Idaho National Laboratory

MODULE B

Traditional Engineering Analysis and PRA Approaches To Safety Analysis

Traditional Engineering Analysis And PRA Approaches To Safety Analysis

- **Purpose**
  - **This module compares and contrasts the traditional engineering and PRA approaches to safety analysis**

Objectives

- **Upon completion of this module, students should be able to**
  - **Describe the traditional engineering approach to control risk**
  - **Compare and contrast this approach with that used in PRA**
  - **Give examples of how defense-in-depth is included in the design the traditional approach, and how PRA illustrates the level of protection provided by design**

Outline

- Design Basis Approach to Risk
- Role of Defense-in-Depth in Design
- Limitations of the Traditional Approach
- The PRA Approach to Assessing Risk
- How PRA Illustrates Defense-in-Depth

Design Basis (Traditional) Approach to Risk

- Focused on setting design requirements
- Specific accidents to be analyzed and designed for [Design Basis Accidents (DBAs)]
- Includes worse-case single active failure
- Only safety-related equipment is credited
- Operator actions generally not included
- Includes margins to address uncertainties

Design Basis (Traditional) Approach to Risk: (cont.)

- Establishes requirements for
  - Engineering margin
  - Quality assurance
  - Analysis methodology
- Requires redundancy and separation for critical systems
- Establishes principles for Defense-in-Depth

Defense-In-Depth Provides Barriers Physical, Procedural, Organizational) To Fission Product Release And Layers Of Protection

Layers of Defense in Depth
(Establishes Design & Operational Requirements)

Layers of defense in depth	Objective	Approach
1	Prevention of abnormal operation and failures	Training, conservative design (redundancy, engineering margin) and high quality in construction and operation
2	Control of abnormal operation and detection of failures	Control, limiting, and protection systems and other surveillance features
3	Control of accidents within the design basis	Engineered safety features and emergency operating procedures
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Accident mitigation strategies
5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

Examples of Layer 1 Barriers and Layer of Protection Prevention of Abnormal Operation and Failures

Ceramic fuel pellets	Only a fraction of gaseous and volatile fission products is released from the pellets
Metal cladding	Cladding contains fission products from the pellets
Reactor vessel and piping	Contains fission products & other radioactive materials
Procedures	Plant/Unit operating procedures, system operating procedures, surveillance procedures
Fire prevention	Fire prevention program required - e.g. restricting storage/use of flammable materials, good electrical practice

Examples of Layer 2 Barriers and Layer of Protection Control of Abnormal Operation and Detection of Failures

Metal cladding	<0.5% of fuel pins permitted to develop pinhole sized leaks over life of fuel
Reactor vessel and piping	Leak detection system and In-Service Inspection required
Reactor Control System	Shutdown response to certain abnormal conditions
Fire detection	Detection systems required
Tech Specs	Limiting safety system settings
Procedures	Abnormal operating procedures reduce human error

Examples of Layer 3 Barriers and Layer of Protection Control of Accidents within the Design Basis

RPS	Limits energy deposition of accidents
ECCS	Protects cladding integrity
Procedures	Emergency operating procedures reduce human errors
Fire control	Fire suppression systems are required
Reactor vessel and piping	8- to 10-inch thick steel vessel and 3- to 4-inch thick steel piping contain reactor coolant and any fission products released from the fuel cladding

Examples of Layer 4 Barriers and Layer of Protection

Control of Severe Plant Conditions, Including Prevention of Accident Progression and Mitigation of the Consequences of Severe Accidents

Containment	Contains any fission products released from the reactor vessel or coolant piping
Tech Specs	Indirectly limit hydrogen generation from cladding metal/water reaction -> protects containment integrity
Containment pressure suppression and cooling	Protects containment integrity
Fire areas	Redundant systems are required to be in separate fire areas to reduce the threat from fire
Separation of redundant systems	Redundant systems are also required to be separated to be reduce the common threat from other hazards

Examples of Layer 5 Barriers and Layer of Protection

Mitigation of Radiological Consequences of Significant Releases of Radioactive Material

Exclusion area	Separates plant from public; entrance restricted
LPZ/evacuation plan	Residents in low population zone are protected by emergency evacuation plans
Population center distance	Plants are located at a distance from population centers (>25,000)

Limitations of Traditional Approach

- **Universe of accidents is limited**
  - **Single failures only**
  - **Limited treatment of operators**
- **Use of margins to address uncertainties, based on engineering judgment**
  - **Can lead to excessively conservative design**
  - **Can lead to belief that DBAs are limiting**
- **No direct assessment of risk significance (importance)**
- **Does not provide quantitative risk results for decision-making**

The PRA Approach to Assessing Risk

- **Focused on estimating the level of risk and risk-contributing features of design**
  - **PRA identifies accident initiators and inductively derives accident scenarios (i.e., not limited to predetermined set of accidents)**
  - **Analyzes multiple failures, including failures of redundant "barriers"**
  - **Non-safety equipment is credited when the equipment is specifically called out in Emergency Operating Procedures (EOPs)**
  - **More extensive treatment of operator actions**
  - **Use of conservative margins avoided; focus on "best-estimate" analysis where possible**
  - **Goes beyond Design Basis**

Other PRA Approach Characteristics

- **Assesses risk-significance of modeled elements**
- **Provides quantitative results and “models” for decision-making**

ECCS Single Failure Analysis Example
from FSAR Chapter 6, NUREG-0800 Requirements

- The single failure criterion imposes redundancy in safety systems, reducing failure likelihood
- Single Failure Analysis consists of postulating:
  - Initiating occurrence (including multiple failures from a single cause) [Probability = 1.0]
  - + Single Active Component Failure (or passive failure during long term recirculation cooling following an accident) [Probability = 1.0]
  - + Other appropriate hazard (e.g. DBE) [Probability = 1.0]
  - In some respects this approach appears overly conservative because the failures are considered to be certain
  - However, many types of common cause failures are ignored

Single Failure Analysis Example (cont.)
Contrast

Traditional Engineering Single Failure Analysis	PRA
Evaluates a random failure and its consequential effects, in addition to an initiating occurrence, that result in the loss of capability of a component to perform its intended nuclear safety function Evaluates each component, one at a time	Evaluates likelihood of consequences of the failure of all components modeled
Assumes component fails with a probability of 1.0	Assumes each component fails with a best estimate failure rate
No credit for non-qualified components	Credit given for non-qualified components
No common cause failure	Accounts for common cause failure
Limited credit for human actions	Credit for human actions

How PRA "Illustrates" Defense-in-Depth
(analyzes effectiveness of design/operational barriers)

Defense-in-Depth Layer	Objective	Approach	PRA Treatment
1	Prevention of abnormal operation and failures	Training, conservative design (redundancy, margin), quality construction and operation	Models frequency of initiating events
2	Control of abnormal operation and detection of failures	Control, limiting, and protection systems and other surveillance features	As above and models systems (see below) and surveillance failures
3	Control of accidents within design basis	Engineered safety features and emergency operating procedures	Models safety, non-safety systems and human response
4	Control of severe plant conditions	Accident mitigation strategies	Models RCS and containment response and other severe accident mitigation measures in Level 2
5	Mitigation of radiological consequences	Offsite emergency response	Models emergency response and estimates health effects in Level 3

Exercise Demonstrating Traditional Engineering vs. PRA Approach to Safety

- In an instructor-led discussion, have the class design a system made up of piping, pumps, normally-closed injection valves, and supporting power & actuation circuits which will successfully deliver water from a single tank to a single vessel upon low level in the vessel without operator intervention, while meeting the following traditional engineering requirements:
  - Can handle the worst-case single active failure within the system
  - Must be able to handle loss of an entire division of power as a DBA
  - Must be able to handle a 0.2g safe shutdown earthquake (SSE) as another DBA
- From a PRA approach to looking at the system we have designed:
  - What active or passive failures (singularly or in multiples) are factors in assessing the overall "goodness" of our system design?
  - How might operator action be credited in the reliability of the system even though an original design constraint was that the system work without operator action?
  - While the system is designed for the SSE, what other types of outside challenges to the system might we want to consider in assessing the system's overall strengths and weaknesses?
- During the exercise, have the class comment on defense-in-depth features included in our design and how PRA might be used to "measure the goodness" of our use of these "defense-in-Depth" features.