ELECTRIC POWER RESEARCH INSTITUTE

Defense-in-Depth and Diversity for Digital Upgrades

Presented at the

Regulatory Information Conference (RIC) 2006

Session Th5D
Digital Instrumentation & Control
March 9, 2006

Raymond C. Torok
Senior Project Manager
Instrumentation & Control
EPRI

Industry Perspective on "D3"

- Software common-mode failure is a legitimate issue for digital upgrades
  - Need to ensure "adequate coping capability"
  - Treated as beyond-design-basis per NRC guidance
- Regulatory uncertainty remains, with chilling effect on plant upgrades
  - Changing interpretations of regulatory guidance
  - Protracted, unpredictable reviews
- Current NRC guidance (deterministic approach of Branch Technical Position HICB-19) is problematic
  - **Can require backups that add complexity and cost without improving safety**
  - **May not address events that are risk-significant**
  - **Discourages plant upgrades that would enhance safety**
  - Requires analysis of events that are not safety-significant

Use of Risk-Insights Would Improve Current Deterministic Approach

- Keep focus on safety – show where software has risk significance
- Allow consideration of plant and digital system characteristics that protect against digital failure and digital CCF, e.g.,
  - Data validation
  - Procedures that allow changes to only one channel at a time
  - Operating system “blind” to plant transients
- Allow consideration of risk associated with adding diverse backups (e.g., spurious actions)
- Consistent with updated technical and regulatory trends
- Technical issues can be addressed
  - Digital system failure probabilities
  - Modeling digital equipment in PRA

Deterministic versus Risk-Informed Example 1 – Large Break LOCA

LBLOCA with digital CCF in low pressure injection (LPI)

- Deterministic (BTP-19) method
  - Insufficient time for operator action
  - Credit for leak detection backup (per BTP-19) may not be allowed
  - Diverse actuation of LPI and supporting systems needed as backup
- Application of risk insights would:
  - Consider low probability of digital CCF in LPI system
  - Show LBLOCA concurrent with digital CCF is a negligible contributor to core damage frequency (CDF)
  - Show that a diverse backup for the I&C
    - Would not reduce risk (because large rotating components dominate)
    - Would add complexity and increase probability of spurious actuation

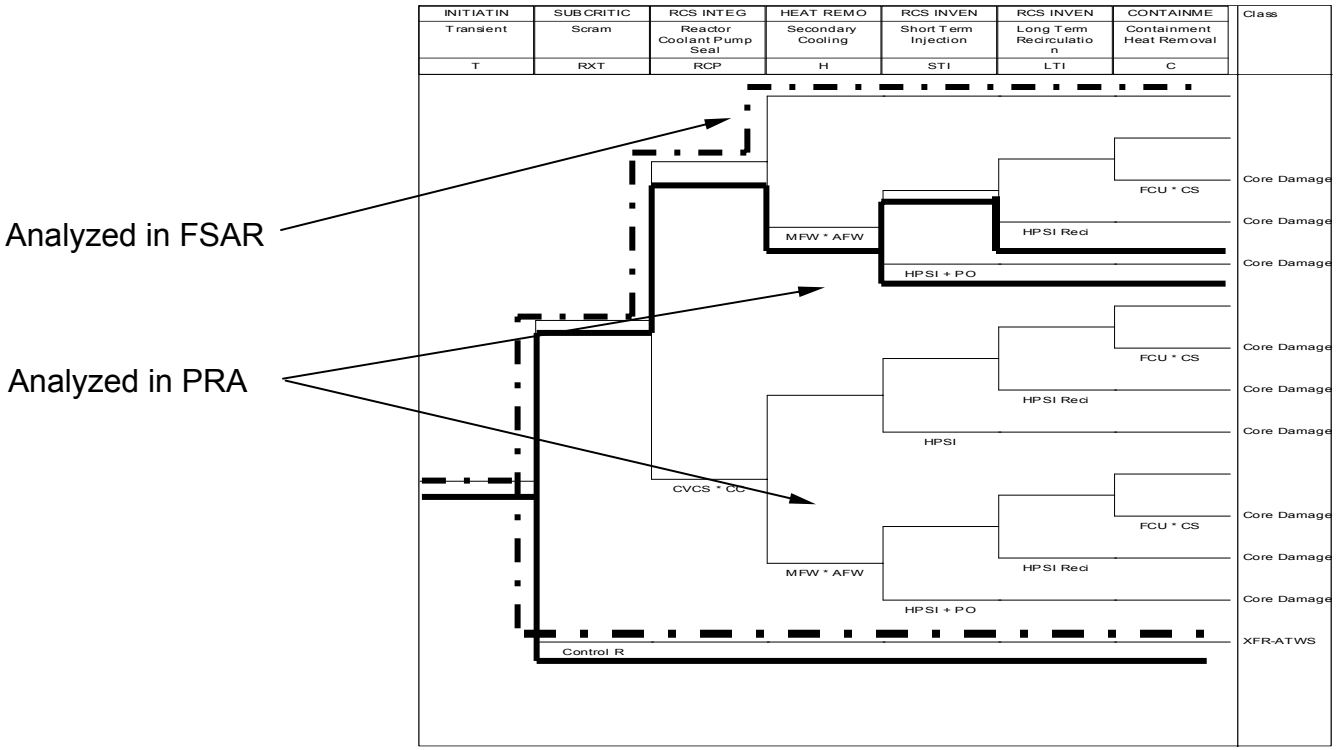
BTP-19 method adds hardware and complexity, with questionable safety benefit

Deterministic versus Risk-Informed Example 2 – Risk-Significant Events from PRA

Deterministic (BTP-19) focus is on SAR events

PRA considers additional beyond-design-basis events

– **Some risk-significant events are not evaluated using BTP-19 method**



Risk-informed method improves coverage of risk significant events

Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades

("D3 Guideline" - EPRI 1002835, December 2004)

- EPRI "D3 Guideline" applies "risk insights" to D3 evaluation
- Provides guidance on:
  - When I&C systems are susceptible to digital common cause failure
  - Where D3 in the I&C is of value in the context of the plant design
  - How reliable a digital system needs to be in the nuclear plant context
- Does not attempt to:
  - Identify all the possible digital system failure modes
  - Precisely determine digital failure probabilities
  - Develop detailed models of digital systems for use in PRA

Nor do we believe these are generally necessary for D3 evaluation

Risk Insights – When is D3 of value for a digital I&C system?

- Dictated by:
  - Frequency of the initiating event
  - Existing D3 of the mechanical and electrical mitigating systems
- High frequency events benefit most from D3 in I&C (e.g., Turbine Trip, Loss of FW)
  - Plant has multiple, diverse mitigating systems
  - Want to preserve existing diversity of electrical / mechanical equip.
- Low frequency events receive little benefit from adding diversity in the I&C (e.g., LOCAs, MSLB)
  - Typically single mitigating system with little diversity between redundant trains of electrical / mechanical equipment

Risk Insights – How reliable does a digital I&C system need to be?

- High frequency events benefit most from reliable I&C
  - Reliability of a channel of digital I&C needs to be similar to that of a functionally similar channel of analog I&C
  - Some degree of diversity needed in actuating mitigating systems (e.g., operator can implement EOPs independent of digital failure)
- For low frequency events, risk is insensitive to reliability of the I&C
  - Usually a single mitigating system with failure probability dominated by major rotating equipment
  - Even assuming CCF of I&C in redundant channels (beta = 1) doesn't make I&C dominant
  - Adding diverse backup for digital I&C has negligible impact on safety

Conclusions/Recommendations

- BTP-19 is out of date and needs improvement
- More balanced design and licensing decision making would help
  - Rule-based (prescriptive) vs. performance-based, e.g.,
    - Could require RPS and ESFAS to be separate and diverse, but for most plants this is unnecessary, because neither backs up the other
    - Better to focus on the real requirement (misbehavior of one system shall not disable another safety function when it's needed)
  - Programmatic (process-based) vs. product or performance-based
    - Could focus primarily on software development process, but good process does not ensure high dependability or safety
    - Better to also consider actual design characteristics and system behaviors, which are more directly linked to dependability and safety

Conclusions/Recommendations, cont'd

- Risk insights should be applied in D3 evaluation
  - Would improve ability to manage safety issues associated with CCFs
  - Can estimate reliability of digital equipment well enough for D3 evaluations **now**, based on deterministic evaluation of the software
  - Can derive useful risk insights for D3 evaluations **now**
    - Without precise knowledge of failure probabilities
    - Without detailed PRA modeling of digital I&C
  - Future research by RES and others will improve methods, accuracy
    - Software reliability
    - Modeling digital systems in PRA
- More and better coordination between NRC and industry is essential for timely resolution of D3 issues