APRIL 18, 2007

PROJECT PLAN - TWG # 2
DIVERSITY AND DEFENSE-IN-DEPTH

1. BACKGROUND:

NRC regulations require licensees to incorporate diversity and defense-in-depth into a nuclear facility's overall safety strategy to ensure that abnormal operating occurrences and design basis events do not adversely affect public health and safety. The responsibility for incorporating appropriate diverse systems and defense-in-depth approaches into safety system designs lies with the licensee. The responsibility for independently evaluating the design lies with the NRC.

Historically, safety system designers have relied on three strategies for addressing potential common cause failures (CCFs): functional defense-in-depth, functional diversity, and system diversity. These approaches have worked well in analog protection systems because CCFs were assumed to be caused by slow processes such as corrosion and equipment wearing out, which could be identified by an operator in sufficient time to prevent multiple failures. This assumption, while shown to be valid for analog safety systems, does not fully address the potential for CCFs in software-based safety systems.

Implicit in the development of digital safety systems is the need to eliminate or mitigate the effects of potential CCFs during the safety system development process. However, the ability to identify CCF vulnerabilities during the system development phase has become especially problematic as the complexity of safety systems has increased. Consequently, the NRC published requirements and guidance for identifying and mitigating CCFs by analyzing safety system designs to ensure an acceptable level of diversity and defense-in-depth was present.

Guidance for performing diversity and defense-in-depth analyses of systems to identify appropriate diversity and defense-in-depth in nuclear power plant instrumentation and control system designs is provided in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (ML9501180332), as well as Branch Technical Position (BTP) 7-19, "Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" [Chapter 7, "Instrumentation and Controls," of NUREG-0800, "Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants"]. This guidance was developed for nuclear power plant safety systems; however, the diversity attributes and associated criteria identified in the guidance are applicable for other nuclear facilities as well. The intention of this guidance is to provide the licensee and the staff a means for assessing whether additional diversity is required in a digital safety system on the basis of the safety system and nuclear power plant design features. The industry indicated that this guidance addressing the problem statements identified below, however, is needed to provide additional details for clarification and to reduce potential regulatory uncertainty.

The NRC staff is also working closely with the industry to improve the current guidance as appropriate, and this Task Working Group (TWG) will develop guidelines and recommendations for confirming that sufficient diversity and defense-in-depth has been incorporated into a digital safety system design.

2. SCOPE:

The following areas and associated activities will be addressed by the TWG:

a. Describe existing regulatory requirements and regulatory guidance associated with diversity and defense-in-depth requirements, without consideration of specific nuclear facility designs (e.g., existing nuclear power plant designs and new nuclear power plant designs). This description will define the recommended boundaries for the ultimate products of this TWG.

b. Identify acceptable diversity and defense-in-depth strategies for implementing digital safety functions and systems. The strategies will be based upon existing guidance and the approaches taken by other countries, industries, and agencies; and upon recommendations from the scientific community and academia.

c. Determine the criteria supporting operator actions in lieu of automated system responses to design basis and other accidents. For example, when could operator responses to instrumentation indications be credited for mitigating certain types of design basis accidents?

d. Identify consensus standards that could be endorsed as regulatory guidance. For example, ANSI/ANS Std 58.8-1994 (® 2001), "Time Response Design Criteria for Safety-Related Operator Actions," may provide acceptable guidance for crediting operator actions as part of a diversity strategy for certain classes of design basis events.

e. Develop one or more Regulatory Issue Summaries (RISs), or other vehicle(s) as directed by the NRC Digital I&C Steering Committee, to document, by inclusion or reference, the interim staff guidance developed or identified by this TWG. The RIS will include references to suitable standards and other guidance that can be used to develop and license safety system diversity and defense-in-depth features.

f. Recommend new guidance to be incorporated into NRC Standard Review Plans.

3. PROBLEM STATEMENT:

Nuclear industry and NRC guidance does not explicitly identify what constitutes acceptable diversity and defense-in-depth in nuclear facility safety system designs. The following issues should be addressed to resolve this issue.

a. Adequate Diversity: Additional clarity is desired on what constitutes adequate Diversity and Defense-in-Depth. Determine: 1) How much Diversity and Defense-in-Depth is enough; 2) If there are precedents for good engineering practice; 3) If sets of diversity attributes and criteria can provide adequate diversity; 4) How much credit can be taken for designed-in robustness in determining the required amount of diversity; and 5) If there are standards that can be endorsed?

b. Manual Operator Actions: Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.

c. Credit for leak detection: Additional clarity is a desired for crediting leak detection as part of a diversity and defense-in-depth coping strategy.

d. BTP-19 Position 4 Challenges: Current Commission policy addresses system-level actuation in BTP-19, Position 4. Industry has proposed that further clarification is needed relative to when and if credit can be taken for component-level verses system-level actuation of equipment. Clarify the rationale for when and why BTP-19, Position 4 would not be applicable for existing plant upgrades.

e. Effects of Common-Cause Failure (CCF): BTP-19 guidance recommends consideration of CCFs that "disable a safety function." However, additional clarity is desired regarding the effects that should be considered (e.g., fails to actuate and/or spurious actuation).

f. Common-Cause Failure Applicability: Clarification is desired on identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity).

g. Echelons of Defense: As described in NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements," the following plant safety functions must be controlled to mitigate plant accidents:

1. Reactivity control
2. Reactor core cooling and heat removal from the primary system
3. Reactor coolant system integrity
4. Radioactivity control
5. Containment conditions

Current nuclear power plant designs maintain the above safety functions within safe margins using the following echelons of defense:

1. Control systems
2. Reactor Trip System (RTS)
3. Engineered Safety Features Actuation System (ESFAS)
4. Monitoring and indications

Additional clarification is desired regarding how the echelons of defense for maintaining the above safety functions should factor into diversity and defense-in-depth analyses. A particular concern is that the current BTP-19 guidance does not consider plant design characteristics and operating procedures that affect how diversity and defense-in-depth are actually used to maintain the safety functions.

h. Single Failure: Additional clarification is needed regarding the acceptance criteria for addressing common cause failures versus the acceptance criteria for addressing single failures in safety system designs.

4. DELIVERABLES:

Interim guidance and Standard Review Plan guidance and acceptance criteria will be drafted. The Diversity and Defense-in-Depth Task Working Group will address the following issues and propose the following specific products:

a. Adequate Diversity: Interim staff and industry guidance and a revision to the Standard Review Plan will be developed that describe adequate diversity that considers engineering approaches and acceptance criteria that have been developed in other countries, industries, and agencies. Additionally, academia and scientific organization recommendations for implementing appropriate diversity and defense-in-depth strategies will be considered in developing the guidance.

b. Manual Operator Actions: Interim staff guidance and an update to the Standard Review Plan will be developed that describes the conditions under which operator actions can be credited as a diverse method for initiating safety functions. Development of this guidance will be coordinated with the efforts of the Highly Integrated Control Room - Human Factors Task Working Group (#5).

c. Credit for Leak Detection: This issue is a subset of the Manual Operator Actions issue, and should be integrated into that effort. Consequently, a separate guidance document is not expected to be produced.

d. BTP-19, Position 4 Challenges: Interim staff guidance will be developed that describes the conditions under which credit can be taken for component-level verses system-level actuation of equipment. This guidance will address upgrades for currently operating nuclear plants and fuel cycle facilities, as well as new plant designs. Changes to BTP-19 may be recommended to make the guidance generically applicable to all plant designs.

e. Effects of Common-Cause Failure: BTP-19 guidance recommends consideration of common cause failures that "disable a safety function." Interim staff guidance and a revision to the Standard Review Plan will be developed to guide the process for evaluating potential common-cause failure analyses and for specifying the failure states that should be integrated into safety system design

basis analyses (e.g., fails to actuate and/or spurious actuation).

f. Common-Cause Failure Applicability: Interim staff guidance and a revision to the Standard Review Plan will be developed for digital system design attributes that are sufficient to eliminate consideration of common-cause failures. These attributes will include recommended diversity strategies and acceptance criteria for attributes such as degree of simplicity, complexity, and robustness.

g. Echelons of Defense: Interim staff guidance and a revision to the Standard Review Plan guidance and acceptance criteria will be developed to describe appropriate levels of defense-in-depth in safety system designs.

h. Single Failure: Interim staff guidance and a revision to the Standard Review Plan guidance and acceptance criteria will be developed that addresses the conditions under which software failures are to be considered common-cause failures or single failures in plant design basis analyses.

5. MILESTONES, ASSIGNMENTS AND DELIVERABLES:

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fsct/Actual**	**Lead**	**Support**
1 Adequate Diversity					
1a) Propose acceptable diversity and defense-in-depth strategies on the basis of approaches used by other countries, industries, and agencies and recommendations by academia and scientific organizations.			F	NEI	N/A
1b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
1c) Receive public comments			F	NRC	N/A
1d) CRGR interaction (as needed)			F	NRC	N/A
1e) ACRS interaction (as needed)			F	NRC	NEI
1f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
2 Manual Operator Actions					
2a) Develop criteria for specifying response times for manual operator actions as a component of a diversity and defense-in-depth strategy			F	NEI	N/A
2b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
2c) Receive public comments			F	NRC	N/A
2d) CRGR interaction (as needed)			F	NRC	N/A
2e) ACRS interaction (as needed)			F	NRC	NEI
2f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
3 Credit for Leak Detection					
3a) Identify bases and criteria for crediting leakage detection as part of an acceptable diversity strategy.			F	NEI	N/A

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fsct/Actual**	**Lead**	**Support**
3b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
3c) Receive public comments			F	NRC	N/A
3d) CRGR interaction (as needed)			F	NRC	N/A
3e) ACRS interaction (as needed)			F	NRC	NEI
3f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
4 BTP-19, Position 4 Challenges					
4a) Clarify BTP-19 guidance regarding the use of component-level and system-level manual initiations of safety functions.			F	NRC	NEI
4b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
4c) Receive public comments			F	NRC	N/A
4d) CRGR interaction (as needed)			F	NRC	N/A
4e) ACRS interaction (as needed)			F	NRC	NEI
4f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
5 Effects of Common-Cause Failure					
5a) Develop guidance for evaluating potential common-cause failures and for specifying the failure states that should be integrated into safety system design basis analyses, considering both failures to actuate and spurious actuations.			F	NRC	NEI
5b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
5c) Receive public comments			F	NRC	N/A
5d) CRGR interaction (as needed)			F	NRC	N/A
5e) ACRS interaction (as needed)			F	NRC	NEI

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fsct/Actual**	**Lead**	**Support**
5f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
6 Common-Cause Failure Applicability					
6a) Identify acceptance criteria for design attributes that could eliminate consideration of common-cause failures in safety system designs. These attributes could include, for example, the degree of simplicity, complexity measurements, and robustness of system design.			F	NRC	NEI
6b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
6c) Receive public comments			F	NRC	N/A
6d) CRGR interaction (as needed)			F	NRC	N/A
6e) ACRS interaction (as needed)			F	NRC	NEI
6f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
7 Echelons of Defense					
7a) Develop guidance and acceptance criteria for appropriate levels of defense-in-depth in safety system designs, and application principles for defense-in-depth in safety system designs.			F	NRC	NEI
7b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
7c) Receive public comments			F	NRC	N/A
7d) CRGR interaction (as needed)			F	NRC	N/A
7e) ACRS interaction (as needed)			F	NRC	NEI
7f) Issue final interim guidance if appropriate	✓		F	NRC	N/A

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due Date**	**Fsct/Actual**	**Lead**	**Support**
8 Single Failure					
8a) Develop guidance that addresses consideration of software failures with respect to single failure licensing basis considerations.			F	NRC	NEI
8b) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
8c) Receive public comments			F	NRC	N/A
8d) CRGR interaction (as needed)			F	NRC	N/A
8e) ACRS interaction (as needed)			F	NRC	NEI
8f) Issue final interim guidance if appropriate	✓		F	NRC	N/A
LONG-TERM					
Revise consensus standards (e.g., IEEE), if appropriate			F	NEI	N/A
Issue permanent regulatory guidance for milestones 1-8, if appropriate	✓		F	NRC	N/A