



# U.S. Nuclear Regulatory Commission

## MEETING WITH AREVA NP, INC.

Discussion of June 2010 Diversity and Defense-in-Depth  
Request for Additional Information

Two White Flint, Rockville, Maryland

July 22, 2010

# Agenda

3

- Objectives
- Diverse Actuation System Functionality
- Diverse Actuation System Implementation
- Diverse Actuation System Diversity Guidance
- Diverse Actuation System DAS Performance Guidance
- Addressing I&C Vulnerabilities
- Questions / Comments
- References

# Objectives

4

□ Discuss:

-Diverse Instrumentation and Control Regulations and Guidance

-Diversity and Defense-in-Depth Analysis Guidance

-Diversity Best Estimate, Deterministic Analysis, Limits and Goals

# Diverse Actuation System Functionality

- **10 CFR part 50, Appendix A, General Design Criterion 22, Protection System Independence**

The protection system shall be designed to assure that the effects of postulated accident conditions on redundant channels do not result in loss of the protection function. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

- **SRM to SECY-93-087, Item II.Q, Defense Against Common-Mode failures in Digital Instrumentation and Control Systems**

If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function.

# DAS Implementation

6

- **10 CFR 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-water-cooled Nuclear Power Plants**

- Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system....

- This equipment must be designed to perform its function in a reliable manner....

- **Quality Guidance**

- SRM to SECY-93-087, Item II.Q, Defense Against Common-Mode failures in Digital Instrumentation and Control Systems**

The diverse or different function may be performed by a non-safety related system if the system is of sufficient quality to perform the necessary functions under the associated event conditions.

- Generic Letter 85-06, Quality Assurance Guidance for ATWS Equipment that is not Safety-Related**

Explicit quality assurance guidance is provided in its enclosure. The lesser safety significance of diverse equipment (i.e., ATWS equipment) necessarily results in less stringent quality assurance guidance.

# DAS Implementation continued

BRANCH TECHNICAL POSITION 7-19, GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

7

## Design Diversity

- Design diversity
- Equipment diversity
- Functional diversity
- Human diversity
- Signal diversity
- Software diversity

## Diversity Performance Guidance

### Anticipated Operational Occurrences

For each AOO in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using best estimate analyses should not result in radiation release exceeding 10 % of the 10CFR100 guideline or violation of the integrity of the primary coolant pressure boundary.

### Postulated Accidents

For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using best-estimate analyses should not result in radiation release exceeding the 10CFR100 guideline or violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).

# Diversity Guidance

## NUREG/CR-6303 Diversity Attributes

8

<b>Design Diversity</b>	<b>Equipment Diversity</b>	<b>Functional Diversity</b>	<b>Human Diversity</b>	<b>Signal Diversity</b>	<b>Software Diversity</b>
<b>Different technologies</b>	<b>Different manufacturers of fundamentally different designs</b>	<b>Different underlying mechanism</b>	<b>Different design organization</b>	<b>Different reactor or process parameters sensed by different physical effects</b>	<b>Different algorithms, logic, and program architecture</b>
<b>Different approaches within a technology</b>	<b>Same manufacturer of fundamentally different designs</b>	<b>Different purpose, function, control logic, or actuation means</b>	<b>Different engineering management team within the same company.</b>	<b>Different reactor or process parameters sensed by the same physical effect</b>	<b>Different timing, order of execution</b>
<b>Different architecture</b>	<b>Different manufacturers making the same design</b>	<b>Different response time scale</b>	<b>Different designers, engineers, or programmers.</b>	<b>The same reactor or process parameter sensed by a different redundant set of similar sensors</b>	<b>Different operating system</b>
	<b>Different versions of the same design</b>		<b>Different testers, installers, or certification personnel.</b>		<b>Different computer language</b>

# Diverse Actuation System Performance Guidance

- **SRM to SECY-93-087, Item II.Q, Defense Against Common-Mode failures in Digital Instrumentation and Control Systems**

In performing the assessment, the vendor or applicant shall analyze each postulated common-[cause] failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

# Diverse Actuation System Performance Guidance continued

## Anticipated Operational Occurrences

For each AOO in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using best estimate analyses should not result in radiation release exceeding 10 % of the 10CFR100 guideline or violation of the integrity of the primary coolant pressure boundary.

## Postulated Accidents

For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using best-estimate analyses should not result in radiation release exceeding the 10CFR100 guideline or violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).

# DAS Performance Guidance continued

## 10CFR100 Limit Requirements

□ **10CFR100.21(c)(1)**

(c) Site atmospheric dispersion characteristics must be evaluated and dispersion parameters established such that:

(1) Radiological effluent release limits associated with ***normal operation*** from the type of facility [i.e., stationary power reactor] proposed to be located at the site can be met for any individual located offsite

□ **10CFR34(a)(ii)(D)**

(D) ... Special attention must be directed to plant design features intended to mitigate the radiological consequences of accidents. In performing this assessment, an applicant ***shall assume a fission product release from the core into the containment assuming that the facility is operated at the ultimate power level contemplated.***

- Therefore, an applicant's diversity and defense-in-depth deterministic analysis should ***assume a fission product release from the core into the containment assuming that the facility is operated at the ultimate power level contemplated.***

# DAS Performance Guidance continued

## 10CFR100 Limit Requirements

□ **10CFR100.21(c)(2)**

(2) Radiological dose consequences of postulated accidents shall meet the criteria set forth in 50.34(a)(1) of this chapter for the type of facility proposed to be located at the site;

□ **10CFR34(a)(ii)(D)(1) and (2)**

(1) An individual located at any point on the boundary of the exclusion area for any 2-hour period following the onset of the postulated fission product release, **would not receive a radiation dose in excess of 25 rem** total effective dose equivalent (TEDE).

(2) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) **would not receive a radiation dose in excess of 25 rem** total effective dose equivalent (TEDE)

# Addressing I&C Vulnerabilities

## **Branch Technical Position 7-19, Acceptance Criteria**

The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

# REFERENCES

- 10 CFR Part 50  
[<http://www.nrc.gov/reading-rm/doc-collections/cfr/part050.html>]
- SRM to SECY-93-087, Item II.Q, Defense Against Common-Mode failures in Digital Instrumentation and Control Systems [ADAMS Accession No. ML003708056]
- NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems [ADAMS Accession No. ML071790509]
- Generic Letter 85-06, Quality Assurance Guidance for ATWS Equipment that is not Safety-Related [ADAMS Accession No. ML031140390]
- Branch Technical Position 7-19, Guidance for Evaluation of Diversity and Defense-in-depth in Digital Computer-based Instrumentation and Control Systems  
[ADAMS Accession No. ML070550072]