



# 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 (I&Cs)

**Secondary** – Organization responsible for the review of reactor systems and the organization responsible for the review of human factors engineering (HFE)

### A. BACKGROUND

Digital instrumentation and control (DI&C) systems can be vulnerable to common-cause failure (CCF) caused by software errors or software developed logic, 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 U.S. Nuclear Regulatory Commission (NRC) staff documented a diversity and defense-in-depth (D3) analysis of a digital computer-based Reactor Protection System (RPS) in which defense against software CCF (or simply CCF hereafter) was based upon an approach using a specified degree of system separation between echelons of defense. The RPS consists of the Reactor Trip System (RTS) and the Engineered Safety Features Actuation System (ESFAS). Subsequently, in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," the NRC staff included discussion of its concerns about CCF in digital systems used in nuclear power plants (NPPs).

Revision 6 – March 2010

---

### USNRC STANDARD REVIEW PLAN

This Standard Review Plan (SRP), NUREG-0800, has been prepared to establish criteria that the NRC staff responsible for the review of applications to construct and operate nuclear power plants intends to use in evaluating whether an applicant/licensee meets the NRC's regulations. The SRP is not a substitute for the NRC's regulations, and compliance with it is not required. However, an applicant is required to identify differences between the design features, analytical techniques, and procedural measures proposed for its facility and the SRP acceptance criteria and evaluate how the proposed alternatives to the SRP acceptance criteria provide an acceptable method of complying with the NRC regulations.

The SRP sections are numbered in accordance with corresponding sections in Regulatory Guide 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)." Not all sections of RG 1.70 have a corresponding review plan section. The SRP sections applicable to a combined license application for a new light-water reactor (LWR) are based on RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)."

These documents are made available to the public as part of the NRC's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Individual sections of NUREG-0800 will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience. Comments may be submitted electronically by email to [NRR\\_SRP@nrc.gov](mailto:NRR_SRP@nrc.gov).

Requests for single copies of SRP sections (which may be reproduced) should be made to the U.S. Nuclear Regulatory Commission, Washington, DC 20555, Attention: Reproduction and Distribution Services Section, or by fax to (301) 415-2289; or by email to [DISTRIBUTION@nrc.gov](mailto:DISTRIBUTION@nrc.gov). Electronic copies of this section are available through the NRC's public Web site at <http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/>, or in the NRC's Agencywide Documents Access and Management System (ADAMS), at <http://www.nrc.gov/reading-rm/adams.html>, under Accession # ML093490771.

---

As a result of reviews of advanced light-water reactor (ALWR) design certification (DC) applications for designs using digital protection systems, the NRC staff documented its position with respect to CCF in digital systems and D3. 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). SECY-91-292 and SECY-93-087 did not address the consolidation of the four echelons of D3 (echelons described in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems") into one digital system, nor did the Commission address combining echelons of defense at the time it established policy on CCF.

On the basis of experience in detailed reviews, the NRC staff has established acceptance guidelines for D3 assessments as described in this branch technical position (BTP). Further guidance reflected herein was established through the efforts of the DI&C Task Working Group #2 on D3 with the development of DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues Interim Staff Guidance," Revision 2. This interim staff guidance (ISG) was developed with extensive review of D3 issues including both internal review within the NRC and external input through public meetings with representatives from industry, vendors, and the general public.

In summary, while the NRC considers (software) CCF in digital systems to be beyond design basis, digital safety systems should be protected against the effects of CCF.

#### 1. Regulatory Basis

Title 10 of the *Code of Federal Regulations*, Section 50.55a(h) (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 NPPs with construction permits (CPs) issued before January 1, 1971, the applicant/licensee may elect to comply instead with its plant-specific licensing basis. For NPPs with CPs 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 (DBE) 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) Events for Light-water-cooled Nuclear Power Plants," requires in part various diverse methods of responding to ATWS.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that "Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in the loss of the protection function."

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

10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," governs the issuance of early site permits, standard DCs, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities.

10 CFR Part 100, "Reactor Site Criteria," provides guideline values for fission product releases from NPPs licensed to operate prior to January 10, 1997 that have voluntarily implemented an alternative source term under the provisions of 10 CFR 50.67.

- 10 CFR 50.67 provides guideline values for fission product releases from currently operating NPPs that have implemented an alternative source term.
- 10 CFR 50.34(a)(1)(ii)(D) provides guideline values for CP applicants and NPPs licensed to operate under Part 50 after January 10, 1997.
- 10 CFR 52.47(a)(2)(iv) provides guideline values for standard design certifications.
- 10 CFR 52.79(a)(1)(vi) provides guideline values for combined licenses.
- 10 CFR 52.137(a)(2)(iv) provides guideline values for standard design approvals.
- 10 CFR 52.157 (d) provides guideline values for manufacturing license approvals.

These guideline values can be commonly referred to as the siting dose guideline values.

## 2. Relevant Guidance

Regulatory Guide (RG) 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 CCF, and Clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion.

RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with a few noted exceptions, provides guidance for complying with requirements for safety systems that use digital computers. Additional guidance on the application of IEEE Std. 7-4.3.2 is provided in Standard Review Plan (SRP) Appendix 7.1-D.

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.

Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," April 16, 1985, provides quality assurance guidance for non-safety-related ATWS equipment.

NUREG-800, SRP Chapter 18, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," defines a methodology, applicable to both existing and new reactors, for evaluating manual operator actions as a diverse means of coping with Anticipated Operational Occurrences and Postulated Accidents that are concurrent with a software CCF of the digital I&C protection system.

### 3. Purpose

The purpose of this BTP is to provide guidance for evaluating an applicant/licensee's D3 assessment, design, and the design of manual controls and displays to ensure conformance with the NRC position on D3 for I&C systems incorporating digital, software-based or software-logic-based RTS or ESFAS. This BTP has the objective of confirming that vulnerabilities to CCF have been addressed in accordance with the guidance of the SRM on SECY-93-087 and clarification from ISG, DI&C-ISG-02, Revision 2, specifically:

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

## **B. BRANCH TECHNICAL POSITION**

### 1. Introduction

#### 1.1 Echelons of Defense

The NRC staff identified four echelons of defense against CCFs in NUREG/CR-6303:

- Control System - The control system echelon consists of (usually) non-safety equipment that is used in the normal operation of a NPP and routinely prevents operations in unsafe regimes of NPP operations.
- RTS - The RTS echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.
- ESFAS - 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 primary cooling system, and containment).
- Monitoring and Indicators - The monitoring and indicators echelon consists of sensors, displays, data communication systems, and manual controls required by operators to respond to NPP operating events.

## 1.2 Plant Critical Safety Functions

As described in NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements," sufficient information should be provided to the nuclear reactor operators to monitor (and thereby control) the following plant critical safety functions and conditions:

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

## 1.3 Combining RTS and ESFAS

Earlier traditional I&C echelons of defense architectures consisted of discrete and separate components in four echelons of defense. In digital systems, formerly discrete systems (e.g., the RTS and the ESFAS) could be combined into a single DI&C system. Digital systems that combine most, if not all RTS and ESFAS functions within a single digital system in both new NPP designs and upgrades to current operating plant systems could introduce new CCF mechanisms that do not exist in systems that use separate discrete components. However, the four echelons of defense described above are only conceptual and, with the exception of the monitoring and indication echelon of defense noted in Point 4 (see Section 1.4, "Four-Point Position"), NRC regulations do not require nor does this guidance imply that RTS and ESFAS echelons of defense must be independent or diverse from each other. Plant responses to postulated CCF that could impair a safety function should be in accordance with the acceptance criteria of this BTP, regardless of the echelons of defense that may be affected.

## 1.4 Four-Point Position

On the basis of reviews of the ALWR DC applications for designs that use digital safety systems, the NRC has established the following four-point position on D3 for new reactor designs 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 CCF have been adequately addressed.
  
- Point 2        In performing the assessment, the vendor or applicant/licensee should analyze each postulated CCF for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using either realistic assumptions (e.g., plant operating at normal power levels, temperatures, pressures, flows, normal alignments of equipment, etc.) to analyze the plant response to design basis events, or using 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 CCF could disable a safety function, the applicant/licensee should identify an existing diverse means or add a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF to perform either the same function as the safety system function that is vulnerable to the CCF 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 (see Section 1.6, "D3 Assessment").
  
- Point 4        In addition to the above three points, a set of displays and controls (safety or non-safety) should be provided in the main control room (MCR) for manual system level 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, RCS integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the safety systems in Points 1-3 discussed above. However, these displays and controls could be those used for manual operator action. Where they serve as backup capabilities, the displays and controls also should be able to function downstream of the lowest-level components subject to the CCF that necessitated the use of the diverse backup system or function.  
One example would be the use of hard-wired connections. For digital system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy this point (see Section 1.5, "Safety-Related Manual Actuation"). However, if existing displays and controls are digital and/or the same platform is used this point may not be satisfied.

The above four-point position is based on the NRC concern that software based or software logic based digital system development errors are a credible source of CCF. In this guidance,

common software includes software, firmware<sup>1</sup>, and logic developed from software-based development systems. Generally, digital systems cannot be proven to be error-free and, therefore, are considered susceptible to CCF because identical copies of the software based logic and architecture are present in redundant channels of safety-related systems. Also, some errors labeled as “software errors” (for example) actually result from errors in the higher level requirements specifications used to direct the system development that fail in some way to represent the actual process. Such errors further place emphasis on the use of diversity to avoid or mitigate CCF.

## 1.5 Safety-Related Manual Actuation

Two types of manual actuation methods may be required. For safety systems, to satisfy IEEE Std. 603 -1991, Clauses 6.2 and 7.2, which are incorporated by reference in 10 CFR 50.55a(h), a safety-related means shall be provided in the control room to implement manual initiation at the division level of the RPS functions. Point 3 states that not only should there be a diverse backup means for the automated safety-related RPS subject to a potential CCF, but if the required safety-related RPS manual actuation system (required per IEEE Std. 603 – 1991) is also subject to the same CCF as the automated safety-related actuation system, then a diverse manual backup actuation (safety or non-safety) should also be provided. The indicators and controls described in Point 4 may be able to address the need for this independent and diverse manual actuation backup. If an IEEE Std. 603 -1991 required safety-related manual actuation system is independent and sufficiently diverse from the automated safety-related RPS actuation system, then a second diverse non-safety related manual actuation system would not be needed.

## 1.6 D3 Assessment

To defend against potential CCF, the NRC staff considers D3 and the use of defensive measures to avoid or tolerate faults and to cope with unanticipated conditions to be key elements in high quality digital system designs. However, despite high quality in the development and use of defensive design measures, system errors could still defeat safety functions in redundant, safety-related channels. Therefore, as set forth in Points 1, 2, and 3, the applicant/licensee should perform a D3 assessment of the proposed DI&C system to demonstrate that vulnerabilities to CCF have been adequately addressed. In this assessment, the applicant/licensee may use realistic assumptions (e.g., plant operating at normal power levels, temperatures, pressures, flows, normal alignments of equipment, etc.) to analyze the plant response to DBEs (as identified in the SAR). If a postulated CCF could disable a safety function that is required to respond to the DBE being analyzed, an independent and diverse means of effective response (with documented basis) is necessary. The D3 analysis methods used in ALWR DC and for operating plant upgrades are documented in NUREG/CR-6303, which describes an acceptable method for performing such assessments.

When the RTS and ATWS mitigation system in an operating plant is modified, the requirements of the ATWS rule, 10 CFR 50.62, must be met. The 10 CFR 50.62 regulation requires that the

---

<sup>1</sup> IEEE 100, “The Authoritative Dictionary of IEEE Standards Terms,” defines firmware as the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

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 control processing unit architecture), function, people (design and verification/validation team), and initiating events.

### 1.7 Diverse Backup Method

When an independent and diverse method is needed as a backup to an automated system used to accomplish a required safety function as a result of the D3 assessment identifying a potential CCF, the backup function can be accomplished via either an automated system, or manual operator actions performed from the MCR. The preferred independent and diverse backup method is generally an automated system.

### 1.8 Potential Effects of CCF: Failure to Actuate and Spurious Actuation

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 or 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

A simple failure of the total system might not be the worst case failure, particularly when analyzing the time required for identifying and responding to the condition. For example, a failure to trip might not be as limiting as a partial actuation of an emergency core cooling system (ECCS), but with indication of a successful actuation. In cases such as this, it may take an operator longer to evaluate and correct the safety system failure than it would if there was a total failure to send any actuation signal. For this reason, the evaluation of failure modes as a result of CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate. 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 addressed; however, failures that are non-detectable may prevent a system actuation when required. Consequently, non-detectable faults are of concern. Therefore, a diverse means to provide the required safety function, or some other safety function that will adequately address each licensing-basis event should be provided.

Software or software logic based CCF was declared a “beyond-DBE” by the Commission in the SRM issued in response to SECY-93-087. Such a CCF that causes an undesired trip or actuation can be detected (although not always anticipated) because this type of failure is self-announcing. However, there may be circumstances in which a spurious trip or actuation would not occur until a particular signal or set of signals occur. 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.

Spurious actuations caused by CCF may challenge safety systems if the actuated equipment places the plant into an unsafe condition. For example, a spurious actuation of the ECCS high pressure injection system could increase the primary coolant system pressure of a pressurized water reactor and thereby challenge the pressurizer safety valves, which could lead to a small break loss of coolant accident. The effects of spurious trips and actuations should be evaluated by the applicant/licensee.

#### 1.9 Design Attributes to Eliminate Consideration of CCF

Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, there are two design attributes that are sufficient to eliminate consideration of software based or software logic based CCF:

- (1) Diversity – If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels use a diverse digital system. A D3 analysis performed consistent with the guidance in NUREG/CR-6303 determines that the two diverse digital systems are not subject to a CCF. In this case, no additional diversity would be necessary in the safety system.

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

What constitutes “sufficient diversity” should be evaluated on a case-by-case basis, considering diversity attributes and attribute criteria that preclude or limit certain types of CCF. Diversity attributes and associated attribute criteria, and a process for evaluating the application may provide more objective guidance in answering, “What is sufficient diversity?”.

## 2. Information to be Reviewed

The information to be reviewed is the D3 assessment conducted by the applicant/licensee. If the D3 assessment indicates the need for a diverse means to accomplish a protective safety function, then the independent and diverse backup means should be evaluated, including any HFE analysis associated with manual operator actions as an independent and diverse backup method.

## 3. Acceptance Criteria

### 3.1 Specific 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 conclusions should be reached and supported by summation of the results of the analyses and the independent and diverse backup methods provided. Since the acceptance criteria address confirmation that anticipated operational occurrences and design-basis accidents (DBAs) are mitigated in the presence of CCF, the focus of the D3 analyses should be 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 CCF in the protection systems.

- (1) For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions (e.g., plant operating at normal power levels, temperatures, pressures, flows, normal alignments of equipment, etc.) analyses should not result in radiation release exceeding 10 percent of the applicable siting dose guideline values 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 CCF, the plant response calculated using realistic assumptions analyses should not result in radiation release exceeding the applicable siting dose 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 CCF 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 realistic assumptions analyses does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values 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 CCF 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 realistic assumptions analyses does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values 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 a 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.
- (6) For safety systems to satisfy IEEE Std. 603–1991 Clauses 6.2 and 7.2, which are incorporated by reference in 10 CFR 50.55a(h), a safety-related means shall be provided in the control room to implement manual initiation at the division level of the RTS and ESFAS functions. The means provided shall minimize the number of discrete operator manual manipulations and shall depend on operation of a minimum of equipment. If the means is independent and diverse from the safety-related automatically initiated RTS and ESFAS functions, the design meets the system-level actuation criterion in Point 4 of this BTP. If credit is taken for a manual actuation method that meets both the IEEE Std. 603–1991, Clauses 6.2 and 7.2 requirements and a need for a diverse manual backup, then the applicant/licensee should demonstrate that the criteria are satisfied and sufficient diversity exists.
- (7) If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the independent and diverse means of actuating the protective safety functions can be accomplished via either an automated system (see Section 3.4, “Use of Automation in Diverse Backup Safety Functions” below), or manual operator actions that meet HFE acceptability criteria (see Section 3.5, “Use of Manual Action in Diverse Backup Safety Functions” below.)
- (8) If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the independent and diverse means of actuating the protective safety functions should meet the following criteria: The independent and diverse means should be:
  - a) at the division level;
  - b) initiated from the control room;
  - c) capable of responding with sufficient time available for the operators to determine the need for protective actions even with malfunctioning indicators, if credited in the D3 coping analysis;
  - d) appropriate for the event;
  - e) supported by sufficient instrumentation that indicates:

1. the protective function is needed,
2. the safety-related automated system did not perform the protective function, and
3. the automated backup or manual action is successful in performing the safety function.

(9) If the D3 assessment reveals a potential for a CCF, then, in accordance with the augmented quality guidance for the independent and diverse backup system used to cope with a CCF, the design of a diverse automated or diverse manual backup actuation system should address how to minimize the potential for a spurious actuation of the protective system caused by the diverse system. Use of design techniques (for example: redundancy, conservative setpoint selection, and use of quality components) to mitigate these concerns is recommended.

The adequacy of the diversity provided with respect to the above criteria should be justified by the licensee/applicant and explicitly addressed in the staff's safety evaluation.

### 3.2 RTS and ESFAS Interconnection

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. Further, RTS and ESFAS could be combined into a single DI&C platform provided D3 is adequately addressed to protect against CCF.

### 3.3 Single Failure and CCF

Since CCF is not classified as a single failure (as defined in RG 1.53), postulated CCF need not be assumed to be a single failure in design basis evaluations. Consequently, realistic assumptions (e.g., plant operating at normal power levels, temperatures, pressures, flows, normal alignments of equipment, etc.) can be employed in performing analyses to evaluate the effect of CCF coincident with DBEs.

### 3.4 Use of Automation in Diverse Backup Safety Functions

If automation is used in the backup safety system functions, then the functions should be provided by equipment that is not affected by the postulated RPS CCF and should be sufficient to maintain plant conditions within recommended acceptance criteria for the particular anticipated operational occurrence or DBA. The automated backup function may be performed by a non-safety system, if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The automated backup systems should be similar in quality to systems required by the ATWS rule (10 CFR 50.62), as described in the enclosure to GL 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related." Other systems that are credited in the analysis that are in continuous use (e.g., the normal RCS inventory control system or normal steam generator level control system) are not required to be upgraded to the augmented quality discussed above.

### 3.5 Use of Manual Action in Diverse Backup Safety Functions

If manual operator actions are used as backup to safety system functions, a suitable HFE analysis should be performed by the applicant/licensee to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular anticipated operational occurrence or DBA. The acceptability of such actions is to be reviewed by the NRC staff in accordance with Appendix 18-A of SRP Chapter 18, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses."

Note: As the difference between time available and time required for operator action decreases, there is increasing potential that uncertainties in the estimate of time required will invalidate a conclusion that operators can perform the action reliably within the time available (e.g., less than 30 minutes between the time available and the time required for operators to perform the protective action).

Diverse backup system manual initiations of safety systems should be performed on a system-level basis for each division. This recommendation does not prohibit the use of manual controls for operating individual safety system components after the corresponding safety system functions have been actuated. The design and normal operation of any such non-safety displays and controls shall not prevent any safety systems from performing the intended protective safety function when actually required to be actuated.

### 3.6 Applicability to Current or New Plants

This guidance applies to both the currently operating NPPs licensed under 10 CFR Part 50 and new NPPs licensed under 10 CFR Part 52. The potential for CCF in digital safety systems should be considered whether the systems are to be used in new plants or for upgrades in existing plants. The main difference is that new NPPs predominantly will use digital technology, whereas currently operating plants may introduce digital upgrades in a phased approach. Therefore, Point 4 applies to new plants and to existing plants installing digital equipment in RTS or ESFAS.

### 3.7 Effects of CCF on Spurious Actuation

In general, spurious trips and actuations are of a lesser safety concern than failures to trip or actuate on demand by the RPS. There may be plant and safety system challenges and stresses; however, challenges that are significant are already set forth in plant design basis evaluations.

### 3.8 Diversity Types

NUREG/CR-6303 provides a method for determining uncompensated CCF in safety system designs. Section 2.6, "Diversity," of NUREG/CR-6303 defines six diversity attributes and 25 related diversity criteria. When NUREG/CR-6303 was published (December 1994), computer-based digital systems were assumed to comprise the next generation of safety systems. Proposed safety system designs, however, include digital systems that are not computer-based, such as programmable logic devices, field programmable gate arrays, and application-specific integrated circuits. These digital devices and components use software to develop the logic that later resides within the digital component (called "firmware") and often

cannot be changed in an individual component. These all should be considered in the determination of diversity.

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 logic such as a real-time operating system, should 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 on the basis of the difference in manufacturer name are insufficient without consideration of the above.
- With respect to computer software and software-based logic diversity, experience indicates that independence of failure causes may not be achieved in cases where multiple versions of software, for example, are developed using the same set of software, system, and logic requirements. Other considerations, such as technology, functional and signal diversity that lead to different software, system, and logic requirements form a stronger basis for diversity.

### 3.9 System Testability

If a portion or component of a system can be fully tested, then it can be considered not to have a potential for software-based CCF. Fully tested or 100% testing means testing every possible combination of inputs, internal and external states, and every signal path. Further, in assessing the system states, the guidance provided in IEEE Std. 7-4.3.2-2003, Clause 5.4.1, "Computer system [equipment qualification] testing," should be addressed:

"Computer system [equipment] 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."

The use of the term "software" or "software-based" should be extended to any form of logic that is used in a safety system to accomplish a safety system function and requires the use of software for its development. Similarly, the use of the phrase "All portions of a computer" should be extended to "All components of a safety system requiring a software development system."

Clause 5.4.1 of IEEE Std. 7-4.3.2-2003 directs 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 logic and diagnostics should be representative of the logic 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.

### 3.10 Displays and Manual Controls

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 systems that will place the plant in a safe 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 NPP designs because all of the protection and control systems are expected to be digital-based and thus vulnerable to CCF. These displays and controls provide plant operators with information and control capabilities that are not subject to CCF due to errors in the plant automatic DI&C safety systems because the displays and controls are independent and diverse from the safety system.

The point at which the manual controls are connected to safety equipment should be downstream of DI&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 a plant in a safe shutdown condition.

HFE 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

In reviewing the applicant/licensee's D3 analysis using the above acceptance criteria and the detailed guidance of NUREG/CR-6303, emphasis should be given to the following topics:

#### 4.1 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 and logic errors, will not propagate to other equipment or software.

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

#### 4.2 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.

#### 4.3 Postulated Common Cause Failures

In certain cases, the NRC staff has concluded that software-based components may be sufficiently simple and deterministic in performance that measures such as, for example, online error checking and exhaustive testing can provide adequate assurance that a component is not a significant source of CCF. CCF 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 CCF, the NRC 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.

#### 4.4 Effect of Other Blocks

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

#### 4.5 Identification of Alternate Trip or Initiation Sequences

Thermal-hydraulic analyses, using realistic assumptions (e.g., plant operating at normal power levels, temperatures, pressures, flows, normal alignments of equipment, etc.), 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.)

#### 4.6 Identification of Alternative Mitigation Capability

For each DBE, alternate mitigation actuation functions that will prevent or mitigate core damage and unacceptable release of radioactivity should be identified.

When a CCF 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 in accordance with Appendix 18-A of SRP Chapter 18.

Note: As the difference between time available and time required for operator action decreases, there is increasing potential that uncertainties in the estimate of time required will invalidate a conclusion that operators can perform the action reliably within the time available (e.g., less than 30 minutes between the time available and the time required for operators to perform a protective action).

#### 4.7 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. DI&C-ISG-02, "Task Working Group #2: Diversity and Defense-in-Depth Issues Interim Staff Guidance," Revision 2, USNRC, June 5, 2009 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML091590268).
2. NUREG-800, SRP Chapter 18, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses."
3. GL 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," April 16, 1985 (ADAMS Accession No. ML031140390).
4. IEEE 100, "The Authoritative Dictionary of Standards Terms."
5. IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."
6. IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems."
7. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
8. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations."
9. NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979.

10. NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements (GL No. 82-33)," December 17, 1982 (ADAMS Accession No. ML031080548).
11. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994 (ADAMS Legacy Library Accession No. 9501180332).
12. RG 1.53, "Application of the Single-Failure Criterion to Safety Systems," Office of Nuclear Regulatory Research (RES), USNRC, 2003.
13. RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," RES, USNRC, 2003.
14. 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 (ADAMS Accession No. ML010390526).
15. SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors," September 16, 1991 (ADAMS Accession No. ML051750018).
16. SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993 (ADAMS Accession No. ML003708021).
17. SRM on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," July 21, 1993 (ADAMS Accession No. ML003708056).

---

**PAPERWORK REDUCTION ACT STATEMENT**

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR Part 50 and 10 CFR Part 52, and were approved by the Office of Management and Budget, approval number 3150-0011 and 3150-0151.

**PUBLIC PROTECTION NOTIFICATION**

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

---