Nuclear Safety

Module 3

DEFENSE IN DEPTH

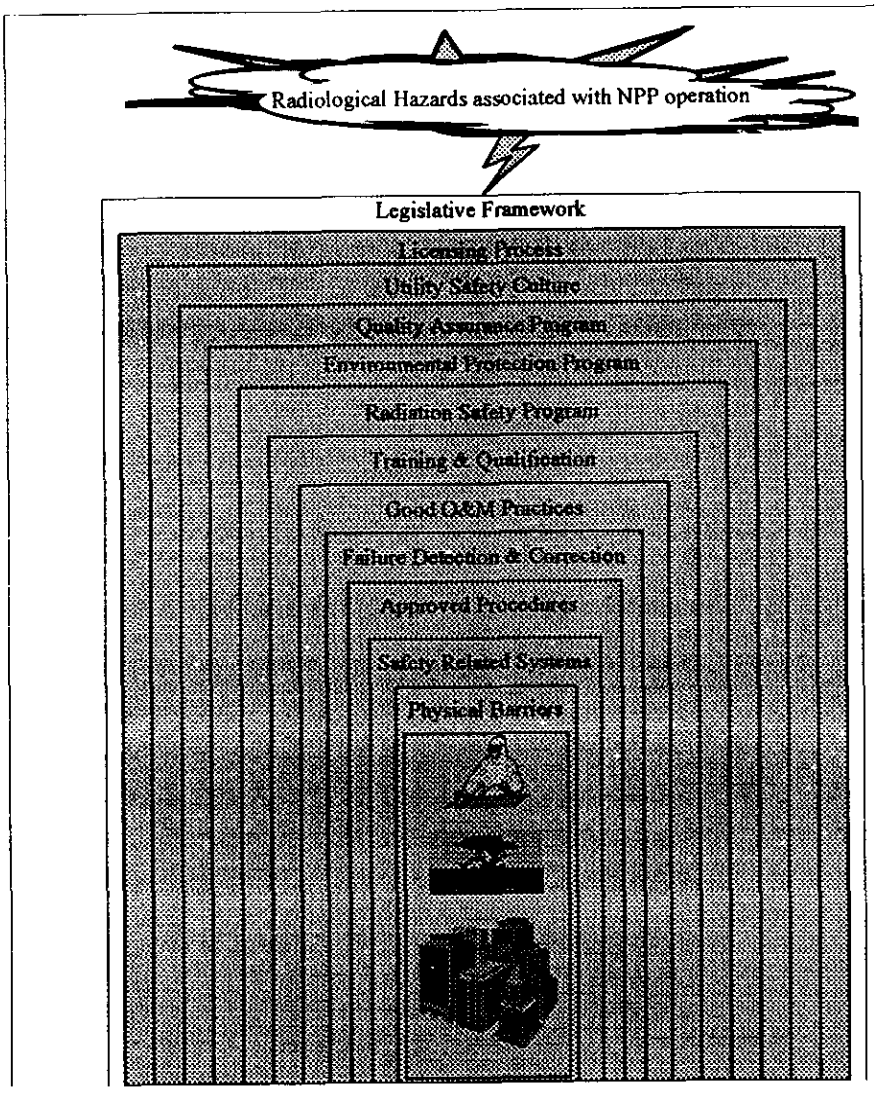
Defense in Depth

The principle that multiple, redundant nuclear safety provisions are required to protect workers, the public and the environment from the radiological hazards of NPP operations.

Assumptions Inherent in Defense in Depth Safety Philosophy

1. People make mistakes
2. Design isn't perfect
3. Equipment fails

Safety Culture Model



Defense in Depth in Accident Management

1) **Accident prevention**
2) **Accident mitigation**
3) **Accident management**

Defense in Depth in Accident Management

1) Accident prevention

- quality design, procurement, construction, *operations and maintenance for reliable systems*
- faults detected and corrected promptly
- when systems fail, upsets prevented from escalating
  - » automatic system response
  - » unit placed in safe state by well-trained staff using approved procedures
- standby safety support systems

Defense in Depth in Accident Management

2) **Accident mitigation**

- shut down, cool, contain (via special safety systems, for serious process failures)
- AIM procedures executed by trained staff

Defense in Depth in Accident Management

3) Accident accommodation

- emergency response procedures executed by trained staff
- public notifications and protective measures
  - » eg, banning food & water, sheltering, evacuation, KI pills
- Province, Municipalities and Federal Govt. respond per Nuclear Emergency Plans

Maintenance on Safety Related Systems

- O&M activities on safety related systems can impair or remove a layer of defense
- Then countermeasures are required to compensate for the increased risk
  - *Example 1*: Quiet mode operation to reduce probability of upset
  - *Example 2*: Synchronizing SG to class 3 bus to increase reliability
  - *Example 3*: Dedicated Operator when placing one liquid zone on manual control

Why Use Approved Procedures?

- Extra layers of defense provided
- Technical and Operational reviews ensure that:
  - potential effects on other systems have been considered
  - barriers to releasing radioactivity are not compromised
  - procedures addressing system failures really do put unit into a safe state

Defense in Depth in Event Diagnosis

- Operator training (classroom, field, simulator, co-piloting)
- Diagnostic aids (eg, CSP display, PRAG)
- Independent diagnosis by SOS and SS
- Monitoring critical safety parameters during recovery to ensure that unit is responding predictably, consistent with diagnosis

Placing an Automated Control System on Manual Control

- Observe similar constraints as designed into automated system
- Dedicate an Operator where appropriate, to simulate the 'undistracted' operation of the automatic controller--eg, controlling one liquid zone level

Role of Training & Qualification in Defense in Depth

Equips staff to:

- recognize when a layer of defense is jeopardized
- perform critical O&M activities safely--eg,
  - Instrument calibration
  - Safety system testing
  - Panel checks
- identify equipment failures at incipient stage
- execute emergency procedures safely

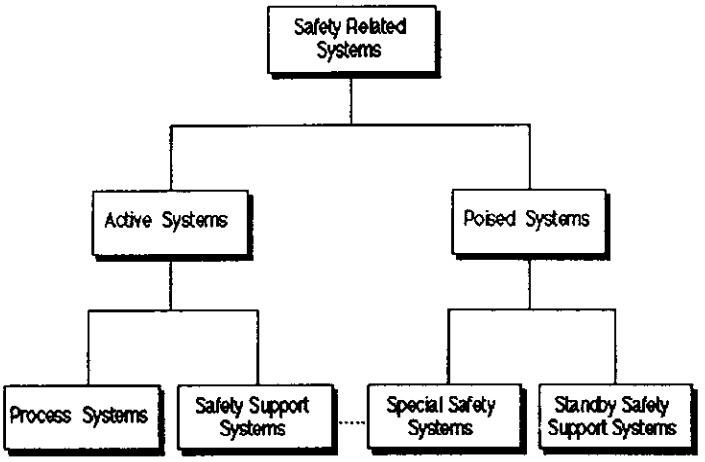
The 5 Barriers between Fission Products and the Public

1. Ceramic fuel
2. Fuel sheath
3. HTS boundary
4. Containment
5. Exclusion zone

Impact of Large Scale Fuel Failures on the Five Physical Barriers

- At least 2 barriers breached (ceramic and sheath)
- In event of a LOCA, third barrier (HTS boundary) also breached
- In event of a dual failure, fourth barrier (Containment) also breached

Classification of Safety Related Systems



Examples of Active and Passive Systems

Process System	Safety Support System	Special Safety System	Standby Safety Support System
• PHT	• Electrical power	• SDS1	• Steam Gen./Boiler Emergency Cooling
• Mod. Aux.	• Process water	• SDS2	• Standby generators
	• Instrument air	• ECI	• Containment venting
	• Backup heat sinks	• Containment	• Setback and stepback
	• Secondary control area		• Emergency water
	• Annulus gas		• Emergency power
	• PHT		• Secondary control areas
	• Moderator		• Backup heat sinks

Trip and Safety Margins