Other Approaches to Safety

Dirk Dunning, PE

Oregon Department of Energy

Lessons from Chernobyl

- **Bad design kills**
- **Mitigating bad design kills**
- **People forget reasons for mitigations**
- **Safety must be baked into the design**
- **Decisions on the fly can kill**
- Operating outside the design envelope can and often does have disastrous consequences
- Complex designs defy understanding and lead to errors

Standard Engineering Design

- **Robust**
- **Elegant**
- **Simple - K.I.S.S.: Keep it Simple Stupid!**
- **Failsafe**
- **Design for failure**
- **Strict codes**
  - (laws, regulations, lessons learned)
- **Licensure and direct accountability**

U.S. Nuclear Navy

- **Reactor safety first, last and always**
  - No one ever allowed to violate reactor safeguards.
  - Do so and you are done – no 2nd chances
- **Verbatim compliance with procedures**
- **Extraordinary well-trained diligent staff**
  - 100% selected by "the Admiral"
- Immediate analysis and response to incidents
- Continuous retraining & direct accountability
- Direct Responsibility, Accountability, Authority
  - Not theoretical. Once qualified – you do the job.
  - Everyone learns from everyone else's errors
  - Everyone responsible to challenge safety
- **Robust, Simple, Elegant, Overbuilt**

Resilience Engineering

- **Safety:**
  - ***ability to succeed under varying conditions***
- **Robust yet flexible processes**;
- Prepare to be surprised
- Range of outcomes vs. consequences
- Continuously monitor and revise risk models
- **Adapt in the face of disruptions or pressures**
- Adjust performance to the current conditions
- Anticipate shape of risk before damage occurs
  - Failure: adaptation to cope with real world complexity, and
  - Not Breakdown of normal system functions

Inherent Safe Design

- **Safety, health and environmental protection built into process design and operation**
- Minimize hazards and materials
  - **What you don't have, can't leak**
  - Substitute, minimize, moderate, simplify
  - Reduce potential consequences
- **Inherent > Passive > Active > Procedural**
- Focus on experience of people, processes, knowledge, history
- Focus also on human factors as safety issues
  - Design, motivation, complexity, training, belief, physical factors and more…

NRC Principles for a Strong Nuclear Safety Culture

- **Safety Culture:**
  - *An organization's values and behaviors – modeled by its leaders and internalized by its members- that serve to make nuclear safety the overriding priority*
- **Safety-Conscious Work Environment**
- **Collective Responsibility**

NRC Principles for a Strong Nuclear Safety Culture (cont.)

1. Everyone personally responsible
2. Leaders demonstrate commitment
3. Trust permeates the organization
4. Decision-making reflects safety first
5. Nuclear technology special and unique
6. Questioning attitude cultivated
7. Organizational learning embraced
8. Safety undergoes constant examination