# Draft Interim Staff Guidance on Diversity and Defense-in-Depth (D3) Task Working Group Problems 3, 4, 5, and 6 in Digital Instrumentation and Control Systems

## Draft Interim Staff Guidance on D3 TWG Problem 3

**Problem 3:**

BTP-19 Position 4 Challenges: Current Commission policy addresses system-level actuation in BTP-19, Position 4. Further clarification is required for whether credit can be taken for component-level verses system-level actuation of equipment. The NRC should clarify the rationale for applying BTP-19, Position 4 for digital system upgrades in existing plants.

**Background**

BTP-19, Position 4 states:

> "A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3."

The intent of requiring system level actuation was to assure that the actuation, however achieved, was possible using simple controls from within the control room, without requiring plant operators to activate or control individual equipment at various locations within the plant. The exact method of actuating the protective function is not as important as that the actuation be

a) simple,
b) possible from the control room,
c) required with sufficient time available for the operators to determine the need for protective actions even with malfunctioning indicators,
d) appropriate for the event, and
e) supported by sufficient instrumentation that indicates that
    1) the protective function is needed,
    2) the safety-related automated system did not perform the protective function, and
    3) the manual action was successful in performing the protective function.

**Draft Interim Staff Guidance**

In the current Draft ISG on Problems 1 and 2, the staff recommended that BTP-19, Position 4 be re-written to state:

> "In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, radioactivity control, and containment conditions. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same common cause failure (CCF) that necessitated the diverse backup system; one example would be the use of hard-wired connections."

This draft interim guidance does not specify whether the diverse displays and controls be used for component-level or system-level actuation of equipment, as long as the criteria are met.

# Draft Interim Staff Guidance on D3 TWG Problem 4

**Problem 4:**

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

**Background**

IEEE Standard 603-1991, incorporated into 10 CFR by reference in 10 CFR 50.55a(h), states in paragraph 5.1, Single-Failure Criterion: “The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.”

There are two inherent safety functions that safety-related trip and actuation systems provide. The first safety function is to provide a trip or system actuation when plant conditions necessitate that trip or actuation. However, in order to avoid challenges to the safety systems and to the plant, the second function is to not trip or actuate when such a trip of actuation is not required by plant conditions. A simple metric would be:

| | Plant conditions require a trip or actuation | Plant conditions do not require a trip or actuation |
|---|---|---|
| Trip or Actuation occurs | Proper System Operation | **System Failure** (Spurious Actuation) |
| Trip or Actuation does not occur | **System Failure** (Actuation does not occur or incomplete activation) | Proper System Operation |

Therefore, to be in conformance with the single failure criteria, both a failure to trip and a spurious trip are unacceptable.

Software CCF was declared a beyond design basis event by the Commission in Staff Requirements Memorandum dated July 21, 1993, issued in response to SECY-93-087, dated April 2, 1993. The industry has requested additional clarification regarding the effects of software CCF that should be considered.

**Draft Interim Staff Guidance**

When considering the possible types of protection system failures that may occur as a result of failure to actuate, a simple failure of the total system may not be the worst case failure, particularly when analyzing the time required to identify and respond to the condition. A failure to trip may not be as limiting as a partial actuation of an emergency core cooling system, with digital indications of a successful actuation, which may take longer to evaluate and correct than a total failure to send any actuation signal. For this reason, the evaluation of failure modes as a result of software CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate.

Industry also requested that the staff determine whether spurious actuations should be considered when performing single failure analyses associated with software CCF. The primary concern is that an undetected failure within the digital system could prevent proper system operation. A failure or fault that is detected can be repaired; however, failures that are nondetectable may prevent a trip or actuation when required. Consequently, nondetectable faults are of concern. Therefore, a diverse means to provide the required safety function, or some other safety function that will adequately address each chapter 15 event should be provided.

Common cause failures that cause an undesired trip or actuation are detectable because the failure is self-announcing. There may be circumstances in which a spurious trip or actuation would not occur until a particular signal trajectory within the software is reached. In these cases, the spurious trip or actuation would not occur immediately upon system startup, but could occur under particular plant conditions. This circumstance is still self-announcing, even if the annunciation did not occur on initial test or startup. Use of design techniques (e.g., a constant and unchanging signal trajectory within the software that is unaffected by plant conditions), therefore, is recommended.

In general, spurious trips and actuations are lesser safety concern than failures to trip or actuate. There may be plant and safety system challenges and stresses; however, these challenges are not as significant as failure to respond to a chapter 15 event.

For these reasons, beyond design basis software common cause failures, a spurious trip, or actuation of a safety-related digital protection system does not need to be considered in the single failure analysis.

# Draft Interim Staff Guidance on D3 TWG Problem 5

**Problem 5:**

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

**Draft Interim Staff Guidance**

There are two design attributes that are sufficient to eliminate consideration of CCF:

(1) Diversity - In Example 1 for Problems 1 and 2, sufficient diversity exists in the protection system such that CCFs within the channels can be considered to be fully addressed without further action.

> Example 1: A four-channel RPS is designed so that, for each safety function, two channels use one type of digital system and the other two channels use a diverse digital system. A D3 analysis performed consistent with the guidance in NUREG/CR-6303 and BTP-19 determines that the two diverse digital systems are not subject to a CCF. In this case, no additional diversity would be required in the safety system.

(2) Testability - A system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses.

In assessing the system states, the guidance provided in IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," clause 5.4.1, "Computer system [equipment qualification] testing," should be addressed:

> Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.

Clause 5.4.1 requires the system developer/user to perform equipment qualification of the system (i.e., hardware and software) in its operational states while the system is operating at the limits of its equipment qualification envelope. The software and diagnostics should be representative of the software used in actual operation to a degree that provides assurance that the system states produced by the actual system will be tested during the equipment qualification process.

# Draft Interim Staff Guidance on D3 TWG Problem 6

**Problem 6:**

Echelons of Defense: As described in NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements," sufficient information shall be provided to the operators to monitor (and thereby control) the following plant safety functions and conditions:

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

BTP-19 guidance references the echelons of defense described in NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” (Accession No. 9501180332) for maintaining the above safety functions within safe margins for currently operating nuclear power plants:

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 D3 analyses. A particular concern is that the current BTP-19 guidance does not consider plant design characteristics and operating procedures that affect how D3 is actually used to maintain the safety functions.

**Background:**

SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," described the above four echelons of defense. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," and the associated Staff Requirements Memorandum addressed defense against CCFs in digital I&C systems, among other issues. SECY-91-292 and SECY-93-087 did not address the consolidation of these echelons of defense-in-depth into one digital system, and neither did the Commission address combining echelons of defense at the time it established policy on digital system CCFs.

The industry is considering the use of digital I&C systems that combine all RTS and ESFAS functions within a single digital system software program. Combining two echelons of defense into a single software program could introduce new common-cause digital system failure mechanisms that do not exist in systems that use separate software programs, including software CCFs. These CCFs can be satisfactorily addressed if the criteria of ISG Problems 1 and 2 are met.

**Draft Interim Staff Guidance**

The RTS and ESFAS functions may be combined into a single digital platform if the criteria of the ISG addressing Problems 1 and 2 are met.