DEFENSE IN DEPTH
AN INTEGRAL PART OF NUCLEAR SAFETY AT U.S. DEPARTMENT OF ENERGY

Jim O'Brien
Department of Energy
Office of Nuclear Safety
Office of Environment, Health, Safety and Security

DOE Nuclear Facilities Background

- Three basic types of nuclear operations:
  - Nuclear Weapons Stockpile Maintenance
  - Research
  - Environmental Cleanup

- Types of Facilities
  - Research reactors;
  - Weapons disassembly, maintenance, and testing facilities;
  - Nuclear material storage facilities;
  - Processing facilities; and
  - Waste disposal facilities.

Need and Objective for DID

Need

Defense in Depth (DID) is needed so that

no one layer by itself, no matter how effective, is completely relied upon

Objective

To provide assurance that no accidental release of radioactive material occurs.

Definition and Scope of DID

Definition

- Defense-in-depth is a fundamental approach to hazard control for nuclear facilities that is based on several layers of protection to prevent the release of radioactive material.

- These protective layers are generally redundant and independent of each other to compensate for human and mechanical failures

Scope

- All DOE Nuclear Facilities

Implementation Approaches

Required by DOE Order 420.1C, *Facility Design*

Defense-in-depth includes:

- choosing an appropriate site;
- minimizing the quantity of material-at-risk;
- applying conservative design margins;
- applying quality assurance;
- using successive/multiple physical barriers for protection against radioactive releases;
- establishing emergency plans for minimizing the effects of an accident

Implementation Approaches

The layers of protection supporting defense-in-depth principles

- LAYER I: Normal safe operation relying upon a high level of design quality, use of passive SSCs, and competent operating personnel.

- LAYER II: Accident management consisting of automatic systems, or operator actions to return process to within normal operating parameters.

- LAYER III: Accident mitigation. Mitigating consequences by a combination of passive features, automatic systems, and emergency response actions

Challenges to Implementing DID

- Ensuring rigor is applied to each aspect of DID (e.g., design, operations, emergency systems, emergency planning)

- How best to apply system level DID utilizing predefined hierarchy
  - Balance between Prevention and Mitigation
  - Event specific control (Nearest to hazard) versus facility wide control

U.S. DEPARTMENT OF ENERGY

EHSS
Office of Environment, Health, Safety and Security

Sufficiency or Adequacy of DID

- Logical approach based upon fundamental safety principles
- Types and layers defined at DOE are consistent with nuclear industry
- Rigorous implementation is key

Relationship of Risk Analysis to DID

- Additional system level DID required for higher hazard facilities
- Redundant and diverse/independent means of accident prevention and mitigation are consistent with risk reduction
- No quantitative risk reduction performed

Next Steps

- DOE continues to look for improvements in rigor and quality of its designs/operations
- DOE developing Accident Analysis and Hazard Control Handbook that provides additional implementation guidance on DID for hazard control schemes.
- Interactions/Insights from this workshop will be useful to DOE as it looks for means for improving its application of DID in nuclear safety.