



**Defense-in-Depth and Diversity  
for Digital Upgrades**

**NRC Pre-Submittal Meeting for  
D3 Guideline**

Rockville, MD  
April 21, 2005



### Agenda

09:00	Welcome, introduction, purpose of meeting Project genesis/basis/status Guideline approach key technical elements <ul style="list-style-type: none"><li>- Risk-Informed perspective</li><li>- Defensive measures</li></ul> Proposed D3 methods <ul style="list-style-type: none"><li>- Extended Deterministic</li><li>- Standard Risk-Informed</li><li>- Simplified Risk-Informed</li></ul> Next Steps for Review of D3 Guideline
12:00	Adjourn



Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.



## Presenters

- |                     |                            |
|---------------------|----------------------------|
| • Tony Pietrangelo  | NEI                        |
| • Jack Stringfellow | Southern Nuclear           |
| • Ray Torok         | EPRI                       |
| • Thuy Nguyen       | EPRI/Electricite de France |
| • Glenn Lang        | Consultant                 |
| • Dave Blanchard    | Applied Reliability        |



3

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Meeting Purpose

- Pre-Submittal discussion on D3 Guideline  
*Guideline for Performing Defense-in-Depth and Diversity Assessments for Digital Upgrades – Applying Risk-Informed and Deterministic Methods, EPRI 1002835, December 2004*
- Clarify submittal protocol and fee waiver status
- Review technical approach
- Provide forum for questions and discussion



4

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Background

- Submittal letter, NEI to NRC, February 22, 2005 requested:
  - Review of EPRI D3 Guideline
  - Waiver of review fees per 10CFR170.11
- NRC response, March 11, 2005
  - Clarified pre-submittal meeting procedure
  - Proposed pre-submittal meeting to be followed by “initial” submittal
- April 21 meeting scheduled



5

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Basis for Fee Waiver Request

- D3 Guideline provides an alternative approach to current regulatory guidance that:
  - Improves safety focus and regulatory efficiency and effectiveness
  - Facilitates review of licensee evaluations that use risk insights, reducing staff review time
  - Provides a more comprehensive method for assessing the safety significance of digital common-cause failure (CCF)
- Waiver would be consistent with previous related fee waiver
  - 2002 review of NEI 01-01 (Licensing Guideline)
  - D3 Guideline is a derivative of the Licensing Guideline
- The D3 Guideline provides “....a means of exchanging information between industry organizations and the NRC for the specific purpose of supporting the NRC’s generic regulatory improvements or efforts,” per 10CFR170.11 (a)(1)(iii)



6

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## NRC is Familiar with the Technical Approach

- Attended working group meetings July 2002, March 2003, December 2003, August 2004
- I&C, PRA, and Research organizations were represented
- Presentations of the approach were also made at ISA and ANS conferences in 2002-2004



7

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## D3 Guideline Working Group Includes Broad Industry Representation

Utility design, PRA, and licensing engineers, NEI, EPRI,  
Equipment suppliers, System integrators

Jay Amin	TXU	Jim Mcquighan	Calvert Cliffs
Jim Andrachek	Westinghouse	Thuy Nguyen	EPRI, EdF
Paul Bisges	AmerenUE	Denny Popp	Westinghouse
Dave Blanchard	Applied Reliability	Joe Ruether	NMC Prairie Island
Jay Bryan	Duke	Clayton Scott	Triconex
Ray Disandro	Exelon	Bill Sotos	STP
Larry Erin	Westinghouse	Andrea Sterdis	Westinghouse
Bob Fink	MPR	Jeff Stone	Calvert Cliffs
John Hefler	Aitran	Jack Stringfellow	SNC
Tim Hurst	Hurst Technology	Steve Swanson	SNC
Ron Jarrett	TVA	Dinesh Taneja	Bechtel
Glenn Lang	Consultant	Dan Tirsun	TXU
Peter Lobner	DS-S	Ray Torok	EPRI
Rich Luckett	NEI	Philip Wengloski	Calvert Cliffs
Jerry Mauck	Framatome		



8

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Executive Summary

- Current regulatory guidance (BTP-19 and NUREG/CR 6303) is dated, does not take advantage of benefits of risk insights
- Proposed methods in the EPRI D3 Guideline supplement and complement the BTP-19 approach by applying risk insights
- D3 Guideline applies deterministic assessment of digital system attributes (defensive measures) to supplement NUREG/CR 6303 method
- The proposed methods in the D3 Guideline meet the intent of BTP-19 in that they are effective ways to "demonstrate vulnerabilities to common cause failure have been adequately addressed."



Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved

EPRI

## Existing Guidance on D3 for Digital Upgrades

- Branch Technical Position HICB-19 of Chapter 7 of NUREG 0800 (Standard Review Plan) - (BTP-19)
  - "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems"*
- NUREG/CR-6303
  - "Method for Performing Diversity and Defense-in-Depth Analyses in Reactor Protection Systems"*
- Basic approach
  - Reanalyze all initiating events analyzed in the SAR, concurrent with a digital CCF
  - If results are not acceptable, add diverse backup (could be operator or non-safety system)



10

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved

EPRI

## Characteristics of Current D3 Approach

- Deterministic – assume digital CCF occurs and ensure “adequate coping”
- Focus on RPS, ESFAS, and SAR events
- Best estimate analysis and non-safety backups are okay

However.....

- All digital system failures are assumed to be risk-significant
- High risk and low risk events are treated the same



11

Copyright © 2006 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Net Results of Current Regulatory Guidance

- Can require backups that add complexity and potentially increase plant risk
- May not address events that are risk-significant
- Can discourage digital upgrades that would enhance plant safety
- Can discourage vendors from introducing/licensing digital products that would enhance safety
- Requires analysis that may not be relevant from a plant risk perspective
- Plant upgrades have already been impacted, e.g., Callaway, Oconee, and Diablo Canyon



12

Copyright © 2006 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Importance of Risk-Informed Insights

- Nils Diaz, Chairman of the Nuclear Regulatory Commission, stated in his opening speech for the Regulatory Information Conference on March 8, 2005.

**“Risk insights allow attention to be focused on the truly important, risk-significant systems, components, and scenarios.”**

Nuclear Waste News, March 10, 2005



13

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved

EPRI

## D3 Project Basis

- Introduce risk insights
  - Plant design/safety model determines where diversity is of value
- More realistic treatment of digital system characteristics and behaviors, e.g.,
  - Deterministic assessment of defensive measures such as self testing, data validation, and fault-tolerance
- Consider risk associated with adding diverse mitigating functions (e.g., spurious actuations)
- Use existing plant tools, methods and PRA models
- Independent of D3 issue, PRA models will have to be updated to incorporate digital equipment
- Consistent with evolving technical and regulatory trends



14

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved

EPRI

## Example Comparison of Deterministic and Risk-Informed Approaches

Problematic event - Large break LOCA with digital CCF in low pressure injection (LPI) system

- Deterministic (BTP-19) method
  - Insufficient time for operator action
  - Leak detection backup not credited by NRC
  - Therefore, 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)
  - Diverse backup does not reduce risk (large rotating components dominate)
    - May increase risk due to spurious actuation and added complexity
  - Also identify risk-significant effects of the upgrade on other, more frequent, initiators



15

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## D3 Guideline Approach – 3 Alternative Methods for D3 Evaluation

- **Extended Deterministic** – based largely on BTP-19 approach
  - Use risk insights from PRA to address problematic events
- **Standard Risk-Informed** – risk focus with realistic assumptions
  - Update PRA and regenerate risk results
- **Simplified Risk-Informed** – risk focus with conservative assumptions
  - Use input from existing PRA to estimate change in risk
- All three methods include confirmatory defense-in-depth review, similar to the Significance Determination Process (SDP)



16

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## When a D3 Evaluation is Needed

- Current regulatory perspective – perform D3 evaluation for:
  - Substantial digital replacements of RTS or ESFAS
  - Modification that affects previous D3 evaluation
- Risk-Informed perspective – check D3 implications for:
  - Any modification that could have significant impact on plant risk (CDF or LERF)



17

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Identification of Susceptibilities to Digital CCF

- BTP-19 (NUREG/CR 6303) approach suggests:
  - Identify "blocks" such that internal failures don't propagate beyond block boundaries
  - Blocks that contain the same software modules are considered susceptible to digital CCF
- "Defensive measures" approach in the D3 Guideline looks "inside the block" and complements the NUREG/CR 6303 approach. It:
  - Identifies potential mechanisms for digital failure and digital CCF
  - Identifies defensive measures that restrict digital failures / CCFs to small, manageable sets of potential failures
  - Meets intent of NUREG/CR 6303, and goes to the next level
    - Goes beyond process-based evaluation, considers as-built behaviors
    - Shows objectively why there is for low potential for digital failure



18

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Defensive Measures Approach Provides Deterministic Basis

- Evaluation of defensive measures provides a deterministic basis for estimating dependability / reliability of digital equipment for PRA models. However,
  - It is different from standard PRA treatment of hardware reliability - Digital failures are not random
  - It requires expertise in software and digital system design



19

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Important Considerations for Defensive Measures

- Design features may give reasonable assurance that pre-developed components are unlikely to cause digital failures
- **In such cases, focus on the application!**
- In highly reliable digital systems, the functional specification is often the most significant source of failures
  - D3 Guideline suggests defensive measures against functional specification errors
  - NUREG/CR 6303 is silent on this



20

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Extended Deterministic Method

Based on the BTP-19 approach

- Analyze SAR events concurrent with postulated digital CCFs
- Use 'best-estimate' approach
- Use relaxed acceptance criteria per BTP-19

Extension of BTP-19 approach:

- Use risk insights from PRA to address problematic events
- Perform confirmatory review to ensure that all events considered in the PRA have been addressed



21

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved

EPRI

## Standard Risk-Informed Method

- Update the PRA model for the digital upgrade
  - Add potential intra/inter system common cause events into event tree and fault tree models
  - Use realistic-to-bounding assumptions for
    - Reliability of digital equipment
    - Effects of common-cause failure of digital equipment
  - Failure probabilities and beta factors based on defensive measures assessment
- Estimate CDF, LERF post-upgrade
- Perform sensitivity study to address uncertainties in failure probabilities
- Use Regulatory Guide 1.174 acceptance guidance ( $\Delta$ -risk)
- Perform confirmatory review



22

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved

EPRI

## Simplified Risk-Informed Method

- Use input from existing PRA
- Directly estimate upper bound for  $\Delta$ CDF,  $\Delta$ LERF for each initiating event
  - Use conservative assumptions
  - Credit/add diversity or relax assumptions where it has significant impact on risk estimate and can be justified
- Use RG 1.174 acceptance criteria
- Perform confirmatory review



23

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## D3 Confirmatory Review

- The D3 Guideline includes a qualitative method for confirming the results of the D3 evaluation, regardless of which of the methods is used.
  - For the Extended Deterministic Method, it:
    - *Brings in the spectrum of initiating events considered in the PRA and provides assurance that risk significant beyond design basis accident sequence types are addressed.*
  - For the Standard and Simplified Risk-Informed Methods, it:
    - *Generates additional deterministic insights as to the acceptability of the digital upgrade design.*
    - *Helps to document compliance with the Defense-in-Depth principle of Regulatory Guide 1.174*



24

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## D3 Confirmatory Review

Initiating Event Frequency	Mechanical System Designs	≥ 3 diverse trains OR 2 redundant systems	1 train + 1 system with redundancy	2 diverse trains	1 train + recovery of failed train	1 train	Recovery of failed train	None
	Acceptable I&C System Designs	1 automatic redundant safety system AND (1 automatic I&C channel OR manual initiation)		1 automatic redundant safety system OR (1 automatic I&C channel AND Manual Initiation)		1 automatic I&C channel OR Manual Initiation		
1 to 10 <sup>1</sup> / yr	Reactor trip Loss of Condenser							
10 <sup>1</sup> to 1 / yr	Loss of off-site power Total loss of main DY DCS operation (BWR) MSLB (outside crane) Loss of 1 SR AC bus Loss of Instr/Crit air							
10 <sup>2</sup> to 10 <sup>1</sup> / yr	SGTR Stack open PORV/SV MFLB MSLB inside Loss of 1 SR DC bus							
10 <sup>3</sup> to 10 <sup>2</sup> / yr	Small LOCA							
10 <sup>4</sup> to 10 <sup>3</sup> / yr	Medium & large LOCA							
10 <sup>5</sup> to 10 <sup>4</sup> / yr								
< 10 <sup>5</sup> / yr								



Loss of Feedwater

25

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## If Acceptance Criteria (Including Confirmatory Review) are Not Met

- If acceptance criteria not met – have a few basic alternatives
  - Refine parameters and/or assumptions used in the D3 evaluation (with justification)
  - Use one of the other methods
  - Modify design of upgrade to eliminate digital CCFs of concern
  - Add backup function that is not subject to the digital CCFs of concern
  - Do not implement the digital upgrade



26

Copyright © 2005 Electric Power Research Institute, Inc. All rights reserved.

EPRI

## Next Steps for Review of D3 Guideline

- NRC issue pre-submittal comments
- Working group revise D3 Guideline as appropriate to address NRC pre-submittal comments
- NEI send to NRC "initial" submittal of D3 Guideline
- NRC make fee waiver decision
  - If fee waiver approved, NRC proceed with review
  - If fee waiver denied, need to wait for industry funding approval
- Schedule for comments / review process

