NEW

Branch Technical Position HICB-19

Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

A. Background

Digital instrumentation and control (I&C) systems are vulnerable to common-mode failure caused by software error, which defeats the redundancy achieved by hardware architecture. In NUREG-0493, "A Defense-in-Depth & Diversity Assessment of the RESAR-414 Integrated Protection System," the Staff documented a defense-in-depth and diversity (D-in-D&D) analysis of a digital computer-based reactor protection system, in which defense against common-mode failures was based upon 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-mode failures in digital systems used in nuclear power plants. As a result of the reviews of ALWR design certification applications that used digital protection systems, the Staff documented its position with respect to common-mode 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. Based on experience in the detailed reviews, the NRC staff has established acceptance guidelines for D-in-D&D assessments as described in this branch technical position.

1. Regulatory Basis

10 CFR 50.55a(h), "Protection Systems," requires in part that protection systems satisfy the criteria of ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." Section 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," requires in part various diverse methods of responding to anticipated transients without scram (ATWS).

10 CFR 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."

10 CFR 50 Appendix A, GDC 22, "Protection System Independence," requires in part that the effects of natural phenomena, postulated accident conditions, normal operating, maintenance, and testing not result in the loss of protective 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."

10 CFR 50 Appendix A, GDC 24, "Separation of Protection and Control Systems," requires in part that "Interaction of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

10 CFR 50 Appendix A, 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

Reg. Guide 1.53 "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses ANSI/IEEE Std 379, "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation.

Reg. Guide 1.153 "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," as an alternative to ANSI/IEEE Std 279.

NUREG-0493 is the first formal defense-in-depth and diversity assessment of a reactor protection system, the RESAR-414.

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

The Staff Requirements Memorandum on SECY 93-087 describes the NRC position on defense-in-depth and diversity.

3. Purpose

The purpose of this branch technical position is to provide guidance for review of an applicant/licensee's D-in-D&D assessment and design of manual controls and displays to ensure that the requirements of the NRC position on D-in-D&D for I&C systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS) are followed. This branch technical position has three objectives:

- To verify that adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements.

- To verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements.

- To 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 reactor protection system and ESFAS.

B. Branch Technical Position

1. Introduction

Based on experience in detailed reviews, the Staff has established acceptance guidelines for D-in-D&D assessments. The Staff has identified four echelons of defense against common-mode failures:

- Control system — The control echelon consists of that non-safety equipment which routinely prevents reactor excursions toward unsafe regimes of operation, and is used for normal operation of the reactor.

- RTS — The reactor trip echelon consists of that safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- ESFAS — The ESFAS echelon consists of that safety equipment which 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 indication 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 that used digital protection systems, the NRC established the following position on D-in-D&D for the advanced reactors. Points 1, 2, and 3 of this position apply to digital system modifications to operating plants.

1. The applicant/licensee should assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant/licensee shall analyze each postulated common-mode 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/licensee shall demonstrate adequate diversity within the design for each of these events.

3. 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, should be required to perform either the same function or a different function. 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.

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 monitoring of parameters that support the safety functions. The displays and controls should be independent and diverse from the safety computer systems identified in items 1 and 3 above.

The above position is based on the NRC concern that software design errors are a credible source of common-mode failures. Software cannot be proven to be error-free, and therefore is considered susceptible to common-mode failures because identical copies of the software are present in redundant channels of safety-related systems. To defend against potential common-mode failures, the Staff considers high quality,

defense-in-depth, and diversity to be key elements in digital system design. High-quality software and hardware reduces failure probability. However, despite high quality of design, software errors may still defeat safety functions in redundant, safety-related channels. Therefore, as set forth in points 1, 2, and 3 above, the Staff requires that the applicant/licensee perform a D-in-D&D assessment of the proposed digital I&C system to demonstrate that vulnerabilities to common-mode failures have been adequately addressed. In this assessment, the applicant/licensee should analyze design basis events (as identified in the safety analysis report). If a postulated common-mode failure could disable a safety function that is required to respond to the design basis event being analyzed, then a diverse means of effective response (with documented basis) is necessary. The diverse means may be a non-safety system, automatic, or manual if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

The methods and results of D-in-D&D assessments used in ALWR design certification submissions are documented in NUREG/CR-6303. This document describes an acceptable method for performing such assessments.

In those cases where 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 diverse equipment from the RTS. Therefore implementation of RTS digital modifications by a different manufacturer from the ATWS mitigation system satisfies the diversity requirements of 10 CFR 50.62. This is also true in the complementary case in which an existing ATWS system is modified by the inclusion of digital equipment and the RTS is already digital. If "sufficient" difference in manufacturer cannot be demonstrated, then a case-by-case assessment of the RTS and ATWS 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 CPU architecture), function, people (design and verification/validation team), and initiating events.

2. Information to be Reviewed

The information to be reviewed is the D-in-D&D assessment conducted by the applicant/licensee.

3. Acceptance Criteria

The D-in-D&D 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:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode 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 either (1)

demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

3. When a failure of a common element or signal source shared between the control system and the RTS is postulated, and (1) this common-mode failure results in a plant response that requires reactor trip, and (2) the common-mode failure 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 ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

   When a failure of a common element or signal source shared between the control system and the ESFAS is postulated, and (1) this common-mode failure results in a plant response that requires ESF, and (2) the common-mode failure 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 ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

   Interconnections between reactor trip and ESFAS (for interlocks providing for (1) reactor trip if certain ESFs are initiated, (2) ESF initiation when a reactor trip occurs, or (3) operating bypass functions) are permitted provided that it can be demonstrated that functions required by the ATWS rule (10 CFR 50.62) are not impaired.

4. No failure of monitoring or display systems should influence the functioning of the reactor trip system or the 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 by protection system function.

The adequacy of the diversity provided with respect to the above criteria must be justified. NUREG/CR-6303, in 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 for the diversity type. 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 ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby incorporating common failure modes. 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 modes may not be achieved in cases where multiple versions of software are developed to the same software requirements. Other considerations, such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity.

Manual displays and controls provided for compliance with the fourth point of the NRC position on D-in-D&D should be sufficient to both monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition. In addition, the displays and controls should 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 advanced reactors because all of the protection and control systems are digital-computer-based, and thus vulnerable to common-mode failure. The manual capability should consist of hardwired, system-level controls and displays. These controls provide plant operators with information and control capabilities that are not subject to common-mode failures caused by software errors in the plant's automatic digital I&C safety 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, but 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 hardwired either to analog components or to simple (e.g., the component function can be completely demonstrated by test), dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.

These displays may include digital components that are exclusively dedicated to the display function. The functional characteristics (e.g., range, accuracy, time response) of the displays provided 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. The 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 D-in-D&D 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.

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.

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 were to fail to trip the reactor or actuate ESF are included in the

assessment. (Coordination with the Reactor Systems Branch, the Mechanical Engineering Branch, and the Materials and Chemical Engineering Branch is necessary in reviewing these analyses.)

Identification of Alternative Mitigation Capability

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

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

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

Justification for Not Correcting Specific Vulnerabilities

If any identified vulnerabilities are not addressed by provision of alternate trip, initiation, or mitigation capability, justification should be provided. Justification may be based upon the availability of systems outside of the scope of the analysis that act to prevent or mitigate the event of concern. For example, I&C system vulnerability to common-mode failure affecting the response to large-break loss-of-coolant accidents and main steam line breaks has been accepted in the past. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs.

C. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

ANSI/IEEE Std 379-1988. "Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."

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

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

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

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.53. "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

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

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

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.