



RIC 2010
Trends in Shutdown Events
Shutdown Risk – Process and
Configuration Control

Greg Krueger
Exelon
Thursday, March 11, 2010



**Exelon's Configuration Risk
Philosophy**

- At-Power: a blended approach
 - PRA insights complement defense-in-depth approach
 - PRA provides one perspective, but is not sufficient to address all considerations
- Shutdown: a defense-in-depth/qualitative risk approach
 - Safety function defense-in-depth (DID) monitoring
 - Broad definition of "High Risk Evolution" (HRE)
 - Activities that could disrupt safety function
 - Combination of HRE and DID provide qualitative risk perspective



Risk Management Actions

Four color risk management scheme:

-  • Normal Work Controls
-  • Around the Clock Work
• Identify Protected Equipment
-  • Minimize Concurrent Activities
• Notify Plant Management
• Develop Contingency Plans
-  • Not Allowed to be Planned
• Expedite Exit



Key Safety Functions

- Decay Heat Removal
- Spent Fuel Pool Cooling
- Inventory Control
- Electrical Power Availability (includes both On-site and Off-site)
- Reactivity Control
- Containment
- Others as required to address site-specific features or procedures

4



Role of Shutdown PRA

- PRAs can provide a unique integrated perspective on plant safety
 - PRA results are numerical: only as good as the numerical inputs
 - OPEX: Shutdown risk dominated by human errors and response
 - Most difficult aspect of PRA to quantify
- Exelon developed shutdown PRA for one site in 1990s
 - Application found limited additional insights beyond DID/HRE
 - Difficulty translating plant activities into input probabilities

5



Review of INPO SER 2-08 Events

- INPO SER 2-08 spawned the question of whether we should have a shutdown PRA
- The 16 events/examples were reviewed to assess whether shutdown PRA would have provided any benefit, over a traditional Defense In Depth assessment, in identifying or preventing the event:
 - PRA provide no additional benefit: 13 events
 - Very detailed PRA might provide some benefit: 2 events
 - Very detailed PRA would have provided additional benefit: 1 event

6



Review of INPO SER 2-08 Events

- Safety implications of plant event prior to occurrence would not have been highlighted by a detailed shutdown PRA model
- Why??
 - Process and control of the outage schedule are key attributes for the identification and implementation of risk management actions
 - The random failure or combination of failures of equipment in support of a safety function does not dominate the quantitative risk
 - The dynamic changes in schedule and plant configurations appear to contribute most to risk

7



Process Controls

- The Shutdown Safety Management Program (SSMP) requires that when a schedule change or emergent activity occurs, reviews are required for the change and impact on shutdown safety and to make notifications as applicable.
- At dual unit sites the shutdown and at-power schedules are linked to assure impact on the other unit is considered. Some shared systems can impact both units simultaneously and differently.

8



Communications

- Communicate the unit status in a highly visible manner to each shift.
- Identification of the unit status, protected equipment, and significant shutdown safety activities on a shift basis
- Review the unit status, protected equipment, and significant shutdown safety activities at outage meetings. Reasons for status colors other than GREEN is provided to attendees.
- Control room personnel are aware of information such as, time to boil and key safety function status.

9



Conclusions

- Key to shutdown safety is understanding the potential consequences of activities and potential errors
- Defense-in-depth assessment is effective when coupled with
 - Challenge reviews
 - Critical assessment of potential consequences (“What if”)
 - Process Controls
- Adherence to process and communication are effective means in assuring shutdown safety

10
