On "Accident-Proof" Designs: Three Thoughts*

N. Siu
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research

2013 ANS Winter Meeting
Panel: "Revisiting Accident-Proof Nuclear Energy After the Fukushima Accident"
Sponsored by Education, Training & Workforce Development Division (ETWDD)
November 11, 2013

*The views provided in this presentation are those of the author and are not necessarily those of the U.S. Nuclear Regulatory Commission.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Topics

- Terminology
- Learning from past events
- The PRA perspective

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Avoiding the Siren's call

- "Accident-Proof"
- "Worst-case analysis"

Bad

- "Accident-Tolerant"

Better, but…

Students deserve a more nuanced discussion

Realistic analyses to support realistic decisions

- Choices among viable alternatives
- Multiple attributes
- Uncertainty
- Finite time and resources
- Multiple stakeholders
- Decision making processes
- Analysis transparency
- Etc.

NUREG-2150, 2012

Sound familiar?

The [event] "…has revealed some weaknesses in the site protection against external flooding related to:"

- Consideration of extreme meteorological conditions in design
- Procedures and on-site emergency organization
  - Accessibility of equipment outside of protected buildings
  - Simultaneous impact on several plants, with possible loss of both external power supplies and ultimate heat sink
  - Site isolation and difficulties in providing rescue staff and equipment
  - Management of release of the water collected in the flooded facilities

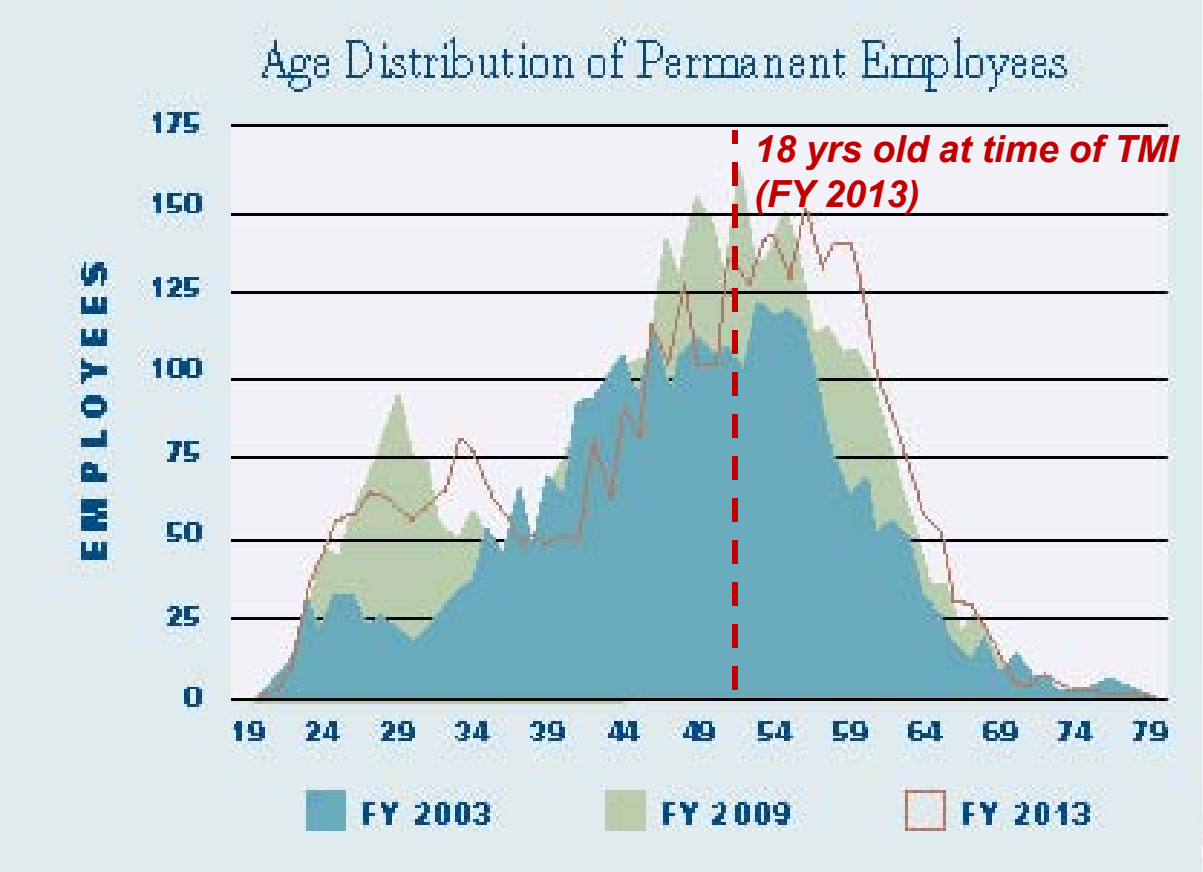
- Vial, Rebour, and Perrin, Severe Storm Resulting in Partial Plant Flooding in 'Le Blayais' Nuclear Power Plant," 2005

And this?

"To cool the reactor, the ordinary water cooling system was not shut down. All of this water was radioactive, and it leaked out onto the floor of the reactor building. By 18h, the floor was awash. Within a few days, the water was 1m deep... Decontamination and clean-up required many months."

- P. Jedicke, "The NRX Incident," 1989

Where were you?



Maintaining awareness of past lessons

- Vast literature
  - Event compilations and summaries(not just power reactors)
  - Detailed investigative reports (voluminous in the case of the Fukushima Dai-ichi reactor accidents)
  - Analyses
- Curriculum for future designers should address “how things fail” (in the field)
- How best to do this?

PRA provides a better viewpoint

- Probabilistic risk assessment (PRA)
  - Identifies and assesses myriad possibilities
    - What can go wrong?
    - How likely is it?
    - What are the consequences?
  - Important qualitative information (what to fix) and quantitative information (how important)
  - Represents current state of knowledge (including operational experience) in treating system as a whole
  - Ethos: ***search*** for potential failures

Goal ≠ "Accident-proof" design
= Risk-managed design

Some classroom challenges

- Changing the students' point of view
  - Focus on failure
  - Importance of analysis breadth
  - Dealing with limited information
  - Explicit recognition and treatment of uncertainty
- Teaching the "what's" and "how's"
  - Importance of understanding the "system"
  - The art of modeling
  - Breadth of toolbox (not just event tree/fault tree analysis)
- Teaching the "why's"
  - Value, limitations, and challenges
  - Risk-informed approaches to real problems
- Preparing for the next step (training)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Recap: challenges to educators

- Ensuring discussions (and terminology) convey realistic design goals and associated challenges
- Ensuring students are aware of key lessons from past accidents and know where and how to look for more information
- Ensuring students are knowledgeable of the value and limitations of PRA (as well as the mechanics) in supporting the development of improved reactor designs