U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

BRANCH TECHNICAL POSITION 7-19

GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS

REVIEW RESPONSIBILITIES

Primary – Organization responsible for the review of instrumentation and controls

Secondary – Organization responsible for the review of reactor systems

A. BACKGROUND

Digital instrumentation and control (I&C) systems can be vulnerable to common-cause failures caused by software errors, which could defeat the redundancy achieved by hardware architecture. In NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," the staff documented a diversity and defense-in-depth (D3) analysis of a digital computer-based reactor protection system in which defense against common-cause failures was based on an approach using a specified degree of system separation between echelons of defense. Subsequently, in SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," the Staff included discussion of its concerns about common-cause failures in digital systems used in nuclear power plants. As a result of the reviews of advanced light-water reactor (ALWR) design certification applications for designs that use digital protection systems, the staff has documented its position with respect to common-cause failures in digital systems and defense-in-depth. This position was documented

as Item II.Q in SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," and was subsequently modified in the associated staff requirements memorandum (SRM). Based on experience in the detailed reviews, the NRC staff has established acceptance guidelines for D3 assessments as described in this branch technical position (BTP).

1. Regulatory Basis

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with Institute of Electrical & Electronics Engineers (IEEE) Standard (Std.) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before January 1, 1971, the applicant/licensee may elect to comply instead with their plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991, Clause 5.1, requires in part that "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." IEEE Std. 279-1971, Clause 4.2, requires in part that "any single failure within the protection system shall not prevent proper protective action at the system level when required."

10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram [ATWS]," requires in part various diverse methods of responding to ATWS.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21, "Protection Systems Reliability and Testability," requires in part that "no single failure results in the loss of the protection system."

GDC 22, "Protection System Independence," requires in part "that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions … 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."

GDC 24, "Separation of Protection and Control Systems," requires in part that "[i]nterconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

GDC 29, "Protection Against Anticipated Operational Occurrences," requires in part defense against anticipated operational transients "to assure an extremely high probability of accomplishing … safety functions."

2. Relevant Guidance

Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety

Systems," providing supplements and an interpretation. IEEE Std. 379-2000, Clause 5.5, identifies D3 as a technique for addressing common-cause failure, and Clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," summarizes several D3 analyses performed after 1990 and presents a method for performing such analyses.

The SRM on SECY 93-087 describes the NRC position on D3.

3. Purpose

The purpose of this BTP is to provide guidance for evaluating an applicant/licensee's D3 assessment and the design of manual controls and displays to ensure conformance with the NRC position on D3 for I&C systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS). This BTP has the objective of confirming that vulnerabilities to common-cause failures have been addressed in accordance with the guidance of the SRM on SECY-93-087, specifically:

- Verify that adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements.
- Verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements.
- Verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the protection systems.

B. BRANCH TECHNICAL POSITION

1. Introduction

The Staff has identified four echelons of defense against common-cause failures:

- Control System - The control system echelon consists of non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used in the normal operation of the reactor.
- Reactor Trip System - The RTS echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- Engineered Safety Features Actuation System - The ESFAS echelon consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).
- Monitoring and Indicators - The monitoring and indicators echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

As a result of the reviews of ALWR design certification applications for designs that use digital protection systems, the NRC has established the following four-point position on D3 for ALWRs and for digital system modifications to operating plants:

Point 1 The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.

Point 2 In performing the assessment, the vendor or applicant/licensee should 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 or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.

Point 3 If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. 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.

Point 4 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 above four-point position is based on the NRC concern that software design errors are a credible source of common-cause failures. Software cannot typically be proven to be error-free and is therefore considered susceptible to common-cause failures because identical copies of the software are present in redundant channels of safety-related systems. For digital system modifications to operating plants, retention of existing displays and controls in the main control room may satisfy Point 4.

To defend against potential common-cause failures, the staff considers high quality system designs, including the use of defensive design measures to avoid or tolerate faults and to cope with unanticipated conditions, and D3 to be key elements in digital system design. High-quality software and hardware reduce failure probability. However, despite high quality of design and use of defensive design measures, software errors may still defeat safety functions in redundant, safety-related channels. Therefore, as set forth in Points 1, 2, and 3, the Staff requires that the applicant/licensee perform a D3 assessment of the proposed digital I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed. In this assessment, the applicant/licensee should analyze design basis events (as identified in the SAR). If a postulated common-cause failure could disable a safety function that is required to respond to the design basis event being analyzed, a diverse means of effective response (with documented basis) is necessary. The diverse means may be an automatic or manual non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

The D3 analysis methods used in ALWR design certification and for operating plant retrofits are documented in NUREG/CR-6303. This document describes an acceptable method for performing such assessments.

When the RTS or ATWS mitigation system in an operating plant is modified, the requirements of the ATWS rule, 10 CFR 50.62, must be met. 10 CFR 50.62 requires that the ATWS mitigation system be composed of equipment that is diverse from the RTS. If "sufficient" difference in manufacturer cannot be demonstrated, a case-by-case assessment of the mitigation system designs should be conducted. This analysis should include differences such as manufacturing division (within a corporate entity), software (including implementation language), equipment (including central processing unit architecture), function, people (design and verification/validation team), and initiating events.

2. Information to be Reviewed

The information to be reviewed is the D3 assessment conducted by the applicant/licensee.

3. Acceptance Criteria

The D3 assessment submitted by the applicant/licensee should demonstrate compliance with the four-point position described above. To reach a conclusion of acceptability, the following four conclusions should be reached and supported by summation of the results of the analyses. Since the acceptance criteria address confirmation that anticipated operational occurrences and design basis accidents are mitigated in the presence of common-cause failure, D3 analyses focus on the protection systems. Other systems important to safety become involved only to the extent that they are credited as providing diverse functions to protect against common-cause failures in the protection systems.

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary. 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.

2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, 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). 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.

3. When a failure of a common element or signal source shared by the control system and RTS is postulated and the common-cause failure results in a plant response that requires reactor trip and also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should assure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary.

4. When a failure of a common element or signal source shared by the control system and ESFAS is postulated and the common-cause failure results in a plant response that requires engineered safety features (ESF) and also impairs the ESF function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should assure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary.

5. No failure of monitoring or display systems should influence the functioning of the RTS or ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated for by protection system function.

The adequacy of the diversity provided with respect to the above criteria must be justified.

Interconnections between the RTS and ESFAS (for interlocks providing for reactor trip if certain ESFs are initiated, ESF initiation when a reactor trip occurs, or operating bypass functions) are permitted if it can be demonstrated that the functions required by the ATWS rule (10 CFR 50.62) are not impaired.

NUREG/CR-6303, Section 3.2, describes six types of diversity and describes how instances of different types of diversity might be combined into an overall case for the sufficiency of the diversity provided. Typically, several types of diversity should exist, some of which should exhibit one or more of the stronger attributes listed in NUREG/CR-6303. Functional diversity and signal diversity are considered to be particularly effective. The following cautions should be noted where applicable:

- The justification for equipment diversity, or for the diversity of related system software such as a real-time operating system, must extend to the equipment's components to assure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating common failure causes. Claims for diversity based just on difference in manufacturer name are insufficient without consideration of the above.

- With respect to software diversity, experience indicates that independence of failure causes may not be achieved in cases where multiple versions of software are developed using the same software requirements. Other considerations, such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity.

Displays and manual controls provided for compliance with Point 4 of the NRC position on D3 should be sufficient both for monitoring the plant state and to enable control room operators to actuate the systems that will place the plant in a hot shutdown condition. In addition, the displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. This additional manual capability is necessary in new reactors because all of the protection and control systems are digital-computer-based and thus vulnerable to common-cause failure. These displays and controls provide plant operators with information and control capabilities that are not subject to common-cause failures due to software errors in the plant's automatic digital I&C safety system because they are independent and diverse from that system.

The point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. To achieve system-level actuation at the lowest possible level in the safety system architecture, the controls may be connected either to discrete hardwired components or to simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.

The displays may include digital components that are dedicated exclusively to the display function. Functional characteristics (e.g., range, accuracy, time response) should be sufficient to provide operators with the information needed to place and maintain the plant in a hot shutdown condition.

Human factors engineering principles and criteria should be applied to the selection and design of the displays and controls. Human-performance requirements should be described and related to the plant safety criteria. Recognized human-factors standards and design techniques should be employed to support the described human-performance requirements.

4. Review Procedures

The applicant/licensee's D3 analysis is reviewed against the above acceptance criteria using the detailed guidance of NUREG/CR-6303. Emphasis should be given to the following topics:

System Representation as Blocks

The system being assessed is represented as a block diagram; the inner workings of the blocks are not necessarily shown. Diversity is determined at the block level. A block is a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment or software.

Examples of typical blocks are computers, local area networks, and programmable logic controllers.

Documentation of Assumptions

Assumptions made to compensate for missing information in the design description materials or to explain particular interpretations of the analysis guidelines as applied to the system are documented by the applicant/licensee.

Postulated Common-Cause Failures

In certain cases, the Staff has concluded that software-based components are sufficiently simple and deterministic in performance that measures such as, for example, online error checking and exhaustive testing provide adequate assurance that the component is not a significant source of common-cause failure. Common-cause failure of such components need not be considered in the course of a D3 analysis. When a basis is given that a block is not susceptible to software common-cause failure, the Staff should examine the justification carefully. The safety evaluation of Westinghouse WCAP-15413, “Westinghouse 7300a ASIC-Based Replacement Module Licensing Summary Report," provides an example of the basis for such a determination.

Effect of Other Blocks

When considering the effects of a postulated common-cause failure, diverse blocks are assumed to function correctly. This includes functions of blocks that act to prevent or mitigate consequences of the common-cause failure under consideration.

Identification of Alternate Trip or Initiation Sequences

Thermal-hydraulic analyses, using best-estimate (realistic assumptions) methods, of the sequence of events that would occur if the primary trip channel failed to trip the reactor or actuate ESF are included in the assessment. (Coordination with the organization responsible for the review of reactor systems is necessary in reviewing these analyses.)

Identification of Alternative Mitigation Capability

For each design basis event, alternate mitigation actuation functions that will prevent or mitigate core damage and unacceptable release of radioactivity are identified.

When a common-cause failure is compensated by a different automatic function, a basis is provided that demonstrates that the different function constitutes adequate mitigation for the conditions of the event.

When operator action is cited as the diverse means for response to an event, the applicant/licensee should demonstrate that adequate information (indication), appropriate operator training, and sufficient time for operator action are available.

Justification for Not Correcting Specific Vulnerabilities

If any identified vulnerabilities are not addressed by design modification, refined analyses, or provision of alternate trip, initiation, or mitigation capability, justification should be provided.

C. REFERENCES

1. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

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

3. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

4. NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.

5 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

6. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2003.

7. SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," September 1991.

8. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993.

9. Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 15, 1993.

10. Safety Evaluation by the Office of Nuclear Reactor Regulation Westinghouse Electric Company Topical Report WCAP-15413, "Westinghouse 7300a ASIC-Based Replacement Module Licensing Summary Report," Project No. 700, Office of Nuclear Reactor Regulation, February 8, 2001.
