

# Development of Nuclear Safety Design Criteria

Bates Estabrooks,  
UPF Safety Basis Team Lead

May 5–8, 2008  
2008 EFCOG Safety Analysis Working Group

# DOE-STD-1189 and Design Criteria

- A **guiding principle** of DOE-STD-1189 is the incorporation DOE O 420.1B, *Facility Safety*, design criteria
- Application of these requirements and translation into design criteria requires further elaboration and specification in design documents
- DOE-STD-1189 requires a paradigm shift for nuclear safety analysts
  - Instead of analyzing what already exists, appropriate criteria may be crafted to ensure the design satisfies safety requirements



# For Example...

---

- Water accumulation is a concern for nuclear criticality safety (DOE O 420.1B Chap. III)
  - Considerations:
    - Limit flooding height by defining limit
    - Address any jet or hydraulic forces from pipe failures
    - Address impacts from fire-fighting efforts
  - Example Criteria:
    - Rooms, sumps, etc. shall be designed to allow a liquid depth of not greater than 2 inches
    - Fissile material processing and handling equipment shall retain loading, spacing, etc. requirements during design basis events (DBEs) and fire-fighting activities



# Another Example...

---

- Ensure critical safety functions needed to control processes. (DOE O 420.1B Chap. I)
  - Considerations:
    - Control circuitry should not be affected by failure of process circuits
    - Control circuits must operate in DBE conditions
    - Control circuitry needs to be dependable



# Another Example... (cont.)

## – Example Criteria:

- Circuitry required to perform a safety function shall be electrically isolated from the normal process control functions (e.g., fused/current limited/relay coil to contact/separate raceways, etc).
- SS control circuits shall be designed to SDC-3/LS-D
- Circuitry shall be designed to allow testing to verify operation of the safety function
- Equipment performing a safety function shall perform the required safety function for the expected service conditions associated with the design basis events (e.g., natural phenomena, fires)
- For active safety functions that are classified as Safety Class, the safety function (not the system or component) shall meet single failure criteria to meet required reliability requirements
- Interlocks/isolation valves shall be provided to prevent failure of the safety function from normal process control systems
- After a safety function is accomplished, the safety function shall not be compromised by performing a reset of the initiating signal. A separate action shall be required to allow return to normal control system operation



# Development of Safety Design Criteria for Y-12's UPF

- UPF design criteria development pre-dates DOE-STD-1189
  - >1,000 page design criteria document pre-CD-1
- Principles applied and criteria developed through multi-disciplinary team (SDIT predecessor)
- DOE-STD-1189 Safety Design Strategy (SDS) developed as part of CD-1 submittal to capture previously implemented strategies



# Disclaimer

---

This work of authorship and those incorporated herein were prepared by Contractor as accounts of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Contractor, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, use made, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency or Contractor thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency or Contractor thereof.

