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&C)

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

Review Note: The revision numbers of Regulatory Guides (RG) and the years of endorsed industry standards referenced in this branch technical position (BTP) are centrally maintained in Standard Review Plan (SRP) Section 7.1-T, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety," (Table 7-1). Therefore, the individual revision numbers of RGs (except RG 1.97) and years of endorsed industry standards are not shown in this BTP. References to industry standards incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

Revision 7 – August 2016

USNRC STANDARD REVIEW PLAN

This Standard Review Plan (SRP), NUREG 0800, has been prepared to establish criteria that the U.S. Nuclear Regulatory Commission (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 regulations. The SRP is not a substitute for the NRC 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 (RG) 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 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 NRO_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 by fax to (301) 415 2289; or by email to DISTRIBUTION@nrc.gov. Electronic copies of this section are available through the NRC public Web site at http://www.nrc.gov/reading rm/doc collections/nuregs/staff/sr0800, or in the NRC Agencywide Documents Access and Management System (ADAMS), at http://www.nrc.gov/reading rm/adams.html under ADAMS Accession No. ML16019A344.

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 and the engineered safety features (ESF) 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).

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 18, 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).

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 No. 2 on D3 with the development of DI&C-ISG-02, "Task Working Group No. 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, NPPs should be protected against the effects of anticipated operational occurrences (AOOs) and postulated accidents with a concurrent CCF in the digital protection system.

1. Regulatory Basis

Title 10 of the *Code of Federal Regulations* (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 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 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 any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures."

IEEE Std 603-1991, Clause 6.2, “Manual Control,” requires in part that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions.

IEEE Std 603-1991, Clause 7.2, “Manual Control,” requires in part that the means of any manual control of any execute features shall not defeat requirements of Clauses 5.1 and 6.2.

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.”

IEEE Std 279-1971, Clause 4.17, “Manual Initiation,” requires in part that the protection system shall include means for manual initiation of each protective action at the system level.

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, “Domestic Licensing of Production and Utilization Facilities,” Appendix A, “General Design Criteria for Nuclear Power Plants,” 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 (ESPs), standard DCs, combined licenses (COLs), standard design approvals (SDAs), and manufacturing licenses (MLs) 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, “Accident Source Term.”

These guideline values can be commonly referred to as the site dose guideline values:

- 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 DCs.
- 10 CFR 52.79(a)(1)(vi) provides guideline values for COLs.
- 10 CFR 52.137(a)(2)(iv) provides guideline values for SDAs.
- 10 CFR 52.157(d) provides guideline values for ML approvals.

2. Relevant Guidance

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, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation.

IEEE Std 379, Clause 5.5, establishes the relationship between CCF and single failures by defining criteria for CCF's that are not subject to single-failure analysis. This clause also identifies D3 as a technique for addressing CCF.

RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "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 SRP, Chapter 7, Appendix 7.1-D.

RG 1.62, "Manual Initiation of Protective Actions," includes information on diverse manual initiation of protective action.

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 in Item 18, II.Q. Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related," April 16, 1985, provides quality assurance guidance for nonsafety-related ATWS equipment.

NUREG-0800, 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 AOOs

and postulated accidents that are concurrent with a software CCF of the DI&C protection system.

NUREG-0800, SRP Section 7.8, “Diverse Instrumentation and Control Systems,” describes the review process and additional acceptance criteria for diverse I&C systems provided to protect against CCF.

3. Purpose

The purpose of this BTP is to provide guidance for evaluating an applicant’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 ESF, auxiliary supporting features, and other auxiliary features as appropriate. 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 provided in this staff guidance, specifically:

- Verify that adequate diversity has been provided in a design to meet the criteria established by NRC guidance.

- Verify that adequate defense-in-depth has been provided in a design to meet the criteria established by NRC guidance.

- Verify that the displays and manual controls for plant 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 in NUREG/CR-6303:

- Control System - The control system echelon usually consists of equipment that is not safety-related that is used in the normal operation of a NPP and routinely prevents operations in unsafe regimes of NPP operations.

- Reactor Trip System - The RTS echelon consists of safety-related equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- Engineered Safety Features - The ESF echelon consists of safety-related 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) and the logic components used to actuate this safety-related equipment, usually referred to as the ESF Actuation System, and controls.

- Monitoring and Indicator System - The monitoring and indicator system echelon consists of sensors, safety parameter displays, data communication systems, and independent manual controls relied upon 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

In addition to divisional independence, many earlier analog I&C architectures consisted of discrete and separate analog components in each echelon 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 using a limited number of digital components in both new NPP designs and upgrades to current operating plant systems could introduce new effects from single failures as well as CCF effects that do not exist in systems that use separate discrete components. While a single random failure could affect multiple echelons in one division, a CCF could affect multiple echelons in multiple divisions. 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 B.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 with respect to a CCF. 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. The foundation of BTP 7-19 is the "NRC position on D3" from the SRM on SECY-93-087, Item 18, II.Q. The four points (i.e., SRM on SECY-93-087 items) are quoted below:

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

Point 2 "In performing the assessment, the vendor or applicant 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 shall demonstrate adequate diversity within the design for each of these events."

Point 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, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety 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 shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above."

The term "best-estimate methods" in Point 2 is more accurately referred to as "realistic assumptions," which are defined as normal plant conditions corresponding to the event. For example:

- power levels,
- temperatures,
- pressures,
- flows, and
- alignment of equipment.

Thus, in performing the assessment, the vendor or applicant should analyze each postulated CCF for each event that is evaluated in the SAR section analyzing power operation accidents at the plant conditions corresponding to the event. This analysis may use realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the Chapter 15, SAR analysis is based.

If the D3 analysis indicates a postulated CCF could disable a safety function, then Point 3 directs that an applicant should identify an existing diverse means or add a diverse means that may be nonsafety (see Section 1.6, "D3 Assessment"). Point 3 also addresses manual initiation methods of RTS and ESFAS, if subject to a postulated CCF.

The independence requirements of a diverse protection system from the safety protection system (i.e., physical, electrical, and communication separation) are defined in IEEE Std 603-1991. The diverse means could be safety-related and part of a safety division, and would then be subject to meeting divisional independence requirements. The diverse means could also be nonsafety-related in which case the IEEE Std 603-1991 requirement to separate safety-related equipment from that

which is not safety-related would still apply and would require independence of the two systems. In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system.

Point 4 directs the inclusion of a set of displays and manual controls (safety or nonsafety) in the main control room (MCR) that is diverse from any CCF vulnerability identified within the "safety computer system" discussed in Points 1 and 3 above and meets divisional independence requirements as applicable for the specific design implementation. These displays and controls are for manual, system level or divisional level (depending on the design) actuation and control of equipment to manage the "(plant) critical safety functions" (see Section B.1.2 above). Further, if not subject to the CCF, some of these displays and manual controls from Point 4 may actually be credited as all or part of the diverse means called for under Point 3.

The Point 4 phrase ". . . safety computer system identified in Items 1 and 3 above" refers to the safety-related automated RTS and ESFAS.

For digital system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy this point (see Section B.1.5, "Manual Initiation of Automatically Initiated Protective Actions Subject to CCF.") However, if existing displays and controls are digital and/or the same platform is used to provide signals to the analog displays, this point may not be satisfied.

Where the Point 4 displays and controls serve as the diverse means, 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 means. One example would be the use of hard-wired connections.

Once manual actuation from the MCR using the Point 4 displays and controls has been completed, controls outside the MCR for long-term management of these (plant) critical safety functions may be used when supported by suitable HFE analysis and site-specific procedures or instructions.

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,[1] 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 divisions 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 place further emphasis on the need for diversity to avoid or mitigate CCF.

[1] 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.

1.5 Manual Initiation of Automatically Initiated Protective Actions Subject to CCF

Two types of manual initiation of automatically initiated protective actions may be necessary. To satisfy IEEE Std 603-1991 Clauses 6.2 and 7.2, a safety-related means shall be provided in the control room to implement manual initiation of the automatically initiated protective actions at the division level. System level actuation of all divisions also may be used to meet the requirements of IEEE Std 603-1991.

If a D3 analysis indicates that the safety-related manual initiation would be subject to the same potential CCF affecting the automatically initiated protective action, then under Point 3 of the NRC position on D3, a diverse manual means of initiating protective action(s) would be needed (i.e., two manual initiation means would be needed). This diverse manual means may be safety or nonsafety. If the system/division level manual initiation required by IEEE Std 603-1991 is sufficiently diverse, the diverse (second) manual system level or division level actuation would not be necessary for the automated protective actions (see Figure 1).

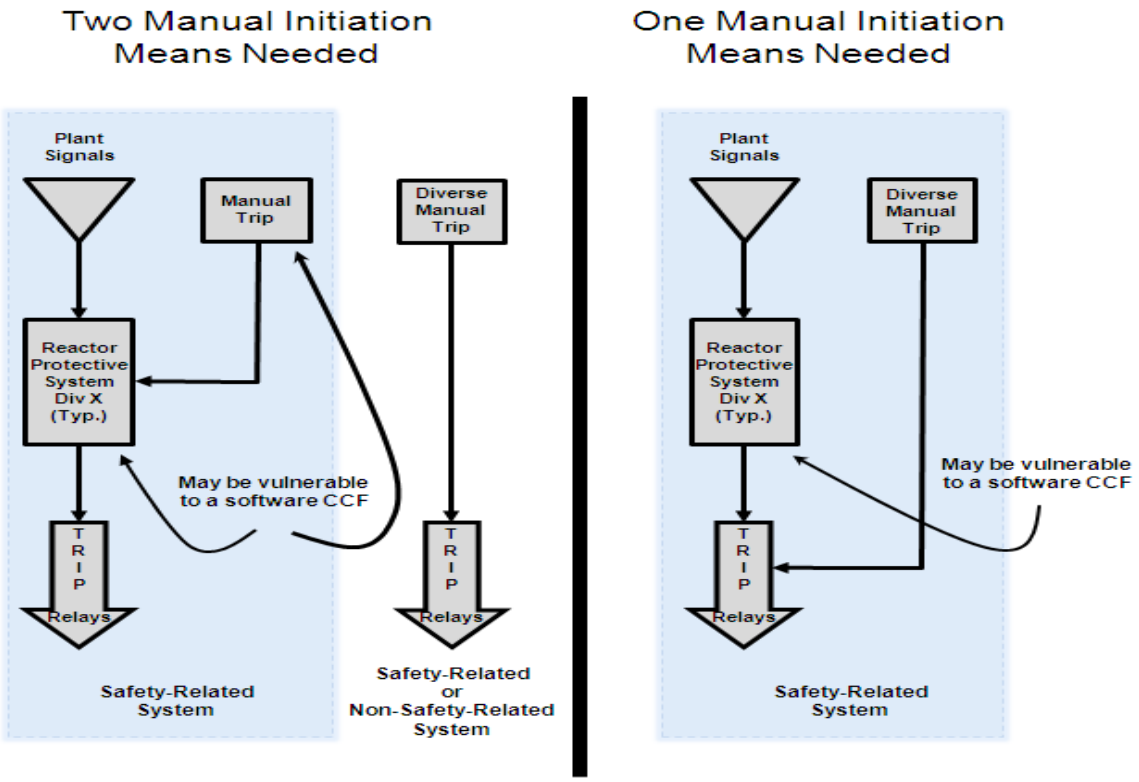

Figure 1. Two Manual Initiation Methods verses One Initiation Method

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 of the NRC position on D3, the applicant 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 may use realistic assumptions to analyze the plant response to DBEs (as identified in the SAR). If a postulated CCF could disable a safety function that is credited in the safety analysis to respond to the DBE being analyzed, a diverse means of effective response (with documented basis) is necessary. The D3 analysis methods used in ALWR DC applications 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. 10 CFR 50.62 requires that the ATWS mitigation system be composed of equipment that is diverse from the RTS. If “sufficient” diversity in manufacturer cannot be demonstrated, a case-by-case assessment of the mitigation

system designs should be conducted. This assessment should include differences such as manufacturing division (within a corporate entity), software (including implementation language), equipment (including control processing unit architecture), function, and people (design and verification/validation team).

1.7 The Diverse Means

When a diverse means is needed to be available to replace an automated system used to accomplish a credited safety function as a result of the D3 assessment identifying a potential CCF, the credited safety function (or a different function that will accomplish the same desired safety protection) can be accomplished via either an automated system or manual operator actions performed from the MCR. The preferred diverse means is generally an automated system.

The primary focus of BTP 7-19 is to identify whether a diverse means of performing protective actions is necessary due to an automated safety function being subject to a postulated CCF. Functions performed manually normally would be expected to still be performed manually in the presence of a CCF (even if different equipment is called upon to function). If the manual actuation method could be adversely affected by the postulated CCF, then a diverse manual means is needed to perform the safety function or an acceptable different function.

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 failure of a system to actuate might not be the worst case failure, particularly when analyzing the time required for identifying and responding to conditions resulting from a CCF in an automated safety system. For example, a failure to trip might not be as limiting as a partial actuation of an emergency core cooling system, 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 in accordance with Section 3 of NUREG/CR-6303. The primary concern is that an undetected failure within a digital safety 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 that is necessary. Consequently, non-detectable faults are of concern. Therefore, a diverse means to provide the credited safety function or some other safety function that will adequately address each DBE should be provided.

A CCF that causes an undesired trip or actuation can be detected (although not always anticipated) because this type of failure normally is self-announcing by the actuated system. However, there may be circumstances in which a spurious trip or actuation would not occur until a particular signal or set of signals are present. 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 (by the actuated system,) even if the annunciation did not occur on initial test or startup.

Failures of the automated protection system stemming from a software CCF can cause spurious actuations. The plant design basis addresses the effects of certain software CCF-caused spurious actuations.

The overall defense in depth strategy of a plant should prevent or mitigate the effects of credible spurious actuations caused by a software CCF that have the potential to place a plant in a configuration that is not bounded by the plant's design basis. The effects of some credible postulated spurious actuations caused by a software CCF in the automated protection system may not be evaluated in design basis accident analyses. In these cases, an analysis should be performed to determine whether these postulated spurious actuations could result in a plant response that results in conditions that do not fall within those established as bounding for plant design. Further, the analysis should identify whether adequate coping strategies, whether for prevention or mitigation, exist for these postulated spurious actuations (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures and the reactor operations team). If existing coping strategies are not effective for responding to the credible postulated spurious actuations that result in plant conditions falling outside those established as bounding for plant design, the licensee should develop additional coping strategies.

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, either of which is sufficient to eliminate consideration of software based or software logic based CCF:

<u>Diversity</u> or <u>Testability</u>

(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 that use a

diverse digital system. If 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, then, 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 and every possible sequence of device states are tested and all outputs are verified for every case (100 percent tested).

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. If the D3 assessment indicates the need for a diverse means to accomplish a protective safety function, then the diverse means should be evaluated, including any HFE analysis associated with manual operator actions as a diverse means.

3. Acceptance Criteria

3.1 Specific Acceptance Criteria

The D3 assessment submitted by the applicant should demonstrate compliance with the NRC position on D3 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 diverse means provided. Since the acceptance criteria address confirmation that AOOs and postulated accidents 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 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 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 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 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 for which the safety analysis credits reactor trip but the 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 assure that the plant response calculated using realistic assumptions and 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 CCF results in a plant response for which the safety analysis credits ESF actuation and also impairs the ESF function, then a diverse means 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 and 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 ESF. 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, a safety-related means shall be provided in the control room to implement manual initiation of the automatically initiated protective actions at the system level or division level (depending on the design) of the RTS and ESF functions. This safety-related manual means shall minimize the number of discrete operator manual manipulations and shall depend on operation of a minimum of equipment. If a D3 analysis indicates that the safety-related manual initiation would be subject to the same potential CCF affecting the automatically initiated protective action, then under Point 3 of the NRC position on D3, a diverse manual means of initiating protective action(s) would be needed, (i.e., two manual initiation means would be needed). If the safety-related system/division level manual initiation required by IEEE Std 603-1991 is sufficiently diverse, the diverse (second) manual means would not be necessary (see Section B.1.5, “Manual Initiation of Automatically Initiated Protective Actions Subject to CCF.”) 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 means, then the applicant should demonstrate that the criteria are satisfied and that sufficient diversity exists. Note that if the diverse means is nonsafety, then IEEE Std 603-1991, Clause 5.6, “Independence,” directs the

separation or independence of the safety systems and the diverse means (see Figure 1).

(7) If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the diverse means of actuating the protective safety functions can be achieved via either an automated system (see Section 3.4, "Use of Automation in Diverse Means" below,) or manual operator actions that meet HFE acceptability criteria (see Section 3.5, "Use of Manual Action as a Diverse Means of Accomplishing Safety Functions" below).

(8) If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the diverse means of actuating the protective safety functions should meet the following criteria: The diverse means should be:

a) at the system or division level (depending on the design);

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 indicators that may be malfunctioning due to the CCF 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. whether the automated diverse means 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 diverse means used to cope with a CCF, the design of a diverse automated or diverse manual actuation system should address how to minimize the potential for a spurious actuation of the protective system caused by the diverse means. Use of design techniques (for example, redundancy, conservative setpoint selection, coincidence logic, 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 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 controller or central processing unit (CPU) 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), a postulated CCF need not be assumed to be a single failure in design basis evaluations. Consequently, realistic assumptions can be employed in performing analyses to evaluate the effect of CCF coincident with DBEs.

3.4 Use of Automation in Diverse Means

If automation is used in the diverse means, then the functions should be provided by equipment that is not affected by the postulated CCF and should be sufficient to maintain plant conditions within recommended acceptance criteria for the particular AOO or postulated accident. The automated diverse means may be performed by a nonsafety system, if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The automated diverse means 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 as a Diverse Means of Accomplishing Safety Functions

If manual operator actions are used as the diverse means or as part of the diverse means to accomplish a safety function, a suitable HFE analysis should be performed by the applicant to demonstrate that plant conditions can be maintained within recommended acceptance criteria for the particular AOO or postulated accident. 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 is a measure of the safety margin and as it decreases, uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed.

Diverse manual initiation of safety functions should be performed on a system level or division level basis (depending on the design). Since single failures concurrent with a CCF are not

required to be postulated and normal alignment of equipment is assumed, the capability for manual actuation of a single division is sufficient. For plants licensed to allow one division to be continuously out of service, the diverse manual actuation should apply to at least one division that is in service (see section B.3.1, Item 9, concerning addressing spurious actuation caused by the diverse means in the design of the diverse means). A CCF that affects normal displays or controls should not prevent the operator from manually initiating safety functions. Prioritization between safety and diverse nonsafety systems to ensure the credited safety function can be accomplished by either system is addressed as follows:

> Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a CCF in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state,") and which do not directly support any safety function, have lower priority and may be overridden by other commands. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.

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.

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 the RTS or ESF.

3.7 Effects of Spurious Actuation Caused by CCF

In cases in which a credible postulated spurious actuation(s) caused by a software CCF is not evaluated in design basis accident analyses, an analysis should be performed to determine whether such a postulated spurious actuation results in a plant response that falls outside the values or ranges of values chosen for controlling parameters as reference bounds for design. Further, the analysis should identify whether coping strategies exist for these postulated spurious actuations and consider the adequacy of such strategies. An applicant or licensee should confirm that a coping strategy has been identified to address the effects from credible spurious actuations caused by a CCF that have the potential to place the plant in a configuration that is not bounded by the plant design basis accident analyses.

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 assessment 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 development tools. 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 percent testing means that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case. Further, in assessing the system states, the guidance provided in IEEE Std 7-4.3.2, 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 relies upon 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 relying upon a software development system."

Clause 5.4.1 of IEEE Std 7-4.3.2 directs the system developer or 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. 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 equipment that can be adversely affected by a CCF. 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 not adversely affected by a CCF of the safety functions credited in the accident analysis. 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'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.

4.3 Exclusion of Components from D3 Analysis

A software-based component may be sufficiently simple and deterministic in performance such that the component is not a source of a CCF. Such components need not be considered in a D3 analysis. When a basis is given that a component is not susceptible to CCF, the NRC staff should examine the justification carefully.

4.4 Effect of Other Blocks

When considering the effects of a postulated CCF, diverse blocks are assumed to function correctly. This includes the 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 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 should be 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 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 is a measure of the safety margin and as it decreases, uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed.

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. Institute of Electrical & Electronics Engineers, IEEE 100, “The Authoritative Dictionary of Standards Terms,” Piscataway, NJ.

2. Institute of Electrical & Electronics Engineers, IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

3. Institute of Electrical & Electronics Engineers, IEEE Std 379, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” Piscataway, NJ.

4. Institute of Electrical & Electronics Engineers, IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Piscataway, NJ.

5. Institute of Electrical & Electronics Engineers, IEEE Std. 7-4.3.2, “IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations,” Piscataway, NJ.

6. U.S. Nuclear Regulatory Commission, “Task Working Group No. 2: Diversity and Defense-in-Depth Issues Interim Staff Guidance,” DI&C-ISG-02, Revision 2, June 5, 2009.

7. U.S. Nuclear Regulatory Commission, “Quality Assurance Guidance for ATWS Equipment that is not Safety-Related,” Generic Letter 85-06, April 16, 1985.

8. U.S. Nuclear Regulatory Commission, “Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses,” NUREG-0800, SRP Chapter 18, Appendix 18-A.

9. U.S. Nuclear Regulatory Commission, “A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System,” NUREG-0493, March 1979.

10. U.S. Nuclear Regulatory Commission, “Clarification of TMI Action Plan Requirements (GL No. 82-33),” December 17, 1982.

11. U.S. Nuclear Regulatory Commission, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” NUREG/CR-6303, December 1994.

12. U.S. Nuclear Regulatory Commission, “Diverse Instrumentation and Control Systems,” NUREG-0800, SRP Section 7.8.

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

14. U.S. Nuclear Regulatory Commission, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Regulatory Guide 1.152.

15. U.S. Nuclear Regulatory Commission, “Manual Initiation of Protective Actions,” Regulatory Guide 1.62.

16. U.S. Nuclear Regulatory Commission, “Digital Computer Systems for Advanced Light-Water Reactors,” SECY-91-292, September 16, 1991.

17. U.S. Nuclear Regulatory Commission, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” SECY-93-087, April 2, 1993.

18. U.S. Nuclear Regulatory Commission, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” SRM on SECY-93-087, July 21, 1993.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in the Standard Review Plan are covered by the requirements of 10 CFR 50, 10 CFR 52 and 10 CFR 100, and were approved by the Office of Management and Budget, approval number 3150-0011, 3150-0151, and 3150-0093.

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.

BTP Section 7-19

Description of Changes

BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"

This BTP section updates the guidance previously provided in Revision 6, dated July 2012. See ADAMS Accession No. ML110550791.

The main purpose of this update is to incorporate the revised software RGs and the associated endorsed standards. For organizational purposes, the revision number of each RG and year of each endorsed standard is now listed in one place, Table 7-1. As a result, revisions of RGs and years of endorsed standards were removed from this section, if applicable. For standards that are incorporated by reference into regulation (IEEE Std 279-1971 and IEEE Std 603-1991) and standards that have not been endorsed by the agency, the associated revision number or year is still listed in the discussion. Additional changes were editorial.

Part of 10 CFR was reorganized due to a rulemaking in the fall of 2014. Quality requirement discussions in the former 10 CFR 50.55a(a)(1) were moved to 10 CFR 50.54(jj) and 10 CFR 50.55(i). The incorporation by reference language in the former 10 CFR 50.55a(h)(1) was moved to 10 CFR 50.55a(a)(2). There were no changes either to 10 CFR 50.55a(h)(2) or 10 CFR 50.55a(h)(3).