Problem Statement 1

Bob Enzinna, Dave Blanchard, and Ray Torok

May 30, 2007

NUCLEAR ENERGY INSTITUTE

NRO DC & COL Digital I&C Modeling Issues

- Modeling digital I&C common cause failures (including software)
- Level of modeling detail
- Failure data
- Adequacy of modeling methods
- Interfacing digital I&C system models with the rest of the PRA
- Integrating risk insights into digital I&C reviews and/or risk-informing digital I&C reviews
- Uncertainties

Industry Sensitivity Studies (both new plants and current plants)

- Two factors dictate the sensitivity of PRA to digital I&C
  - Defense-in-depth and diversity of the mitigating systems into which the I&C is being installed
  - Reliability of the digital trains/systems
- These two factors dictate the scope, level of detail, data needs for modeling digital I&C in PRA

Scope of I&C Modeling in PRA

- PRA should focus on:
  - Mitigating systems (principally plant protection systems -RPS/ESFAS)
  - Diverse backup functions (non-safety automatic backup)
- Normal (operational) plant control systems do not require detailed modeling in PRA
  - Use conservative historical IE frequency until plant-specific data available
- Main control room instrumentation systems do not require detailed modeling
  - Typically implicit in HRA

Level of Detail of I&C Model in PRA

- Model functional effects of CCF between identical hardware, operating system, and application software
- Train, subsystem, or processor level of detail is appropriate for mitigating system controls (perhaps even the mitigating system level is sufficient)
  - Resolve physical dependencies (because computers may perform multiple functions)
  - Conservative if all functions on common processor are assumed to fail
  - Credit functional diversity if diverse functions are on separate processors.
- Treat software CCF as a failure mode of the hardware

Software Reliability

- PRA should include CCF contributions from both operating system (OS) and application software (SW)
- Sources of Failure Data
  - Use of operational experience
  - Conformance to safety standards
    - Quantified reliability levels result from consensus
  - Qualification / Safety Evaluation
    - Use of “pre-qualified” platforms
    - QA requirements of 10-CFR-50 Appendix B
  - Technical analysis

  All involve expert opinion and engineering judgment
- Guidance from D3 TWG on what constitutes adequate diversity and design measures for defense against CCF

Sensitivity Analyses

- Raise failure probability for specific digital events (CCF in particular) to determine
  - P_{df} & β_{cc} that would have a significant effect on results (e.g., approach Safety Goals)
- Document deterministic rationale for results
  - Where risk associate with digital failure is low and reason is not failure probability related
    - Document plant design features and operating characteristics that keep risk low
  - Where risk is low but sensitive to digital failure probability
    - Document defensive measures and diversity attributes of the digital system that keep risk low

Modeling of Digital I&C in DC and COL PRAs

- Consistent with NAS Report
- Consistent with RG 1.206
- Consistent with industry consensus & regulatory guidance on PRA applications
  - NEI 00-02
  - ASME Std RA-S-2005
  - RG 1.200
  - RG 1.174

Conclusions

- Developing industry consensus method for incorporating digital I&C into NPP PRA
- Conservative PRA methodology for DC and COL applications to demonstrate low sensitivity to software CCF
- Key elements of software CCF defense are:
  - Assurance of high reliability software
    - Robust software development life cycle
    - Functional diversity
  - Defensive features in mitigating system I&C designs
    - with respect to plant design as a whole
    - within the digital systems themselves

Path Forward

- A level of detail consistent with the hardware in the existing PRA
- An evaluation to demonstrate sensitivity to digital I&C failures, including common cause
- Identification of plant design features and digital system characteristics that result in acceptable risk