Draft Interim Staff Guidance on
Diversity and Defense-in-Depth Task Working Group
Problem Statement 7

Problem 7:

Single Failure: Additional clarification is required regarding the acceptance criteria for common cause failures (CCFs) versus the acceptance criteria for single failures in safety system designs.

STAFF POSITION:

Based upon the definition of a single failure in 10 CFR 50, Appendix A, and the guidance provided by IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," as endorsed by Regulatory Guide (RG) 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems, Rev. 2" (ML033220006), a software CCF does not meet the criteria for a single failure in single failure analyses.

RATIONALE:

In the July 21, 1993, SRM associated with SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," the Commission determined that software CCF was a beyond design basis event. The staff discussed this issue with the industry and public during a May 9, 2007, meeting of the D3 TWG. The staff determined that this conclusion was appropriate, and that software CCFs are special cases of failures.

Digital system CCFs can be caused by an error in identical software logic that is operating in otherwise independent safety system channels. As with anticipated transient without scram (ATWS) events (i.e., reactor trip system CCFs), a digital system CCF, even when caused by a software error, is considered a failure that is beyond design basis. Therefore, as with ATWS mitigation systems, if a postulated digital system CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is not subject to the same CCF, is needed to perform either the same function or a different function that will mitigate the accident or transient that required the original safety function. Nonetheless, the diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants," defines single failure as the following:

> "Single failure. A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive

component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."

This definition focuses on an occurrence which results in the loss of capability of a component. This is not the case for software CCF. The loss of capability in multiple channels is the result of a design deficiency, manufacturing error, maintenance error, or an operator error, and these errors are specifically exempted from single failure analysis consideration by IEEE Std 379-2000 which is endorsed by RG 1.53. Further, a CCF is not the result of a single component failing and causing cascading failures; instead, it is several related but independent failures all resulting from a common cause. As discussed in IEEE Std 379-2000, extensive NRC requirements for design qualification and quality assurance programs are intended to afford protection from external environmental effects, design deficiencies, and manufacturing errors. Further, requirements for personnel training; proper control room design; and operating, maintenance, and surveillance procedures are intended to afford protection from maintenance and operator errors.

REFERENCES:

7-1. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants.”

7-2. IEEE Std 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

7-3. Regulatory Guide (RG) 1.53, “Application of the Single-Failure Criterion of Nuclear Power Plant Protection Systems,” Rev. 2 (ML003740182)

7-4. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs” (ML003708021)