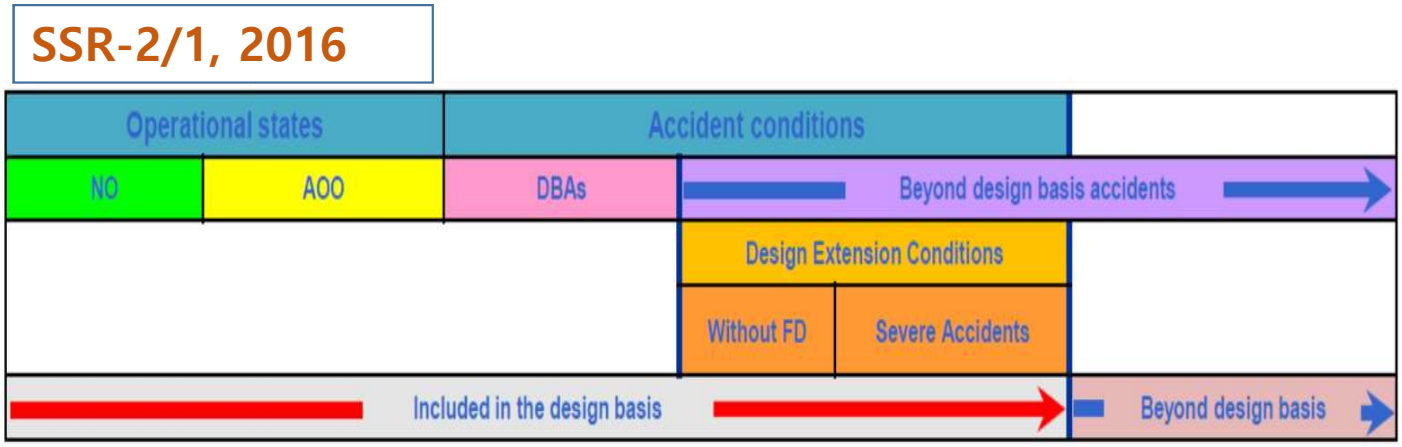


Plant States Definition and Example Conditions(3)

- **DEC (Design Extension Conditions)**
  - DEC comprise conditions in events without significant fuel degradation and conditions in events with core melting
  - **(W/O core melting)**
    - ATWS (Anticipated Transient Without Shutdown) : No drop of control rods
    - SBO (Station Black) : LOOP + EDGs failure
    - Loss of core cooling in the residual heat removal mode
    - Extended loss of cooling of fuel pool and inventory
    - Loss of normal access to the ultimate heat sink
    - Total loss of feed water
    - Multiple steam generator tube ruptures(MSGTR)
  - **(W/ core melting)** : Severe accident phenomena
    - Hydrogen detonation, Basemat melt through due to core-concrete interaction, Steam explosion..

Change of PS & Design Basis Scope(IAEA)





Design Basis ≠ Design Basis Accidents

Beyond Design Basis ≠ Beyond Design Basis Accidents

- **Beyond DBA (NS-R-1)**

Accident sequences that are possible but were not fully considered in the design process because they were judged to be too unlikely

- **Design Extension Conditions(DEC)**

Postulated accident conditions that are not considered for DBAs , but that are considered in the design process for the facility.

Excerpted from IAEA WS Presentation(30 Sep.~4 Oct.2019)

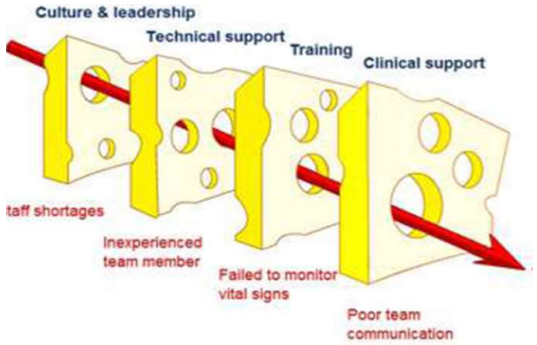
DiD Levels and Essential Means (IAEA TECDOC-1791(2016))

Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
Level 1 (NO)	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1 (NO)
Level 2 (AOO)	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures	(AOO) Level 2
3a (DBA)	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures	Level 3 (DBA)
Level 3 3b (DEC)	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without core melting	Emergency operating procedures	4a (DEC-A)
Level 4 (DEC)	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melting. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	Level 4 4b (DEC-B)
Level 5 (EP)	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	(EP) Level 5

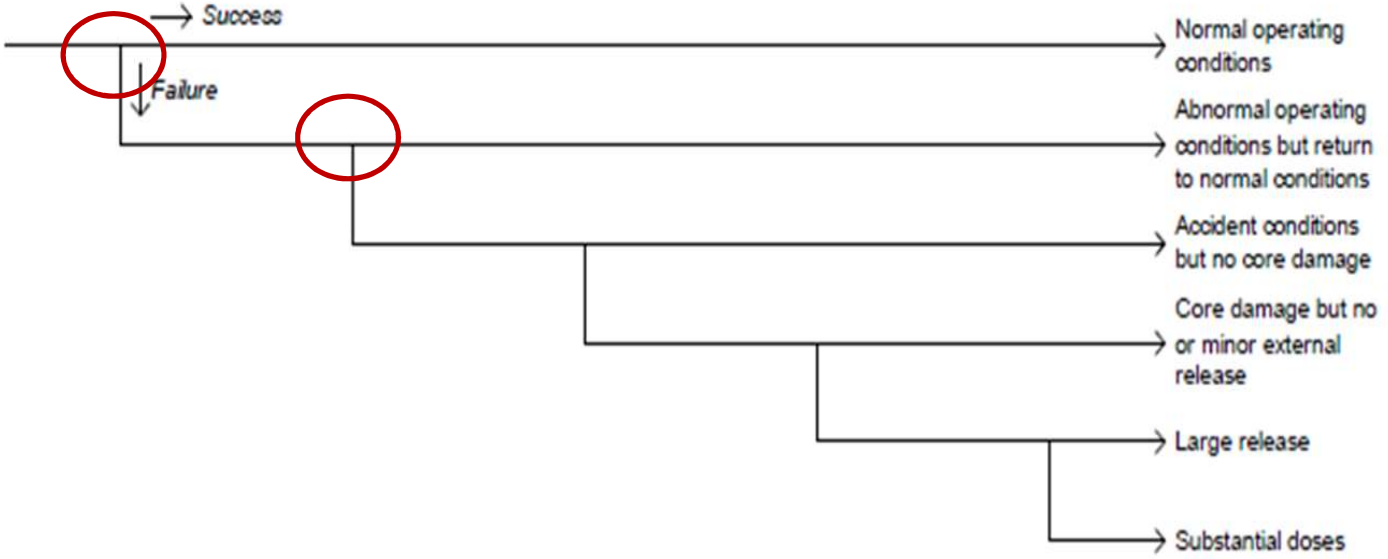
How to maintain NO? (DiD L-1)
How to prevent escalation of AOOs to Accidents? (L-2)

- Design ?
- Operation ?
- Operating Procedure?
- Maintenance & Test ?
- etc. ?

DiD Levels and Relationship with Plant States



DID level 1 Prevention of abnormal operation and failures	DID level 2 Control of abnormal operation and detection of failures	DID level 3 Control of accidents within the design basis	DID level 4 Severe accident management (DEC)	DID level 5 Mitigation of the radiological consequences	Consequence



Main Elements for maintaining Safety in NO & AOOs

- **Nuclear Design** : **Nuclear & Core Design**
- **Integrity of SSCs** : **Code & Std.**
  - Structural Integrity, Classification, Safety & Operational Margin..
- **Plant Control** : **Plant Control Systems**
  - Monitoring : Power, Pressure, Temperature, Water level, Flow, Control rod position..
  - Control system : PPCS, PLCS, FWCS, RRS, SBCS..
- **Plant Protection System** : **Plant Protection System**
  - Automatic shutdown in case of exceeding the setting points for safety
- **Operating Procedures** : **Normal, Abnormal, Surveillance Test**
  - Heat-up, Cool-down, Full power, Test, Abnormal conditions…
- **Operational Limits and Conditions** **(Technical Specifications)**
  - Safety Limits, Limiting Condition of Operation, Operator's Action, Testing & Maintenance..
- **Trained Operators**
  - Safety culture, Strict training, Feedback of operating experiences …

Nuclear & Core Design

- Core Configuration
  - Flux/Power Shape Control
  - Local Linear Heat Rate
- Negative Reactivity(MTC, FTC)
- Shutdown Margin
- Departure from Nucleate Boiling(DNB)
  - DNBR > 1.3

SSCs Integrity

- Classification of the SSCs
  - Safety Classification
  - Seismic Classification
  - Quality Group Classification
  - Electrical Power & I&C Systems Classification
- Integrity Monitoring
  - Leakage Monitoring, Operational Monitoring
- Periodic Inspection
  - Non-Destructive Test (In-Service Inspection)

Application of Code & Standards(Korean Practice)

Class	Seismic	Quality Group	Safety	Quality STD	Quality Req.	Owner Quality Class	
	RG 1.29	RG 1.26	ANSI-51.1/ ANSI-58.14	Applicable Code	10CFR50 App.50 & ASME NQA-1		
Fluid Equip.	Seismic Cat.1	A	SC-1	ASME III, NB	All 18 Criteria	Q (Safety Related)	
		B	SC-2	ASME III, NB			
		C	SC-3	ASME III, NB			
	Non-Seismic Cat.1 (Category II)	D	NNS (SC-4)	ASME VIII, B31.1 & API	Partial	T (Safety Impact)	A (Augmented)
	N/A	Commercial				R (Reliability)	
						S (Industrial)	
Containment	Seismic Cat.1	B	SC-2	ASME III, Div.2 ACI, ANSI/AISC	All 18 Criteria	Q (Safety Related)	
Electric Equip. & I&C	Seismic Cat.1	C	SC-3	IEEE	All 18 Criteria	Q (Safety Related)	

Adopted from KINS-K.A.CARE Training Material (C. Kang)

Safety Classification (based on ANSI/ANS 51.1) (1)

- **Safety Class 1**
  - SC-1 applies to pressure-retaining portions and supports of mechanical equipment that form part of the RCPB whose failure could cause a loss of reactor coolant in excess of the reactor coolant normal makeup capability and whose requirements are within the scope of the (ASME Sec.III.)

- **Safety Class 2**
  - SC-2 applies to pressure-retaining portions and supports of primary containment and other mechanical equipment, whose requirements are within the scope of the (ASME Sec.III), which are not assigned to SC-1 but are relied on to accomplish the following safety functions:

    1) Provide fission product barriers or primary containment radioactive material holdup or isolation
    2) Provide emergency heat removal for the containment atmosphere to an intermediate heat sink, or emergency removal of radioactive material from the containment atmosphere (e.g., containment spray)
    3) Introduce emergency negative reactivity to make the reactor subcritical (e.g., boron injection system), or restrict the addition of positive reactivity via pressure boundary equipment
    4) Provide reasonable assurance of emergency core cooling where the equipment provides coolant directly to the core (e.g., residual heat removal, emergency core cooling)
    5) Provide or maintain sufficient reactor coolant inventory for emergency core cooling

Safety Classification (2)

Safety Class 3

- SC-3 applies to equipment not included in SC-1 or SC-2 that is designed and relied on to accomplish the following safety functions:

1) Provide the functions defined in SC-2 where equipment, or portions thereof, is not within the scope of (ASME Sec.III)
2) Except for the primary containment boundary extension function, provide reasonable assurance of hydrogen concentration control of the primary containment atmosphere to acceptable limits
3) Remove radioactive material from the atmosphere of confined space outside primary containment (e.g., MCR, fuel building) containing SC-1,2, or 3 equipment
4) Introduce negative reactivity to achieve or maintain subcritical reactor conditions (e.g., boron makeup)
5) Provide or maintain sufficient reactor coolant inventory for core cooling (e.g., reactor coolant normal makeup system)
6) Maintain geometry within the reactor to provide reasonable assurance of core reactivity control or core cooling capability (e.g., core support structures)
7) Structurally load-bear or protect SC-1, 2, or 3 equipment
8) Provide radiation shielding for the MCR or offsite personnel
9) Provide reasonable assurance of required cooling for liquid-cooled stored fuel (e.g., SFP and cooling system)
10) Provide reasonable assurance of nuclear safety functions provided by SC-1, 2, or 3 equipment (e.g., provide heat removal for SC-1, 2, or 3 heat exchangers, provide lubrication of SC-1, 2, or 3 pumps, provide fuel oil to emergency diesel engine)
11) Provide actuation or motive power for SC-1, 2, or 3 equipment
12) Provide information or controls to provide reasonable assurance of capability for manual or automatic actuation of nuclear safety functions required of SC-1, SC-2, or SC-3 equipment
13) Supply or process signals or supply power required for SC-1, 2, or 3 equipment to perform its required nuclear safety functions
14) Provide a manual or automatic interlock function to provide reasonable assurance that the proper performance of nuclear safety functions required of SC-1, 2, and 3 equipment is maintained
15) Provide an acceptable environment for SC-1, 2, or 3 equipment and operating personnel

Non-nuclear safety

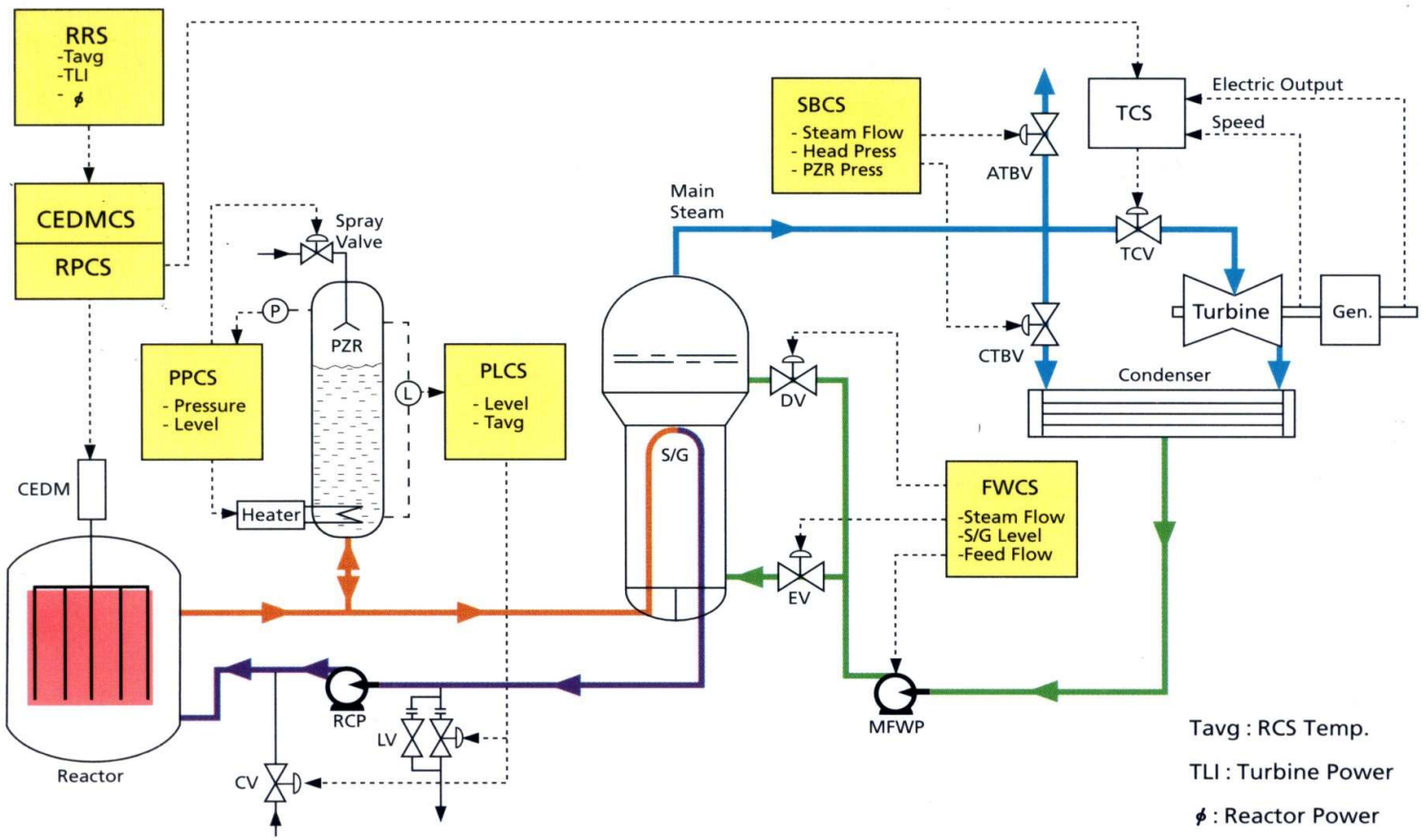
- NNS applies to equipment or structures that are not included in SC-1, SC-2, or SC-3. These items are not relied on to perform a nuclear safety function.

Example of Classification in Safety Analysis Report (APR1400)

SSC Identification	Location[2]	Safety Class	Quality Group	Codes and Standards	10 CFR 50, App. B[3]	Seismic Category	Remarks
79. RC – Reactor Coolant							
a. Reactor vessel	RCB	SC-1	A	ASME Section III NB-2007 with 2008 addenda	Yes	I	
b. SG (primary/secondary)	RCB	SC-1/ SC-2	A/B	ASME Section III NB-2007 with 2008 addenda ASME Section III NC-2007 with 2008 addenda	Yes	I	(N-1)
c. PZR	RCB	SC-1	A	ASME Section III NB-2007 with 2008 addenda	Yes	I	
d. RCP (RCPB Components)	RCB	SC-1	A	ASME Section III NB-2007 with 2008 addenda	Yes	I	(N-3, 4)
87. SI – Safety Injection							
a. Safety injection pumps	AB	SC-2	B	ASME Section III NC-2007 with 2008 addenda	Yes	I	
b. Safety injection tanks	RCB	SC-2	B	ASME Section III NC-2007 with 2008 addenda	Yes	I	
c. Safety injection filling tank	AB	NNS	D	ASME Section VIII-2007 with 2008 addenda	N/A	III	
d. Piping and valves							
1) SIP miniflow line (from SIP orifice or SI-218, 219, 254, 255 to IRWST)	AB	SC-2	B	ASME Section III NC-2007 with 2008 addenda	Yes	I	

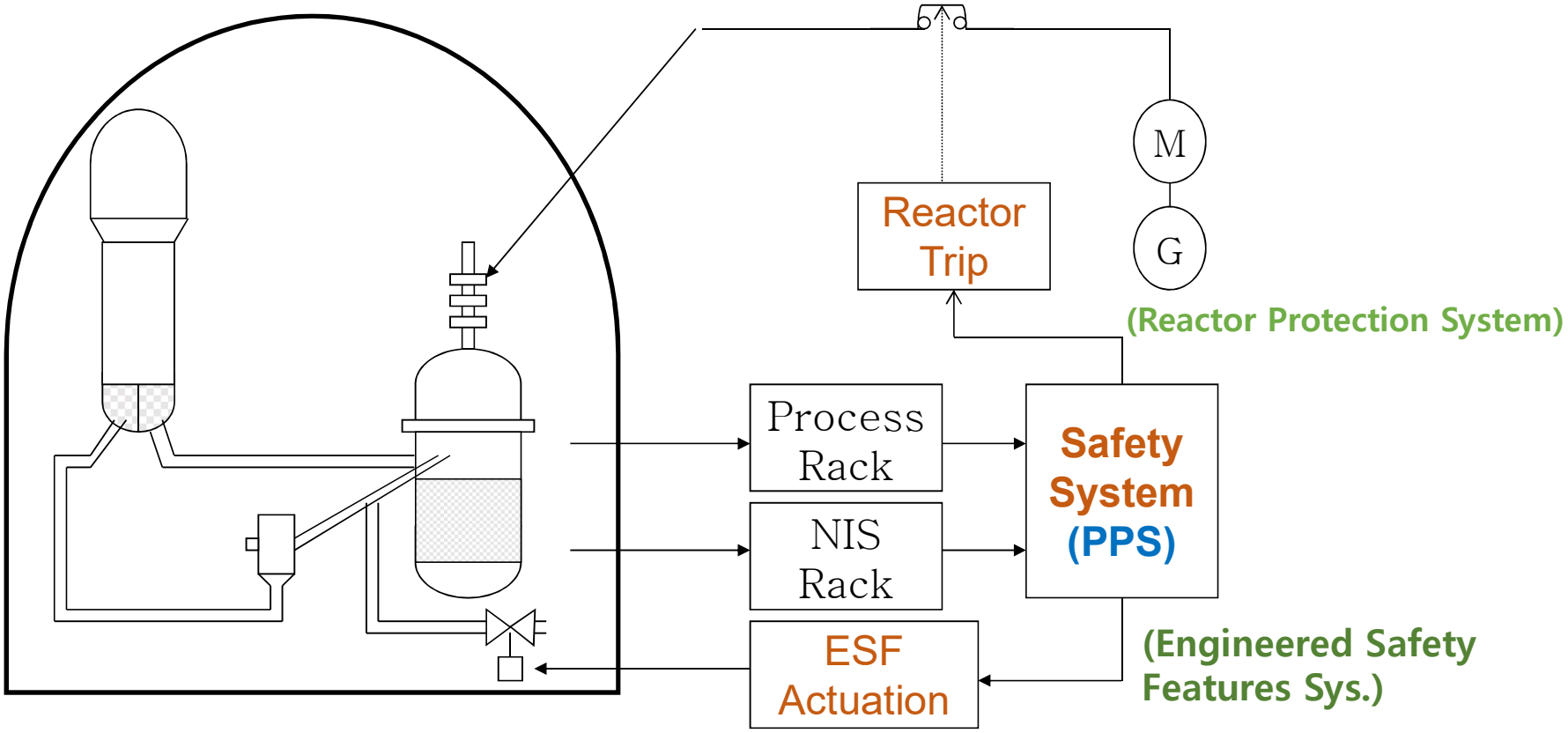
Simplified Plant Control System

- SBCS : Steam Bypass Control Sys.
- FWCS : Feedwater Control Sys.
- RPCS : Reactor Power Cutback Sys.
- PPCS : Pressurizer Pressure Control Sys.
- PLCS : Pressurizer Level Control Sys.
- RRS : Reactor Regulating Sys.



Adopted from KINS-K.A.CARE Training Material (W. Kim)

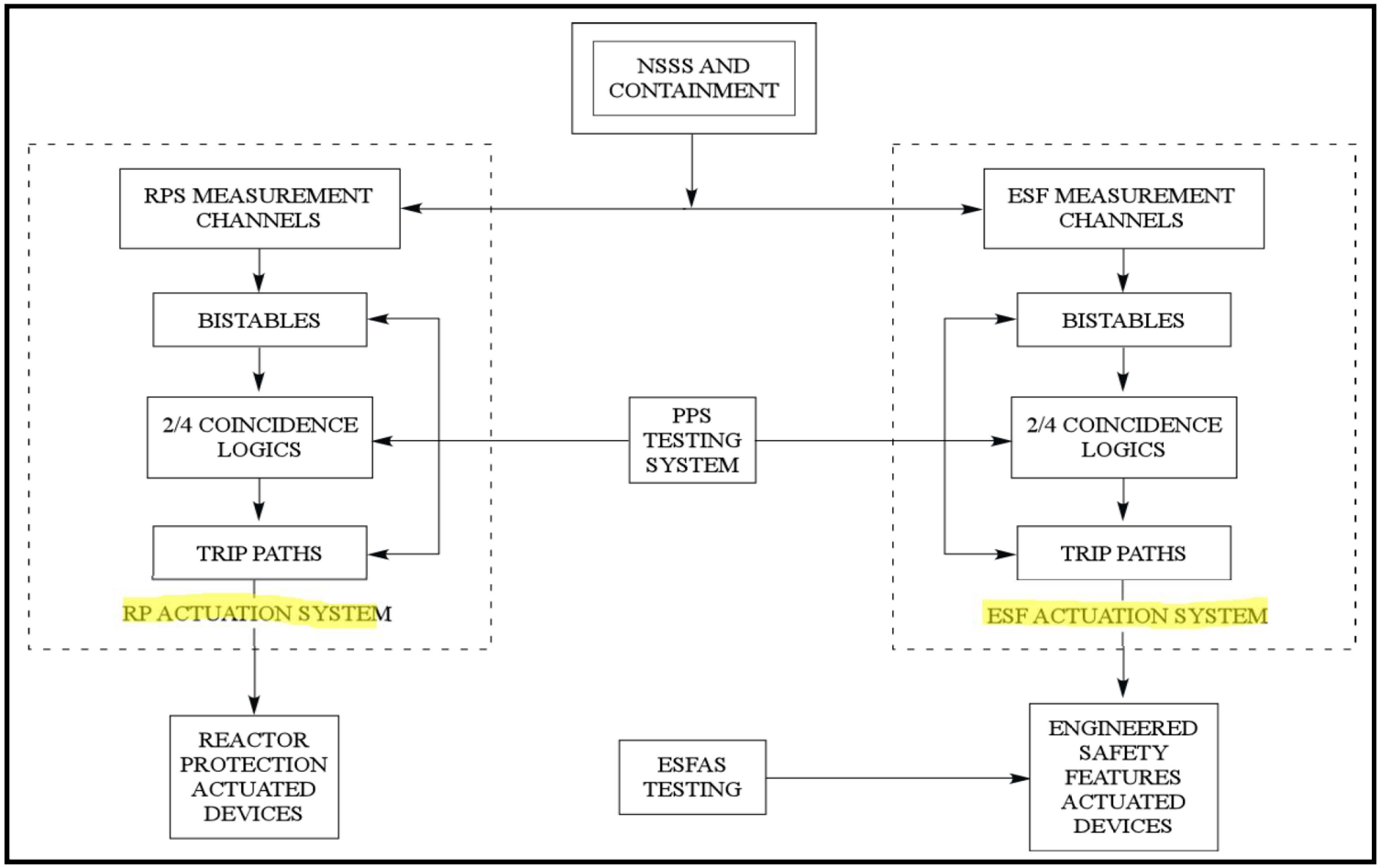
Block Diagram of Plant Protection Systems



[Protection Scheme]

Adopted from KINS-K.A.CARE Training Material(B.Kim)

Configuration of Plant Protection Systems



Reactor Shutdown

Engineered Safety Features Actuation

Adopted from KINS-K.A.CARE Training Material(B.Kim)

Typical RPS Trip Variables and Functions(1)

No	Trip parameters	Coincidence	Setpoint(LSSS)	Functions
1	PZR Pressure - High	2/4	167.55 kg/cm^{2}a (2,384 psia)	To help ensure the integrity of RCS boundary
2	PZR Pressure - Low		124.47 kg/cm^{2}a~7.0 kg/cm^{2}a , Variable STEP : 28.1kg/cm^{2}a	To prevent the DNB. If PZR pressure is bellow the setpoint (28.1kg/cm^{2}a), bypass may be manually initiate. If PZR pressure is above the setpoint (35kg/cm^{2}a), bypass is removed automatically.
3	S/G Level - Low		42.8% (WR)	To prevent the RCS overpressure in the event of a reduction of S/G water inventory
4	S/G Level - High		93%(NR)	To protect turbine from S/G moisture
5	S/G Pressure - Low		62.504 kg/cm^{2}a ~ 0, Variable STEP:14.1kg/cm^{2}a	To prevent RCS overcooling

Adopted from KINS-K.A.CARE Training Material(B.Kim)

Typical RPS Trip Variables and Functions(2)

No	Trip parameters	Coincidence	Setpoints(LSSS)	Function
6	Containment Pressure - High	2/4	133.75 cmH_2O (1.9 psig)	To help ensure the integrity of containment design pressure
7	Reactor Coolant Flow –Low (Rate)		0.030 psi/sec (2.1 cmH_2O)	To prevent DNB
	Reactor Coolant Flow –Low (Floor)		10.69 psid (752.8 cmH_2O)	
	Reactor Coolant Flow –Low (Band)		8.87 psid (624.8 cmH_2O)	
8	Local Power Density - High		21.0 kW/ft (689.0 W/cm)	To protect fuel. If power is below the setpoint(10^{-4}%), bypass is available.
9	DNBR - Low		1.30	To protect fuel and prevent DNB. If power is below the setpoint (10^{-4}%), bypass is available.

Adopted from KINS-K.A.CARE Training Material(B.Kim)

Typical RPS Trip Variables and Functions(3)

No	Trip parameters	Coincidence	Setpoints(LSSS)	Functions
10	Variable Overpower (Rate)	2/4	14.6%/min F.P	To prevent overpower
	Variable Overpower (Ceiling)		109.4% F.P	
	Variable Overpower (Band)		13.6% F.P	
11	Logarithmic Power Level - High		0.018% F.P	To prevent the unplanned criticality from a shutdown condition. If power is above the setpoint(0.001%), bypass is available.
12	Manual			Manual reactor trip

Adopted from KINS-K.A.CARE Training Material(B.Kim)

Approach for Safe Operation during NO & AOOs

- **OLC(Operational Limits and Condition) : Technical Specifications**
  - Controls the operation of the installation
  - Derived from the safety analysis, which identify safe boundaries of operation.
  - OLCs elements closely interrelated
  - Defines operational requirements
    - to ensure that safety systems perform the necessary functions in all operational states and also in DBAs.

- **Typical elements of OLC**
  - Safety limits(SL) : the ultimate boundary of the safe conditions
  - Limiting safety system settings(LSSS),
  - Limits and conditions for normal operation(LCO),
  - Surveillance requirements(SR),
  - Action Statements for deviations from the OLCs (Actions)

(Example) SL for APR1400
(from Docu. of NRC Design Certificate)

2.0 SAFETY LIMITS (SLs)

2.1 SLs

MODE	TITLE	REACTIVITY CONDITION (k_{eff})	% RATED THERMAL POWER[a]	AVERAGE REACTOR COOLANT TEMPERATURE (°F)
1	Power Operation	≥ 0.99	> 5	NA
2	Startup	≥ 0.99	≤ 5	NA
3	Hot Standby	< 0.99	NA	≥ [350]
4	Hot Shutdown[b]	< 0.99	NA	[350] > T_{avg} > [200]
5	Cold Shutdown[b]	< 0.99	NA	≤ [200]
6	Refueling[c]	NA	NA	NA

2.1.1 Reactor Core SLs

2.1.1.1 In MODES 1 and 2, the departure from nucleate boiling ratio (DNBR) shall be maintained ≥ 1.29.

2.1.1.2 In MODES 1 and 2, the peak fuel centerline temperature shall be maintained at < 2,804.4°C (5,080°F), decreasing by 32.2°C (58°F) per 10,000 MWD/MTU for burnup and adjusted for burnable poison per CENPD-275-P, Revision 1-P-A.

2.1.2 Reactor Coolant System (RCS) Pressure SL

In MODES 1, 2, 3, 4 and 5, the RCS pressure shall be maintained ≤ 193.3 kg/cm^{2}A (2,750 psia).

Technical Specifications (Example-1)

3.4 REACTOR COOLANT SYSTEM (RCS)

3.4.1 RCS Pressure, Temperature, and Flow Limits

LCO 3.4.1 RCS departure from nucleate boiling (DNB) parameters for pressurizer pressure, cold leg temperature (T_{cold}), and RCS total flow rate shall be within the limits specified below:

a. Pressurizer pressure ≥ 154.7 kg/cm^{2}A (2,201 psia) and ≤ 161.6 kg/cm^{2}A (2,299 psia);

b. T_{cold} ≥ 286.7°C (548°F) and ≤ 293.3°C (560°F) for THERMAL POWER < 90% RTP,

c. T_{cold} ≥ 289.4°C (553°F) and ≤ 293.3°C (560°F) for THERMAL POWER ≥ 90% RTP; and

d. RCS total flow rate ≥ 75.6E6 kg/hr (166.6E6 lb/hr).

APPLICABILITY: MODES 1 and 2 for pressurizer pressure,
MODE 1 for T_{cold},
MODE 2 with k_{eff} ≥ 1.0 for T_{cold},
MODE 1 for RCS total flow rate.

MODE	TITLE	REACTIVITY CONDITION (k_{eff})	% RATED THERMAL POWER[a]	AVERAGE REACTOR COOLANT TEMPERATURE (°F)
1	Power Operation	≥ 0.99	> 5	NA
2	Startup	≥ 0.99	≤ 5	NA
3	Hot Standby	< 0.99	NA	≥ [350]
4	Hot Shutdown[b]	< 0.99	NA	[350] > T_{avg} > [200]
5	Cold Shutdown[b]	< 0.99	NA	≤ [200]
6	Refueling[c]	NA	NA	NA

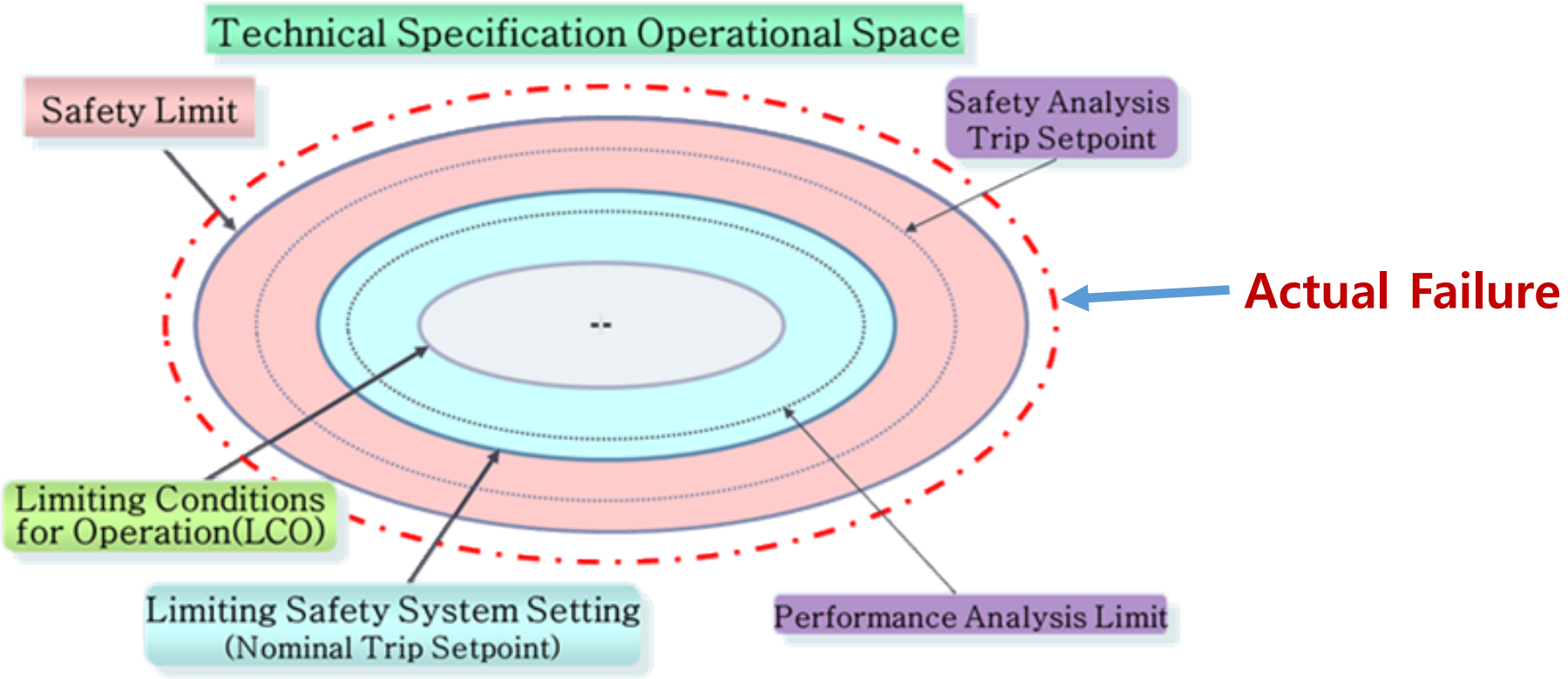
ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. RCS total flow rate not within limits.	A.1	Restore RCS total flow rate to within limits.	2 hours

SURVEILLANCE REQUIREMENTS

SURVEILLANCE		FREQUENCY
SR 3.4.1.1	Verify pressurizer pressure ≥ 154.7 kg/cm^{2}A (2,201 psia) and ≤ 161.6 kg/cm^{2}A (2,299 psia).	12 hours
SR 3.4.1.3	Verify RCS total flow rate ≥ 75.6E6 kg/hr (166.6E6 lb/hr).	12 hours

Safety Margin in Operation



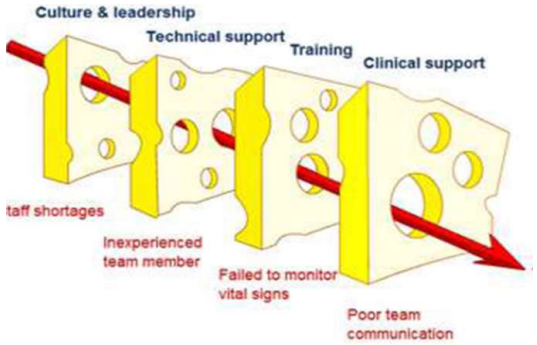
Safe Operation during NO & AOOs

- SSC Integrity ← Design, Manufacturing, Inspection…
- Plant Control ← PCSs, Operational Margin, Operator's Quality
- Operational Limit ← TS (**SL**, LCO, LSSS, SR, Action)

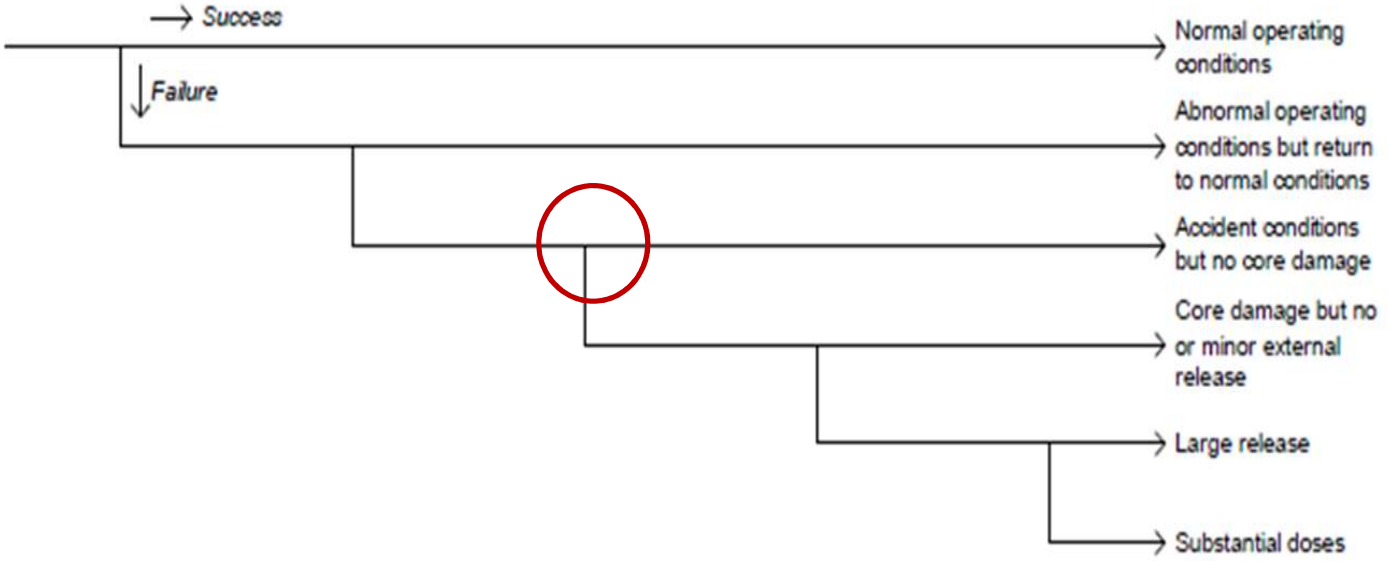
Fundamental Safety Functions

- **Reactivity**
- **Cooling**
- **Confinement**

DiD Levels and Relationship with Plant States



DID level 1 Prevention of abnormal operation and failures	DID level 2 Control of abnormal operation and detection of failures	DID level 3 Control of accidents within the design basis	DID level 4 Severe accident management (DEC)	DID level 5 Mitigation of the radiological consequences	Consequence



DID Level and Essential Means (IAEA TECDOC-1791(2016))

Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
Level 1 (NO)	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1 (NO)
Level 2 (AOO)	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures	(AOO) Level 2
3a (DBA)	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures	Level 3 (DBA)
Level 3 3b (DEC-a)	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without core melting	Emergency operating procedures	4a (DEC-a)
Level 4 (DEC-b)	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melting. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines	Level 4 4b (DEC-b)
Level 5 (EP)	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	Level 5 (EP)

DBA(SSR-2/1)

- **A set of accidents** that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the NPP to withstand, without acceptable limits for radiation protection being exceeded.
  - 5.24. DBAs shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control DBA conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accidents.
  - 5.25. The design shall be such that for DBA conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all DBAs so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions
  - 5.26. The DBAs shall be analyzed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis.

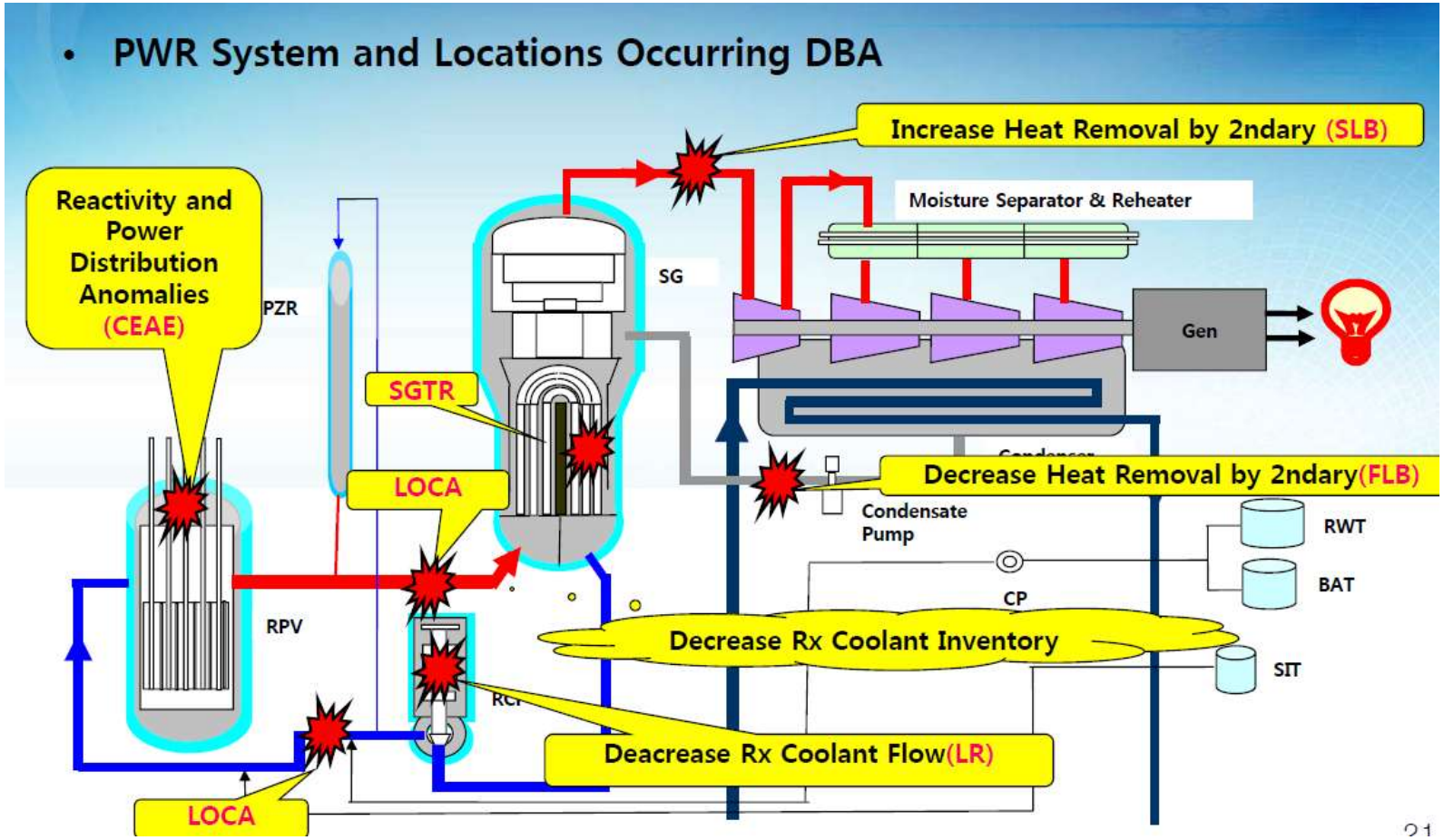
Classification of Initiating Events (by symptom)

- 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
- Increase in reactor coolant inventory
- Decrease in reactor coolant inventory
- Anomalies in distribution of reactivity and power
- Radioactive release from a subsystem or component

Typical DBAs in PWR

- Main Steam Line Break(MSLB)
- Main Feed Line Break (MFLB)
- RCP Shaft Break/Rotor Seizure
- Control Element Assembly Ejection Accident
- Inadvertent opening of Pressure Relief Valve
- Steam Generator Tube Rupture (SGTR)
- Loss of Coolant Accident (LOCA)

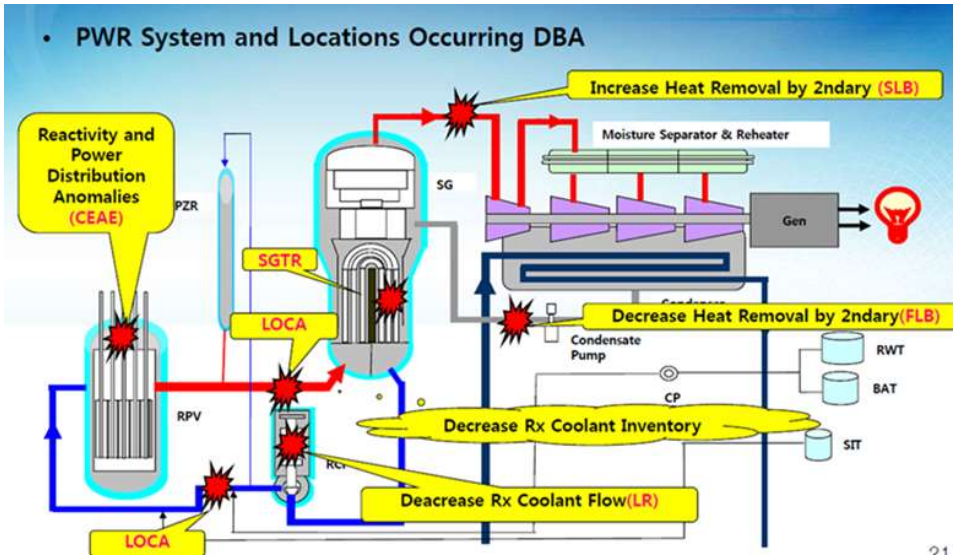
Simplified Figure for Various Initiating Events



IEs in Safety Analysis Report

Initial Events and Frequencies

Section/ Subsection	Event	Frequency of Event
15.1	Increase in heat removal by the secondary system	-
15.1.1	Decrease in feedwater temperature	AOO
15.1.2	Increase in feedwater flow	AOO
15.1.3	Increase in steam flow	AOO
15.1.4	Inadvertent opening of a steam generator relief or safety valve	AOO
15.1.5	Steam system piping failures inside and outside the containment	PA



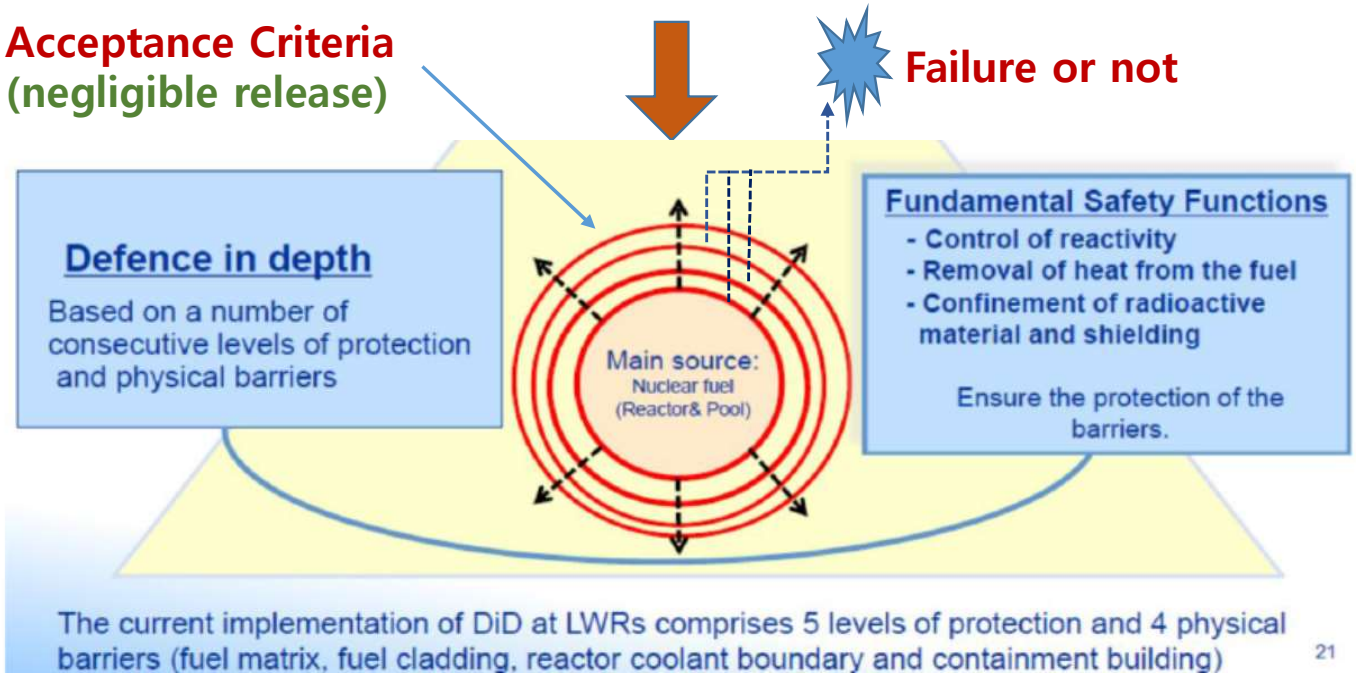
15.6	Decrease in reactor coolant inventory	-
15.6.1	Inadvertent opening of a PWR pressurizer pressure relief valve	PA
15.6.2	Failure of small lines carrying primary coolant outside the containment	AOO
15.6.3	Steam generator tube failure (SGTR)	PA
15.6.4	Radiological consequences of main steam line failure outside the containment (BWR)	N/A
15.6.5	Loss-of-coolant accidents resulting from spectrum of postulated piping breaks within the RCPB (LOCA)	PA

How to prevent escalation of DBA to DEC-B(Core Melt)? (DiD Level-3)

- Design ?
- Operation ?
- Procedures?
- Maintenance & Test ?
- etc ?

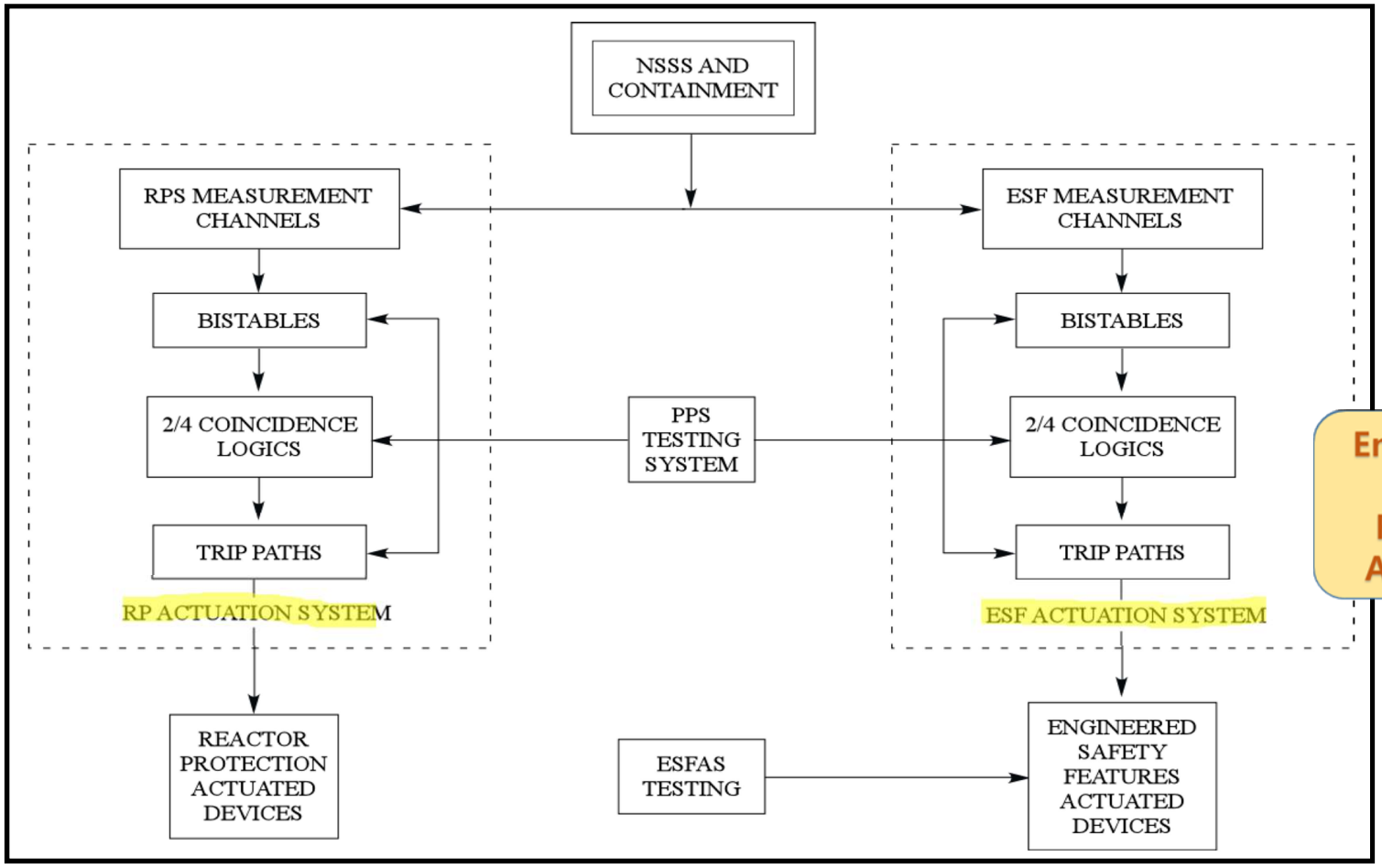
Control of DBAs & Prevention of DEC (DID-3)

- Accident Control ← PPS (RPS, ESF)
- Operation & Procedure ← TS (SL, LCO, LSSS, SR, Actions) , EOP
- Safety Analysis : Deterministic & Probabilistic Approach
- Design of Safety System : ECCS Performance Criteria, Eng. Factors, EQ



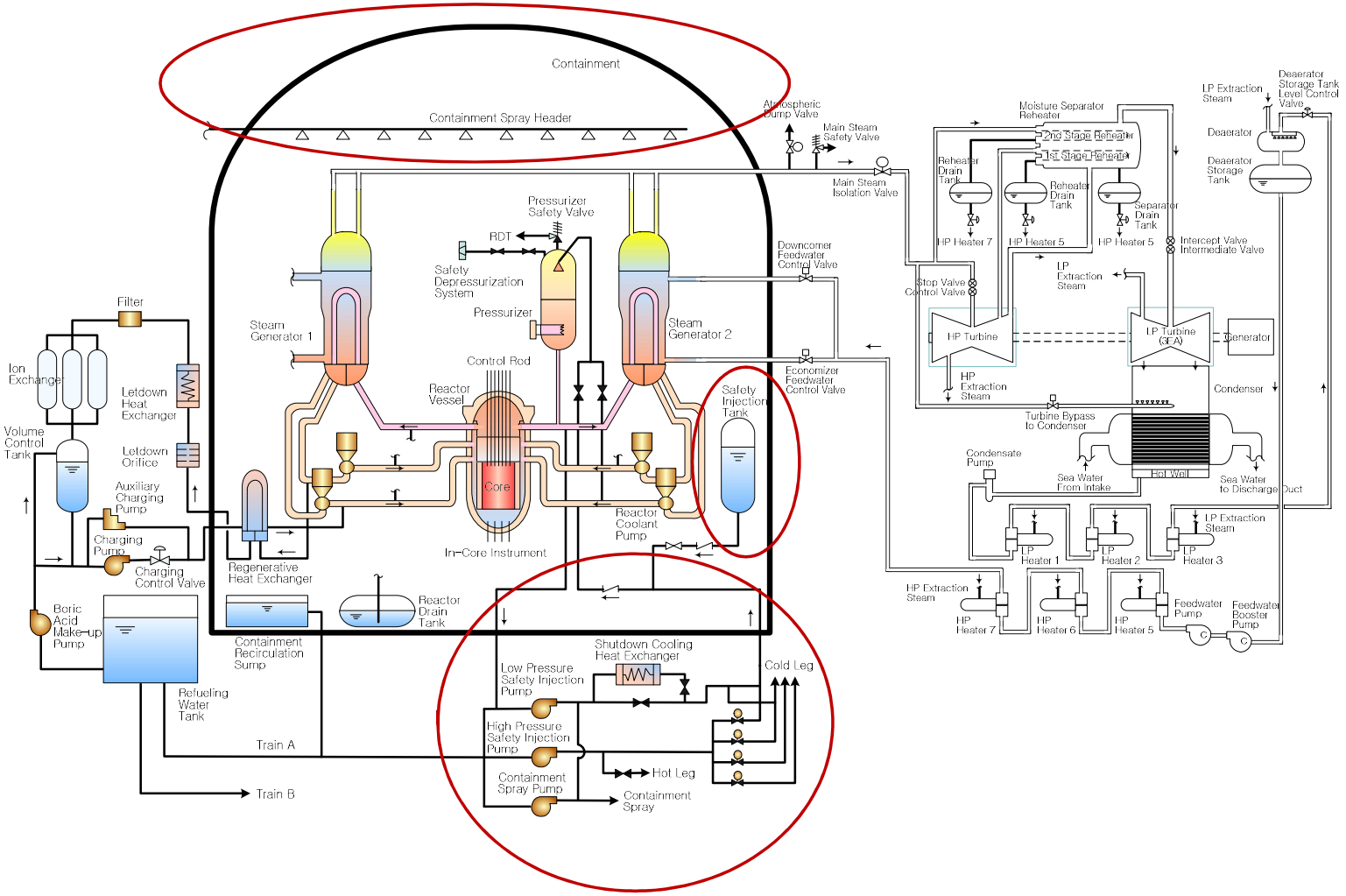
← RPS&ESF

Configuration of Plant Protection Systems



Adopted from KINS-K.A.CARE Training Material(B.Kim)

Plant Overall Configuration of OPR-1000



[Source : KINS-Saudi Training Material]

Engineered Safety Feature (ESF)

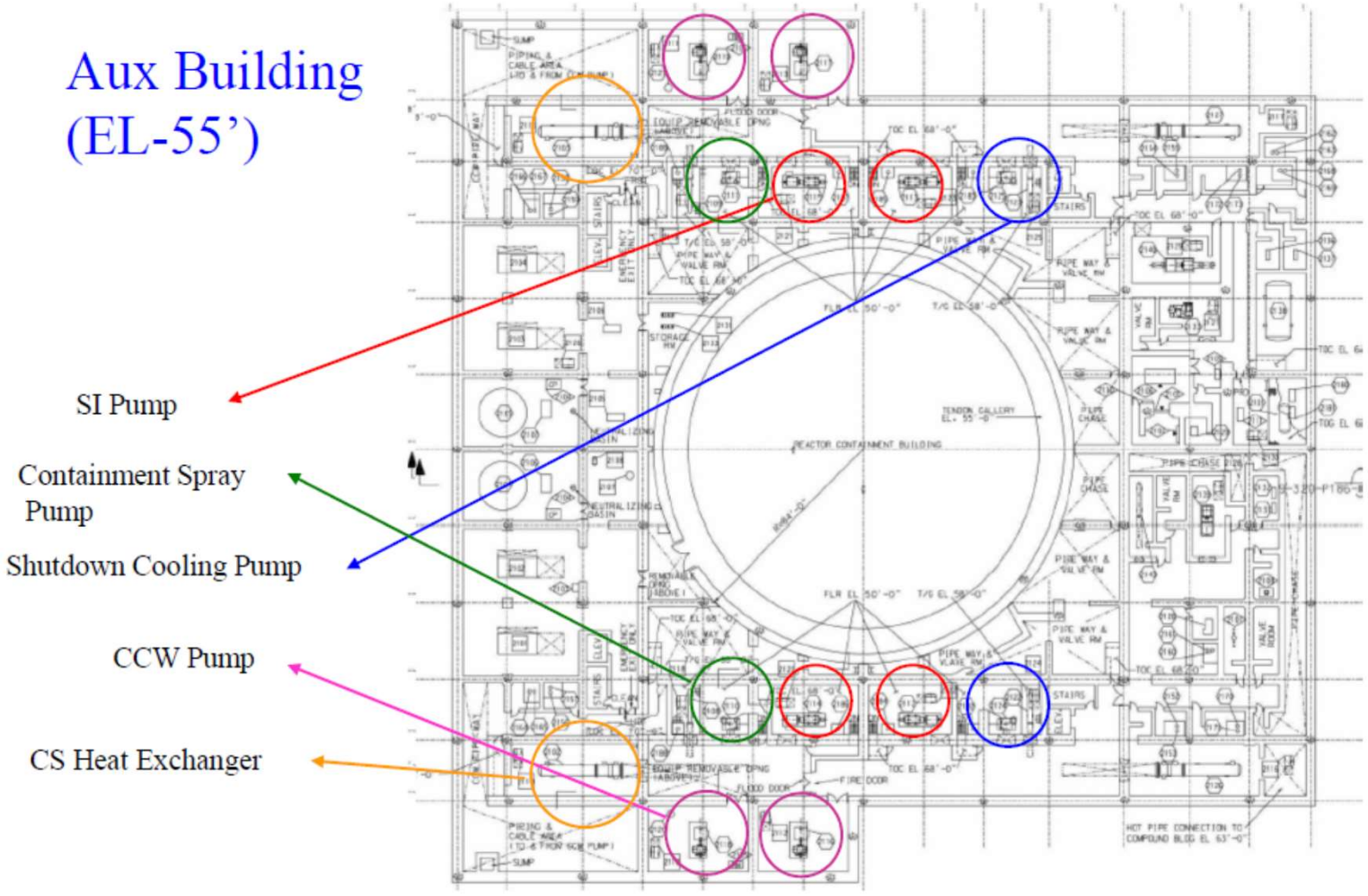
- Purpose
  - To mitigate the consequences of design basis accidents (DBAs) by maintaining long-term core cooling and the integrity of the containment building, and by limiting offsite releases of radioactive materials.
- Engineered basis on any systems, structures, components and provisions ←→ the inherent safety features (MTC etc.)
  - **Emergency Core Cooling System (ECCS)**
    - High Pressure Safety Injection System(HPSIS)/LPSIS
    - Safety Injection Tank(SIT)
  - **Containment System**
    - Containment Spray System
    - Containment Isolation System(CIS)
  - **Auxiliary Feedwater System (AFS)**

Engineered Safety Features(ESF) Actuation Signals

No	ESFAS	Coinci-dence	Input Signals	Setpoint
1	**MSIS** (Main Steam Isolation Signal)	2/4	S/G Pressure - Low	62.504 kg/㎠a(889 psia)
			S/G Level – High (N.R)	93 %
			CV Pressure - High	133.750 cmH_2O(1.9psig)
2	**CIAS** (Cont't Isolation Actuation Signal)		CV Pressure - High	133.750 cmH_2O(1.9psig)
3	**SIAS** (Safety Injection Act. Signal)		PZR Pressure – Low (W.R)	124.47kg/㎠a(1771 psia)
			CV Pressure - High	133.750 cmH_2O(1.9psig)
			PZR Pressure – Low (W.R)	124.47 kg/㎠a(1771 psia)
4	**CSAS** (spray)		CV Pressure – High-High	1421.00 cmH_20 (20.1 psig)
5	**AFAS**-1,2 (Aux. Feed)		S/G Level – Low (W.R)	23.6%
6	**RAS** (Recirculation)		RWT Level – Low	7.7%
7	**MANUAL**		Manual Switches in MCR (A-B, A-D, B-C, C-D) Manual Switches on ESFAS-ARC Cabinet	Manual

Adopted from KINS-K.A.CARE Training Material(B.Kim)

ESF Equipment Arrangement in APR-1400



ECCS Functions

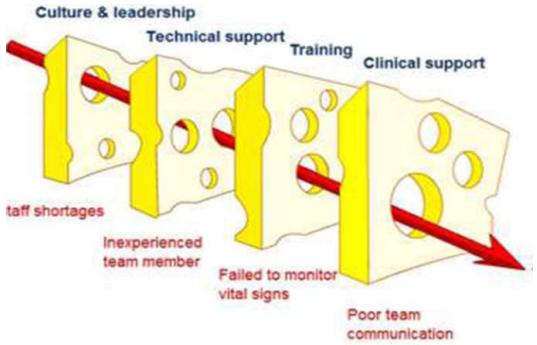
- **Inject borated coolant to reactor core** for emergency core cooling during LOCA to meet the following **Performance Criteria**
  1. Max. fuel clad temp. < 2200 ^{0}F (1,200°C)
  2. Total clad oxidation limit < 17% of clad thickness
  3. Max. hydrogen generation due to water-clad chemical reaction < 1% of max. possible hydrogen reaction
  4. Remain coolable core geometry
  5. Provision for Long-term core cooling

- Provide sufficient borated water to compensate reactivity added by RCS over-cooling; ensure sufficient shutdown margin
- Make up RCS inventory during Steam Generator Tube Rupture
- Provide Feed and Bleed operation during beyond DBA(DEC)

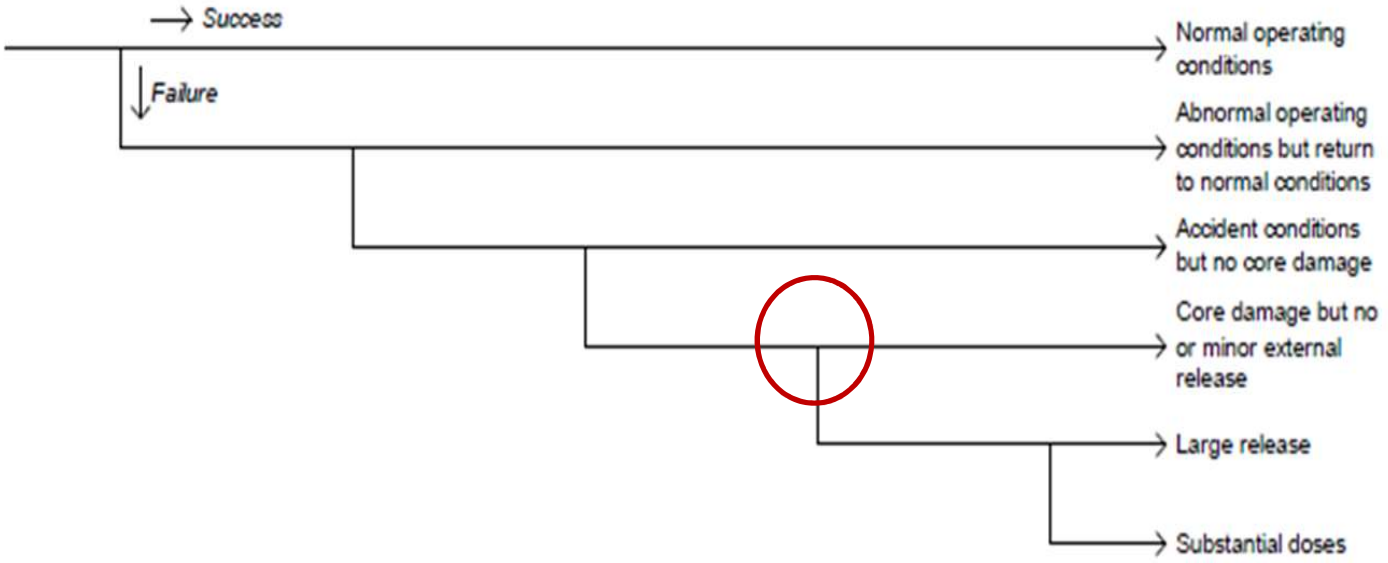
Summary of DBA & DiD Level-3

- **A set of accidents that are to be considered in the design**
  - Shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the NPP to withstand, without acceptable limits for radiation protection being exceeded
- **Essential design means for DiD : Engineered Safety Features**
  - Engineered basis on any systems, structures, components and provisions
    - Emergency core cooling system (ECCS)
    - Containment isolation & spray system (CIS& CSS)
    - Auxiliary feedwater system (AFS)
    - Containment isolation
- **Application to Safety Analysis**
  - DSA : Conservative or Best Estimate approach, Enough margin
  - Performance Criteria for ECCS
    - Prevention of fuel rod damage
    - Coolable Geometry..

DiD Levels and Relationship with Plant States



DID level 1 Prevention of abnormal operation and failures	DID level 2 Control of abnormal operation and detection of failures	DID level 3 Control of accidents within the design basis	DID level 4 Severe accident management (DEC)	DID level 5 Mitigation of the radiological consequences	Consequence



How to mitigate DEC-B (w/ Core Melt)?

- Design ?
- Operation ?
- Procedure?
- Strategy ?
- etc.?

DID Level and Objectives (IAEA TECDOC-1791(2016))

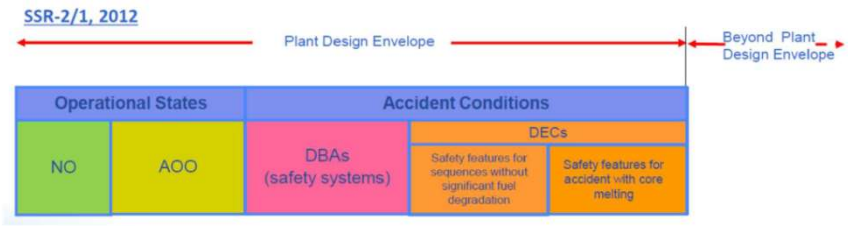
Level of defence Approach 1	Objective	Essential design means	Essential operational means	Level of defence Approach 2
Level 1 (NO)	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures	Level 1 (NO)
Level 2 (AOO)	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures (AOO)	Level 2
3a (DBA)	Control of design basis accidents	Engineered safety features (safety systems)	Emergency operating procedures (DBA)	Level 3
Level 3 (DEC-a) 3b	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without core melting	Emergency operating procedures (DEC-a)	4a Level 4 4b
Level 4 (DEC-b)	Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melting. Technical Support Centre	Complementary emergency operating procedures/ severe accident management guidelines (DEC-b)	
Level 5 (EP)	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans	Level 5 (EP)

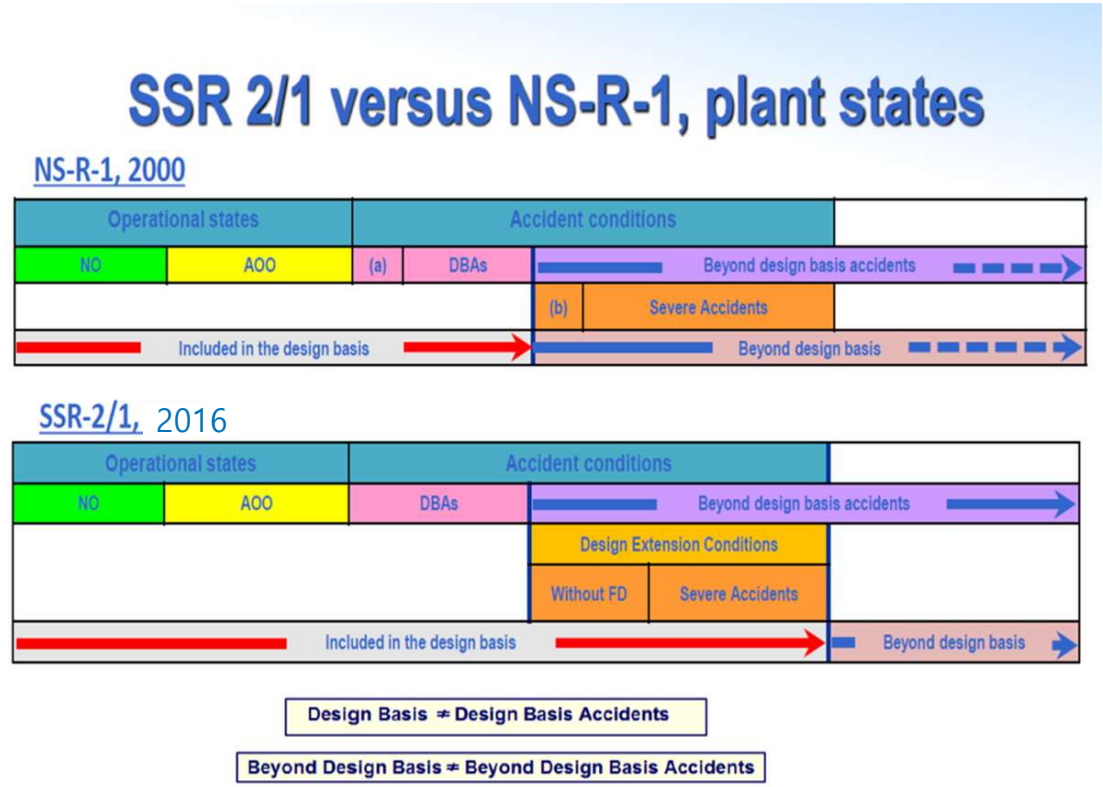
DEC Definition and Types

- **DECs (Design Extension Conditions)**

  - DECs comprise conditions in events
    - without core melt and
    - with core melting (Severe Accident)

  - Postulated accident conditions that are not considered for DBAs , but that are considered in the design process for the facility in accordance with Best Estimate Methodology (or Realistic Approach), and for which releases of radioactive material are kept within acceptable limits.





Identification of DEC w/o Core Melt (1)

- In general, **three types of DECs w/o CM** considered :
  - **Very unlikely events** that could lead to situations beyond the capability of safety systems for DBAs.
  - **Multiple failures** (e.g. CCFs in redundant trains) that prevent the safety systems from performing their intended functions to control the postulated Initiating Events.
    - Ex) LOCA without actuation of a safety injection system. The failures of supporting systems are implicitly included among the causes of failure of safety systems.
  - **Multiple failures that cause the loss of a safety system** while this system is used to fulfil the fundamental safety functions in normal operation.
    - Ex) The same system for the heat removal in accident conditions and during shutdown.(LPSI=SDS)

- **Identification of DECs : use of both deterministic and probabilistic insights**
  - This combination of insights is an effective design technique whether considering the entire NPP design or evaluating a specific safety function such as the containment function.

Identification of DEC w/o Core Melt (2)

- **Deterministically** identified DECs w/o CM through the extensive operating experiences in the light water technology ;
  - ATWS (Anticipated Transient w/o Scram)
  - SBO : LOOP + EDGs failure
  - Loss of core cooling in the residual heat removal mode
  - Extended loss of cooling of fuel pool and inventory
  - Loss of normal access to the ultimate heat sink

- **Probabilistically** identified DEC w/o CM through PSA (ET & FT) ;
  - Total loss of feed water
  - LOCA plus loss of one ECCS (either HPSI or LPSI)
  - Loss of the component cooling water system(CCWS) or the essential service water system (ESWS)
  - Uncontrolled boron dilution
  - Multiple steam generator tube ruptures (MSGTR)
  - Steam generator tube ruptures induced by main steam line break (MSLB)
  - Uncontrolled level drop during mid-loop operation (for PWRs) or during refuelling.

DEC with Core Melt (Severe Accident)

- The progression of a severe accident involves a highly complex set of physical and chemical phenomena in reactor and containment
  - It is necessary to select a representative group of severe accident conditions to be used for defining the design basis of the mitigative safety features for these conditions.

- The features for the mitigation of DEC with CM are such to prevent that those severe accident phenomena
  - Hydrogen detonation
  - Basemat melt through due to core-concrete interaction
  - Steam explosions
  - Loss of containment integrity

- For DECs with CM, maintaining the containment integrity is the main objective.
  - Also implies that the cooling and stabilization of the molten fuel and the removal of heat from the containment need to be achieved in the long term.

Safety Features for DECs (IAEA SSR-2/1 (2016))

- (5.29) The analysis undertaken shall include identification of the features that are designed for use in, or that are capable of preventing or mitigating, events considered in the DECs.

  - **These features:**
    (a) independent, to the extent practicable, of those used in more frequent accidents;
    (b) capable of performing in the environmental conditions including severe accidents;
    (c) reliability to fulfil the function

- (5.30) In particular, the containment and its safety features shall be able to withstand extreme scenarios that includes melting of the reactor core.

❖ **(Severe Accident, SSR-2/1(2000))** Consideration shall be given to the plant's full design capabilities, including the possible use of some systems (i.e. safety and non-safety systems) beyond their originally intended function and AOOs, and the use of additional temporary systems, to return the plant to a controlled state and/or to mitigate the consequences of SA.

Acceptance Criteria for DECs

- SSR-2/1 states that
  - 5.31. " the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'."
  - 5.31A. " for DECs, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures."
- Designers and regulators often develop subsidiary objectives in terms of
  - Radiological consequences (effective doses at specific distances from the site boundary) or
  - Containment leak tightness (e.g. leak for 24 hours)

❖ **The definitions below are from SSR-2/1**

- **Early radioactive release**: a release for which off-site protective measures are necessary but unlikely to be fully effective in due time.
- **Large radioactive release**: a release for which off-site protective measures limited in terms of times and area of application are insufficient to protect people and the environment.

Summary of DID Criteria for Plant States(1)

Level of defense	Objective	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 1 (N.O)	Prevention of abnormal operation and failures	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are bounded by the general radiation protection limit for the Public, typically in the order of 0.1 mSv/year
Level 2 (AOO)	Control of abnormal operation and detection of failures	No failure of any of the physical barriers except minor operational leakages	Negligible radiological impact beyond immediate vicinity of the plant. Acceptable effective dose limits are similar as for normal operation, limiting the impact per event and for the period of 1 year following the event (0.1 mSv/y)

Summary of DID Criteria for Plant States(2)

Level of defense	Objective	Criteria for maintaining integrity of barriers	Criteria for limitation of radiological consequences
Level 3 (DBA & DEC-A)	Control of design basis accidents (DBAs)	No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel	No or only minor radiological impact beyond immediate vicinity of the plant, without the need for any off-site emergency actions. Acceptable effective dose limits are typically in the order of few mSv.
Level 4 (DEC-B)	Control of DECs (mitigation of consequences of severe accidents)	Maintaining containment integrity	Only emergency countermeasures that are of limited scope in terms of area and time are necessary (Practical elimination of Large and Early Radioactive Release)
Level 5 (EP)	Mitigation of radiological consequences of significant releases	Containment integrity severely impacted, or containment disabled or bypassed	Off-site radiological impact necessitating emergency countermeasures

Lecture Topics

- Introduction
  - Fundamental Safety Functions
  - Defense in depth (DID)
- Defense-in-Depth Design in Safety
  - DID Levels and Plant States of NPPs
  - DID Implementation into NPPs
- **Overview of Safety Assessment**
  - **Safety Assessment Process**
  - **Main Elements for Safety Assessment**

Safety Assessment

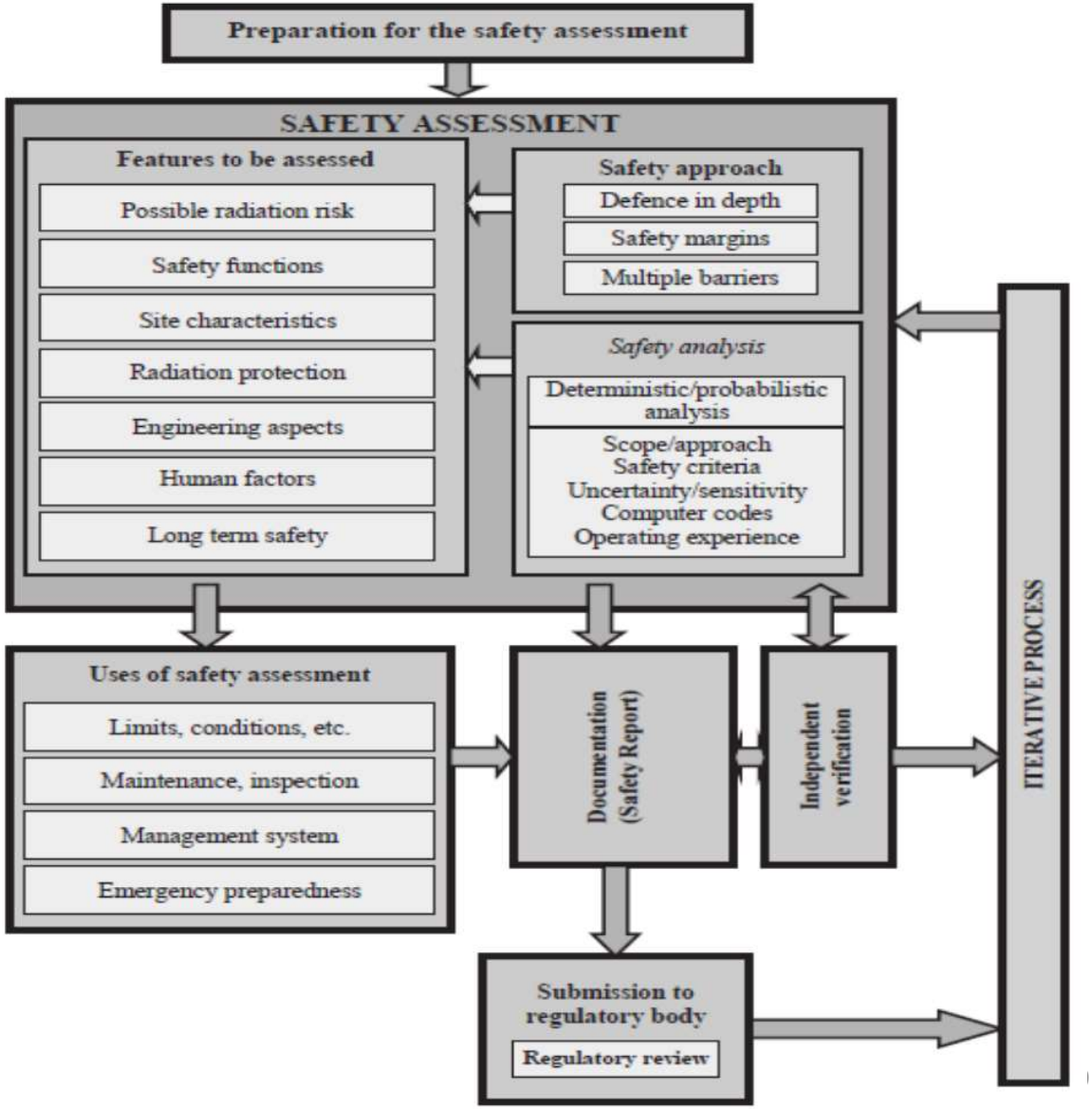
- **Definition**
  - Systematic process
    - to ensure that all the relevant safety requirements are met by the proposed (or actual) design throughout the lifetime of the facility.
  - Safety assessment includes, but is not limited to, the formal safety analysis

- **Purposes**
  - To determine
    - whether an adequate level of safety has been achieved and
    - whether the basic safety objectives and safety criteria are in compliance with the reqirements for protection and safety

- **Responsibility**
  - Carried out and documented by the organization responsible for operating the facility or conducting the activity

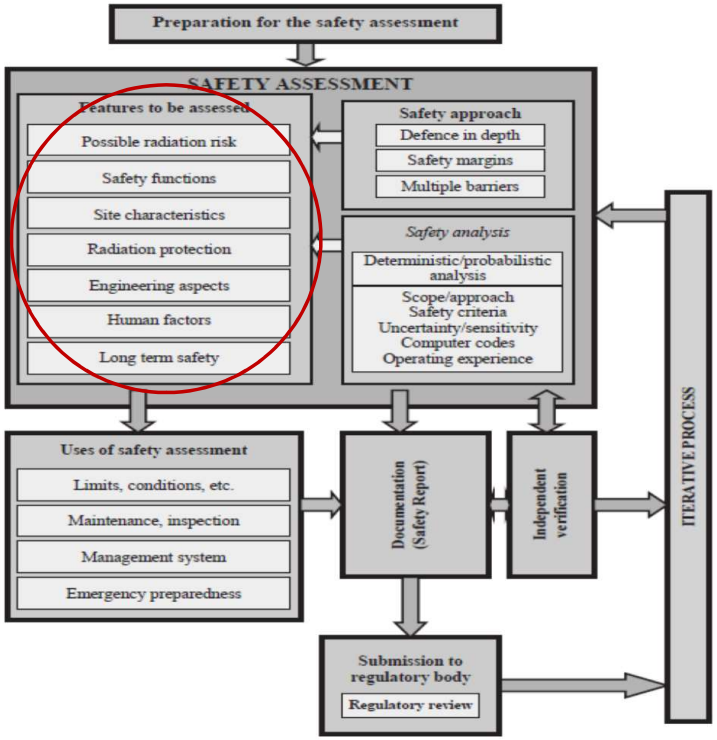
Main Elements of SA

Fig. Overview of the Safety Assessment Process
(IAEA GSR-4)



Features to be assessed

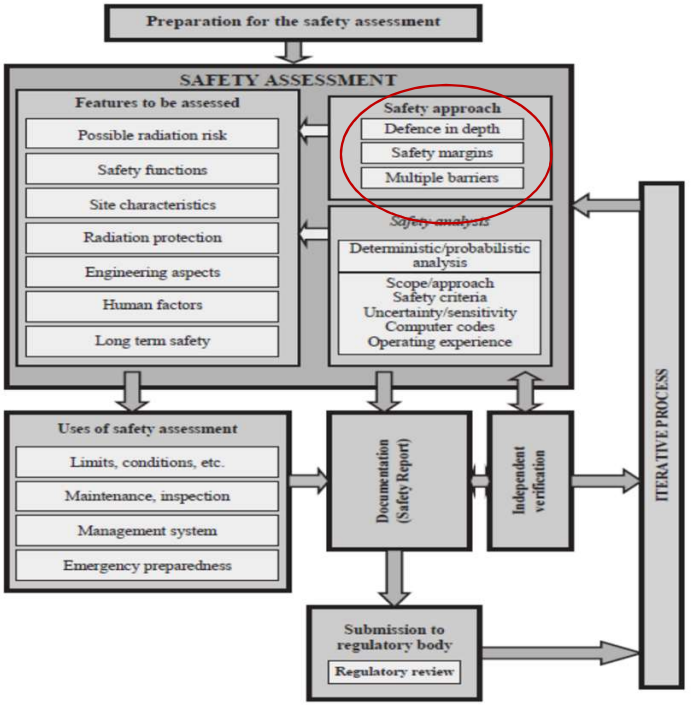
- Possible Radiation Risks
- Safety Functions
- Site Characteristics
- Radiation Protection
- Engineering Aspects
- Human Factors
- Safety over the Lifetime of a Facility



Safety Approach(1)

Defense-in-Depth (DID)

- Whether adequate provisions have been made at each of the levels of DID :
  (a) Address deviations from normal operation
  (b) Detect and terminate safety related deviations from normal operation
  (c) Control accidents within the limits specified in the design;
  (d) Specify measures to mitigate the consequences of accidents that exceed design limits;
  (e) Mitigate radiation risks associated with possible releases of radioactive material



Safety Approach(2)

- **Safety Margin**
  - It shall be determined whether there are adequate safety margins, a wide margin to failure of any SSCs for **the unknown**
  - Adequacy of safety margins and their acceptance shall be determined through the safety analysis.
  - Where practicable, the safety assessment shall confirm that there are adequate margins to avoid cliff edge effects that would have unacceptable consequences.

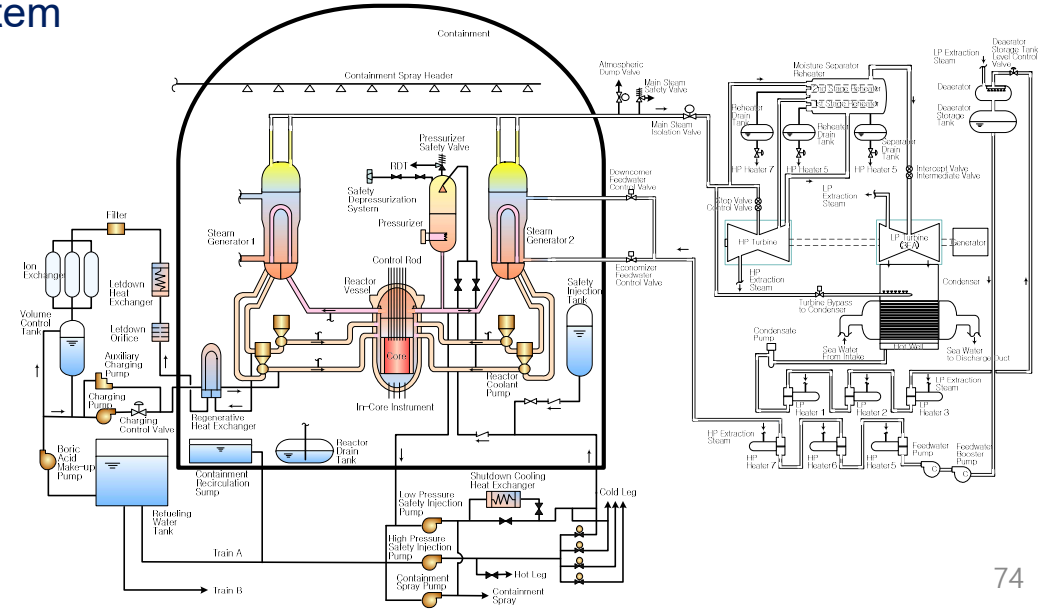
❖ *A 'cliff edge effect' is an instance of severely abnormal conditions caused by an abrupt transition from one status of a facility to another following a small deviation in a parameter or a small variation in an input value*

Safety Analysis

- **Scope of the safety analysis**
  - **Safety analysis** : the evaluation of the potential hazards associated with a facility or an activity.
  - shall address the consequences arising from all conditions in normal operation (including startup and shutdown) and the frequencies and consequences associated with all AOOs and accident conditions.
  - Both **deterministic and probabilistic** approaches shall be included in the safety analysis.

Documentation of SA -Safety Analysis Report (Prepared by Designer /Operator)

Chapter 1 - Introduction and General Description of Plant
Chapter 2 - Sites Characteristics
Chapter 3 - Design of Structures, Components, Equipment, and Systems
Chapter 4 - Reactor
Chapter 5 - Reactor Coolant System and Connected Systems
Chapter 6 - Engineered Safety Features
Chapter 7 - Instrumentation and Controls
Chapter 8 - Electric Power
Chapter 9 - Auxiliary Systems
Chapter 10 - Steam and Power Conversion System
Chapter 11 - Radioactive Waste Management
Chapter 12 - Radiation Protection
Chapter 13 - Conduct of Operations
Chapter 14 - Initial Test Program
Chapter 15 - Accident Analysis
Chapter 16 - Technical Specifications
Chapter 17 - Quality Assurance
Chapter 18 - Human Factors Engineering
(Chapter 19 - PSA and Severe Accidents)



Reference Materials

- IAEA Documentation
  - INSAG-3, Basic Safety Principles for Nuclear Power Plants (1988)
  - INSAG-10, Defense in Depth in Nuclear Safety (1996)
  - INSAG-12, Basic Safety Principles for Nuclear Power Plants (Rev.1 of INSAG-3, 1999)
  - Safety Standards SF-1, Safety Fundamentals (2006 ed.)
  - Safety Standards GSR-4, Safety Assessment of Nuclear Facilities and Activities (Rev.1, 2016)
  - Safety Standards SSR-2/1, Safety of NPPs : Design(Rev.1, 2016)
  - Safety Reports Series, No.46, Assessment of Defense-in-Depth for NPPs(2005)

- USNRC, NUREG/KM-0009, Historical Review and Observations of Defense-in-Depth (2016)
- USNRC, NUREG/CR-6042, Perspectives on Reactor Safety (2002)