U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

7.8 DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

I. AREAS OF REVIEW

This Standard Review Plan (SRP) section describes the review process and acceptance criteria for the diverse instrumentation and control (I&C) systems and equipment provided for the express purpose of protecting against potential common-cause failures of protection systems. The objectives of this review are to assure that the anticipated transient without scram (ATWS) mitigation systems and equipment are designed and installed in accordance with the requirements of 10 CFR 50.62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants,” and that other diverse I&C systems within the scope of this section comply with the NRC position on diversity and defense-in-depth (D3).

1. The following systems are covered by this section:

   - ATWS mitigation systems that are required for compliance with 10 CFR 50.62. As defined in 10 CFR 50.62, an ATWS event is an anticipated operational occurrence followed by failure of the reactor trip portion of the protection system. 10 CFR 50.62 identifies design requirements for ATWS mitigation systems and equipment.

- Diverse manual controls and displays that are provided to comply with the NRC position on D3 as described in the Staff Requirements Memorandum (SRM) regarding SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.” These systems are to be independent and diverse from the associated digital safety systems(s). The associated operator interfaces (controls and displays) must be located in the main control room. They are to provide manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.

- Diverse actuation systems (DAS) that are provided solely for the purpose of meeting the NRC position on D3. DAS and ATWS mitigation system functions may be combined into a single system.

The reactor trip system (RTS), engineered safety features actuation system (ESFAS), control system, or other I&C systems may perform diverse functions credited in meeting the NRC D3 position. The functions of these systems are outside the scope of this section. These functions should meet the criteria applicable to the systems as a whole and should be consistent with the assumption of the applicant/licensee’s D3 analysis. The requirements for these systems and the staff’s review are found in the SRP sections for the individual systems.

2. Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC). For design certification (DC) and combined license (COL) reviews, the staff reviews the applicant's proposed ITAAC associated with the structures, systems, and components (SSCs) related to this SRP section in accordance with SRP Section 14.3, "Inspections, Tests, Analyses, and Acceptance Criteria." The staff recognizes that the review of ITAAC cannot be completed until after the rest of this portion of the application has been reviewed against acceptance criteria contained in this SRP section. Furthermore, the staff reviews the ITAAC to ensure that all SSCs in this area of review are identified and addressed as appropriate in accordance with SRP Section 14.3.

3. COL Action Items and Certification Requirements and Restrictions. For a DC application, the review will also address COL action items and requirements and restrictions (e.g., interface requirements and site parameters).

   For a COL application referencing a DC, a COL applicant must address COL action items (referred to as COL license information in certain DCs) included in the referenced DC. Additionally, a COL applicant must address requirements and restrictions (e.g., interface requirements and site parameters) included in the referenced DC.

Review Interfaces

Other SRP sections interface with this section as follows:

1. SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the staff may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between the organization responsible for the review of I&C and organizations responsible for other review topics.

2. In addition to the coordination described in SRP Section 7.0, the organization responsible for the review of reactor systems evaluates the following aspects of the diverse I&C systems:

   - Consistency of the ATWS mitigation protective functions with the requirements of 10 CFR 50.62 and the ATWS analysis referenced in the safety analysis report (SAR), Chapter 15, for anticipated operational occurrences and to verify the adequacy of the design of mechanical systems used to mitigate ATWS.

   - The adequacy of the set of manual control and display functions is reviewed to confirm it is sufficient to monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition and to control the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

   - For plants with a digital RTS or ESFAS, DAS functions and other D3-related functions are reviewed to confirm that they are consistent with the portions of the accident analysis that support the D3 analysis.

The specific acceptance criteria and review procedures are contained in the reference SRP sections.

II. ACCEPTANCE CRITERIA

Requirements

Acceptance criteria are based on meeting the relevant requirements of the following Commission regulations:

1. 10 CFR 50.55a(a)(1), “Quality Standards.”

2. 10 CFR 50.55a(h), “Protection and Safety Systems,” requires compliance with IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995. For nuclear power plants with construction permits issued before January 1, 1971, the applicant/licensee may elect to comply instead with the plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations.”

   For diverse actuation systems isolated from safety systems, the applicable requirements of 10 CFR 50.55a(h) are IEEE Std 279-1971, Clause 4.7, “Control and Protection System Interaction”; IEEE Std 603-1991, Clause 5.6.3, “Independence Between Safety Systems and Other Systems”; and IEEE Std 603-1991, Clause 6.3, “Interaction Between the Sense and Command Features and Other Systems.”

3. 10 CFR 50, Appendix A, General Design Criterion (GDC) 1, “Quality Standards and Records.”

4. GDC 13, “Instrumentation and Control.”

5. GDC 19, “Control Room.”

6. GDC 24, “Separation of Protection and Control Systems.”

Note that the design of the diverse I&C systems must be such that the protection system continues to meet the requirements of 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” Section III, “Protection and Reactivity Control Systems.” Review of the reactor protection system for these areas of conformance is addressed in SRP Sections 7.2 and 7.3.

Additional requirements applicable to any information system important to safety proposed for standard DC or COLs under 10 CFR 52

7. 10 CFR 52.47(b)(1), which requires that a DC application contain the proposed inspections, tests, analyses, and acceptance criteria (ITAAC) that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the Atomic Energy Act, and the NRC's regulations;

8. 10 CFR 52.80(a), which requires that a COL application contain the proposed inspections, tests, and analyses, including those applicable to emergency planning, that the licensee shall perform, and the acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, the facility has been constructed and will operate in conformity with the combined license, the provisions of the Atomic Energy Act, and the NRC's regulations.

Additional acceptance criteria applicable to ATWS mitigation functions:

9. 10 CFR 50.62, “Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants.”

SRP Acceptance Criteria

Specific SRP acceptance criteria acceptable to meet the relevant requirements of the NRC’s regulations identified above are contained in SRP Section 7.1, SRP Table 7-1, and SRP Appendix 7.1-A, which list standards, regulatory guides, and branch technical positions (BTPs). 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 acceptable methods of compliance with the NRC regulations.

1. For plants with a digital RTS or ESFAS, the NRC position on D3 should be especially noted. This position is contained in Item II.Q, “Defense Against Common-Mode Failures in Digital Instrument and Control Systems,” of the Staff Requirements Memorandum on

SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to diverse I&C functions are as follows:

> "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 [as the safety system], shall be required to perform either the same function [as the safety system function that is vulnerable to common mode failure] or a different function [that provides adequate protection]. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions."
>
> "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[s] …"

2. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h).

3. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h).

4. SRP Appendix 7.1-D provides SRP acceptance criteria for digital I&C compliance with IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision 2.

III. REVIEW PROCEDURES

The reviewer will select material from the procedures described below, as may be appropriate for a particular case. Typical reasons for a non-uniform emphasis are the introduction of new design features or the use in the design of features previously reviewed and found acceptable.

These review procedures are based on the identified SRP acceptance criteria. For deviations from these acceptance criteria, the staff should review the applicant's evaluation of how the proposed alternatives provide an acceptable method of complying with the relevant NRC requirements identified in Subsection II.

SRP Section 7.1 describes the general procedures to be followed in reviewing any I&C system. This part of SRP Section 7.8 highlights specific topics that should be emphasized in the diverse I&C systems review.

The diverse I&C systems review should address the applicable topics identified in SRP Table 7-1. SRP Appendix 7.1-A describes review methods for each topic. Major design considerations that should be emphasized in the review of the diverse I&C systems are identified below.

- Design basis - Design bases should be described in the SAR for each diverse I&C system. The design bases should, as a minimum, address the following topics:

  - The specific design requirements identified in 10 CFR 50.62, as applicable, and any other applicable design requirements.

  - Identification of conditions that require protective action by the diverse I&C systems. For DAS, these events are identified in the applicant/licensee's D3 analysis. For ATWS mitigation systems, these events are limited to anticipated operational occurrences, defined in 10 CFR 50, Appendix A, Definitions and Explanations, as conditions of normal operation that are expected to occur one or more times during the life of the nuclear power unit, and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator, isolation of the main condenser, and loss of all offsite power.

  - Identification by the applicant/licensee of the bounding events and the bases in the analyses that are presented or referenced in SAR Chapter 15. The reviewer should confirm with the organization responsible for the review of reactor systems that the analytical basis for each diverse I&C system is acceptable and consistent with the Chapter 15 analysis, and should confirm with the organizations responsible for the review of reactor systems and plant systems that the design of the mechanical systems used for ATWS mitigation is acceptable.

  - Identification of the range of transient and steady-state conditions for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform.

  - Identification of performance requirements. The performance requirements for which credit is taken in the mitigation of design basis events (e.g., dynamic response, accuracy) should be identified. The review should confirm that the applicant/licensee verifies conformance to these requirements by validation testing and surveillance.

- Quality of components and modules - Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," provides acceptable guidance for the quality assurance of diverse I&C systems and components.

- System testing and surveillance - The applicant/licensee should identify the test, maintenance, surveillance, and calibration procedures. These provisions should be consistent with the guidance of Generic Letter 85-06. The ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device).

- Use of digital systems - See Appendix 7.0-A, Appendix 7.1-D, and BTPs 7-14, 7-17, 7-18, 7-19, and 7-21.

- Power supply availability - The reviewer should confirm with the organization responsible for the review of power systems that power sources will be available during and following a loss of offsite power.

- Environmental qualification - The diverse I&C system equipment as installed should be qualified for the environment that could exist during the events for which the equipment is assumed to respond.

- System status - Information should be available in the control room to indicate the operation of the diverse I&C systems. This aspect of the review may involve considerations included in emergency operating procedures.

- Independence from the protection systems - Diverse actuation systems functions should be independent and diverse from the RTS and ESFAS. ATWS mitigation systems should be diverse from the RTS. For ATWS mitigation systems, 10 CFR 50.62 requires diversity from the sensor output to the final actuation device. See SRP Appendix 7.1-C, subsections 5.6 and 6.3 and SRP Appendix 7.1-B, subsection 4.6.

- Potential for inadvertent actuation - The diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems.

- Manual initiation capability - The ATWS mitigation systems and DAS should include the capability for initiation from the control room.

- Completion of protective action - The ATWS mitigation logic and DAS should be designed such that, once initiated, the mitigation function will go to completion.

- D3 analysis - The I&C functions credited with providing diversity should be consistent with the assumptions of the applicant/licensee's D3 analysis. For example, diverse I&C system equipment should be environmentally qualified for the environments in which the D3 analysis assumes they will operate. When a D3 analysis is not provided, the following diversity criteria should be met:

    - Equipment diversity should be provided to the extent reasonable and practicable to minimize the potential for common-cause failures.

    - Equipment diversity is required from the sensors/transmitters to and including the components used to interrupt control rod power or vent the scram air header.

    - For interruption of control rod power, obtaining circuit breakers from different manufacturers is not, in and of itself, sufficient to provide the required diversity.

    - For mitigating systems other than diverse RTSs (e.g., auxiliary feedwater), diversity is required from the sensors to, but not including, the final actuation device.

    - Sensors need not be of a diverse design or manufacturer.

- Existing RTS sensing lines may be used for ATWS mitigation instruments.

- Sensors/transmitters and sensing lines should be selected such that adverse interactions with existing control systems are avoided.

- Logic and actuation device power for the ATWS mitigation system should be from an instrument power supply independent from the power supplies for the existing RTS. Existing RTS sensor and instrument channel power supplies may be used, provided the possibility of common-cause failure is prevented.

If the ATWS system is explicitly addressed as part of a D3 analysis, the analysis provides the basis for assessing the adequacy of diversity between the ATWS mitigation system and the RTS. Therefore, separate evaluation of the ATWS mitigation system against the above eight diversity criteria is unnecessary if the D3 analysis is provided.

Additional major design considerations that should be emphasized in the review of manual controls and displays are:

- For review of a DC application, the reviewer should follow the above procedures to verify that the design, including requirements and restrictions (e.g., interface requirements and site parameters), set forth in the final safety analysis report (FSAR) meets the acceptance criteria. DCs have referred to the FSAR as the design control document (DCD). The reviewer should also consider the appropriateness of identified COL action items. The reviewer may identify additional COL action items; however, to ensure these COL action items are addressed during a COL application, they should be added to the DC FSAR.

- For review of a COL application, the scope of the review is dependent on whether the COL applicant references a DC, an ESP or other NRC approvals (e.g., manufacturing license, site suitability report or topical report).

- For review of both DC and COL applications, SRP Section 14.3 should be followed for the review of ITAAC. The review of ITAAC cannot be completed until after the completion of this section.

IV. EVALUATION FINDINGS

The reviewer verifies that the applicant has provided sufficient information and that the review and calculations (if applicable) support conclusions of the following type to be included in the staff's safety evaluation report. The reviewer also states the bases for those conclusions.

1. Evaluation findings applicable to any diverse I&C system:

   The staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The staff concludes that the applicant/licensee adequately classified and identified the guidelines applicable to these systems. Based on the review of the system design for

conformance to the guidelines, the staff finds there is reasonable assurance the systems fully conform to the guidelines applicable to these systems. Therefore, the staff finds that the applicable requirements of GDC 1 and 10 CFR 50.55a(a)1 have been met.

The diverse I&C systems are appropriately isolated from safety systems. Therefore, the staff concludes that the independence of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and GDC 24.

Based on the applicant/licensee's commitment to the quality assurance guidance of Generic Letter 85-06 and review of the design of the diverse I&C systems, the staff finds that the quality assurance requirements of GDC 1 have been met.

Based on the review of diverse I&C system status information, manual initiation capabilities, and provisions to support safe shutdown, the staff concludes that information is provided to monitor the system over the anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of diverse I&C functions. These manual controls are to be independent of the digital systems that provide automatic initiation of the same functions. The diverse I&C systems appropriately support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Therefore, the staff finds that the design of the diverse I&C systems satisfies the requirements of GDC 13 and 19.

Based on the licensee's commitment to periodically test the diverse I&C systems from end-to-end [summarize the specific commitment], the staff concludes that an acceptable level of availability for the system can be maintained.

2. Note: The following finding applies to diverse I&C systems involving digital computer-based components.

   Based on the review of software development plans and the review of the computer software development process and design outputs, the staff concludes that the computer systems meet the guidance of Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Therefore, the special characteristics of computer systems have been adequately addressed, and the staff finds that the diverse I&C systems satisfy the requirements of GDC 1.

3. Additional evaluation findings applicable to ATWS mitigation systems:

   The ATWS mitigation system instrumentation includes [summarize the basic functions and elements of the I&C system design submitted for review]. Based on the review of these functions and the design bases submitted by the applicant, the staff concludes that the ATWS mitigation design includes an appropriate set of functions.

   Based on review of the interfaces of the ATWS mitigation system and equipment with the RTS, the staff concludes that the separation and independence design features of the RTS are not compromised by the ATWS mitigation system design. Where isolation devices are provided in the RTS to support ATWS mitigation interfaces, the isolation devices are applied and qualified to the guidelines of SRP BTP 7-11.

Based on the above items, the staff concludes that the design of the ATWS mitigation system is acceptable and satisfies the specific design requirements identified in 10 CFR 50.62 for [identify reactor type].

4. Additional evaluation findings applicable to diverse I&C system manual controls and displays:

   Based on a review of diverse manual displays and controls, the staff concludes that these controls and displays are independent and diverse from the safety computer system, and sufficient for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. Therefore, the staff concludes that the manual controls and displays fulfill the guidance of the Staff Requirements Memorandum on SECY 93-087, item II.Q.

5. Additional evaluation findings applicable to DAS:

   Based on review of DAS functions and design, the staff concludes that the DAS is acceptable. The functional requirements, independence requirements, and diversity requirements for this system are consistent with the applicant's diversity and defense-in-depth analysis, and fulfill the applicable guidance of the SRM on SECY-93-087, Item II.Q.

6. For DC and COL reviews, the findings will also summarize the staff's evaluation of requirements and restrictions (e.g., interface requirements and site parameters) and COL action items relevant to this SRP section.

7. In addition, to the extent that the review is not discussed in other SER sections, the findings will summarize the staff's evaluation of the ITAAC, including design acceptance criteria, as applicable.

8. The conclusions noted above for the diverse I&C systems are applicable to all portions of the systems except for the following, for which acceptance is based on prior NRC review and approval as noted [list applicable system or topics and identify references].

V. IMPLEMENTATION

The staff will use this SRP section in performing safety evaluations of DC applications and license applications submitted by applicants pursuant to 10 CFR Part 50 or 10 CFR Part 52. Except when the applicant proposes an acceptable alternative method for complying with specified portions of the Commission's regulations, the staff will use the method described herein to evaluate conformance with Commission regulations.

The provisions of this SRP section apply to reviews of applications docketed six months or more after the date of issuance of this SRP section, unless superseded by a later revision.

VI. REFERENCES

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

2. IEEE Std 603-1991. “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

3. IEEE Std 7-4.3.2-2003. “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

4. Regulatory Guide 1.152. “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2006.

5. Generic Letter 85-06. “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related,” April 16, 1986.

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

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