U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

7.4 SAFE SHUTDOWN SYSTEMS

REVIEW RESPONSIBILITIES

Primary - Organization responsible for the review of instrumentation and controls

Secondary - None

I. AREAS OF REVIEW

The objectives of the review are to confirm that the safe shutdown systems satisfy the requirements of the acceptance criteria and guidelines applicable to safety systems and that they will perform their safety functions during all plant conditions for which they are required.

This Standard Review Plan (SRP) section describes the review process and acceptance criteria for those instrumentation and control (I&C) systems used to achieve and maintain a safe shutdown condition of the plant as required by 10 CFR 50 Appendix A, General Design Criteria (GDC) 13, “Instrumentation and Control,” and GDC 19, “Control Room.” To the extent that the engineered safety feature (ESF) systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features that are unique to safe shutdown and not directly related to accident mitigation. The features within the scope of SRP Section 7.4 may involve individual component control for safe shutdown versus system-level actuation for accident mitigation, or system-level controls used to achieve and maintain safe shutdown but not used for accident mitigation. System-level controls used for accident

mitigation may also need to be reviewed using SRP Section 7.4 if the safe shutdown functions of these controls involve features or operating modes that are unique to their safe shutdown functions. This SRP section also addresses the review of those systems required for safe shutdown that are not classified as ESF systems. The specific arrangement of these systems depends on (1) the type of plant (PWR or BWR), (2) individual plant design features, and (3) the conditions under which the safe shutdown has to be achieved and maintained. The functional performance requirements of safe shutdown systems and auxiliary supporting features and other auxiliary features are reviewed by other branches in accordance with the SRP sections that address these systems.

During safe shutdown, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core. For definitions of plant-specific shutdown conditions, see Chapter 16 in the applicant/licensee's safety analysis report (SAR). Section 7.5 of the SRP addresses the information systems important to safety that provide information to the operator for the manual control of systems required for safe shutdown. Section 9.5.1 of the SRP includes the I&C provided as part of an alternative or dedicated shutdown capability needed for compliance with GDC 3, "Fire Protection."

Typical functions required for safe shutdown are:

- Reactivity control
- Reactor coolant makeup
- Reactor pressure control
- Decay heat removal
- Suppression Pool Cooling (BWR)

Typical auxiliary supporting features and other auxiliary features (additional information is provided in SRP Appendix 7.1-C) are:

- Electric power systems
- Component cooling water
- Service water
- Instrument air 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. Voice communication between safe shutdown control areas is reviewed by the organization responsible for review of I&C as part of its primary review responsibility for SRP Section 9.5.2.

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 Systems 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 their plant-specific licensing basis. For nuclear power plants with construction permits issued between January 1, 1971, and May 13, 1999, the applicant/licensee may elect to comply instead with the requirements stated in IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations.” For safe shutdown systems that are not safety systems as

defined by IEEE Std 603-1991 and that are 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 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves," or equivalent TMI action plan requirements imposed by Generic Letters.

4. 10 CFR 50, Appendix A, GDC 1, "Quality Standards and Records."

5. GDC 2, "Design Bases for Protection against Natural Phenomena."

6. GDC 4, "Environmental and Missile Design Bases."

7. GDC 13, "Instrumentation and Control."

8. GDC 19, "Control Room."

9. GDC 24, "Separation of Protection and Control Systems."

10. GDC 34, "Residual Heat Removal."

11. GDC 35, "Emergency Core Cooling."

12. GDC 38, "Containment Heat Removal."

13. 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;

14. 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.

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's regulations.

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

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

3. SRP Appendix 7.1-D provides SRP acceptance criteria for the 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, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."

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 utilization 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 specific acceptance criteria, the staff should review the applicant's evaluation of how the proposed alternatives to the SRP criteria 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 instrumentation and control system. This part of SRP Section 7.4 highlights specific topics that should be emphasized in the review of safe shutdown systems.

1. The review should include an evaluation of the safe shutdown systems design against the guidance of IEEE Std 603-1991, or IEEE Std 279-1991, depending on the applicant/licensee's commitment regarding these design criteria. For computer-based safe shutdown systems, the guidance is provided by IEEE Std 7-4.3.2-2003 as endorsed by Regulatory Guide 1.152, Revision 2. These procedures are detailed in SRP Appendix 7.1-B for IEEE Std 279-1971, SRP Appendix 7.1-C for IEEE Std 603-1991, and SRP Appendix 7.1-D for IEEE Std 7-4.3.2-2003.

   SRP Appendices 7.1-B and 7.1-C discuss the requirements of IEEE Std 279-1971 and IEEE Std 603-1991, respectively, and how they are used in the review of safe shutdown systems. SRP Appendix 7.1-D discusses the criteria of IEEE Std 7-4.3.2-2003 and how they are used in the review of safe shutdown systems. Although the primary emphasis is on the equipment comprising the safe shutdown systems, the reviewer should consider the safe shutdown functions at the system level. The safe shutdown systems design should be compatible with the SAR Chapter 15 design bases accident analyses. It is not sufficient to evaluate the adequacy of the safe shutdown systems only on the basis that the design meets the specific requirements of IEEE Std 279-1971 or IEEE Std 603-1991.

Major portions of the systems required for safe shutdown are also used as ESF systems, as discussed in SRP Section 7.3. Therefore, the review under this SRP section includes those aspects of ESF systems that are unique to safe shutdown in addition to those systems required for safe shutdown, that are not classified as ESF systems.

The safe shutdown systems review should address the topics identified as applicable by 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 I&C for the safe shutdown systems are identified below.

A. Independence - See SRP Appendix 7.1-B subsections 4.6 and 4.7 and SRP Appendix 7.1-C subsections 5.6 and 6.3.

B. Use of digital systems - See SRP Appendix 7.0-A and SRP Appendix 7.1-D.

C. Periodic testing - See SRP Appendix 7.1-B subsection 4.10 and SRP Appendix 7.1-C subsections 5.7 and 6.5.

D. Remote shutdown capability[1] - Plant designs should provide for control in locations removed from the main control room that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. This control equipment should be capable of operating independently of (i.e., without interaction with) the equipment in the main control room. This equipment may include the remote shutdown station and other local controls.

   The design of remote shutdown stations should provide appropriate displays so that the operator can monitor the status of the shutdown. Typical parameters for PWR displays are pressurizer pressure, pressurizer level, reactor coolant temperature, steam generator pressure, steam generator level, source-range neutron flux, level indication for tanks involved in shutdown, and shutdown system diagnostic instrumentation. Typical parameters for BWR displays are reactor vessel water level and pressure, suppression pool level and temperature, emergency or isolation condenser level indication for tanks involved in shutdown, and shutdown system diagnostic instrumentation.

[1]Shutdown remote from the control room is not an event analyzed in the accident analysis in Chapter 15 of the SAR. Specific scenarios have not been specified on which the adequacy of shutdown capability remote from the control room is evaluated. However, smoke due to a fire in the control room has long been recognized as the type of event that could force the evacuation of the control room and result in a need to shut down remote from the control room. Regulatory Guide 1.189, “Fire Protection for Operating Nuclear Power Plants,” establishes the bases for safe shutdown with respect to fire protection. Specifically, fire damage limits as they impact safe shutdown have been established therein. These limits do not require consideration of an additional, random, single failure in the evaluation of the capability to safely shut down as a consequence of fire. The evaluation of conformance to Regulatory Guide 1.189 is addressed in SRP Section 9.5.1. Therefore, the application of the single-failure criterion to remote shutdown is applicable only to other events that could cause the control room to become uninhabitable. These events would not result in consequential damage or unavailability of systems required for safe shutdown.

The remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions that could occur as a result of plant cooldown. For example, in the cooldown of a PWR, reactor cooling system pressure will eventually drop below the safety-injection initiation setpoint. Because the control room is not available, it may be impossible to block this trip. Therefore, the remote shutdown capability must be able to accommodate this condition.

Access to remote shutdown stations should be under strict administrative controls.

The equipment in the remote shutdown stations should be designed to the same standards as the corresponding equipment in the main control room.

Remote shutdown station-control transfer devices should be located remote from the main control room and their use should initiate an alarm in the control room.

The location should be consistent with the procedures for remote, alternative, and dedicated shutdown, as appropriate.

Where the control functions are transferred between the control room and the remote shutdown station, the design should maintain parameter indications such that the operators at the control room and the remote shutdown station both have access to the same parameters that are being relied upon.

E. Safe shutdown - System conformance to the single-failure criterion on a system basis and operability from onsite and offsite electrical power as required by GDC 34, 35, and 38.

Safe shutdown systems that are safety systems according to the definition of IEEE Std 603-1991 should fulfil the requirements of that standard. The following topics are recommended for review emphasis with respect to IEEE Std 603-1991:

- Meet the single-failure criterion - See SRP Appendix 7.1-C subsection 5.1,

- Provide the required capacity and reliability to perform intended safety functions on demand - See SRP Appendix 7.1-C subsection 5,

- Provide the required capacity to function during and after design-basis events such as earthquakes and anticipated operational occurrences - See SRP Appendix 7.1-C subsections 5.4 and 5.5,

- Operate with onsite electric power available (assuming offsite power is not available) and with offsite electric power available (assuming onsite power is not available), and

- Provide the capability to be tested during reactor operation - See SRP Appendix 7.1-C subsections 5.7 and 6.5.

2. 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 early site permit (ESP) or other NRC approvals (e.g., manufacturing license, site suitability report or topical report).

3. 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. The NRC staff concludes that the design of the safe shutdown systems and the safe shutdown initiation of the auxiliary supporting features and other auxiliary features systems are acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19, 34, 35, and 38 and 10 CFR 50.55a(a)(1).

   The staff conducted a review of these systems for conformance to the guidelines in the regulatory guides and standards applicable to these systems. The staff concludes that the applicant/licensee adequately identified the guidelines applicable to these systems. Based on the review of the system design for conformance to the guidelines, the staff finds that there is reasonable assurance that the systems fully conform to the guidelines applicable to these systems. Therefore, the staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

   The non-safety portions of safe shutdown systems important to safety are appropriately isolated from safety systems, including the safety portions of the safe shutdown systems. Therefore, the staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and the requirements of GDC 24.

   The review included the identification of those systems and components for the safe shutdown systems that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based on the review, the staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

Based on the review, the staff concludes that the I&C have been provided to maintain variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems within prescribed operating ranges during plant shutdown. Therefore, the staff finds that the systems required for safe shutdown satisfy the requirements of GDC 13.

I&C have been provided within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including a shutdown following an accident. Equipment at appropriate locations outside the control room has been provided (1) with a design capability for prompt, hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. Therefore, the staff concludes that the systems required for safe shutdown satisfy the requirements of GDC 19.

The review of the I&C systems required for safe shutdown includes conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures as appropriate based on their safety function consistent with the GDC applicable to safe shutdown systems. The staff concludes that these systems are testable and are operable on either onsite or offsite electrical power and that the controls associated with redundant safe shutdown systems are independent and satisfy the requirements of the single-failure criterion and, therefore, meet the relevant requirements of GDC 34, 35, and 38.

In the review of the safe shutdown systems, the staff examined the power supply for the pressurizer level indication. Based on this review, the staff concludes that the safe shutdown systems satisfy the requirements of 10 CFR 50.34(f)(xx).

In the review of the safe shutdown systems, the staff examined the dependence of these systems on the available auxiliary supporting features and other auxiliary features. Based on this review and coordination with those having primary review responsibility of auxiliary supporting features and other auxiliary features systems, the staff concludes that the design of the safe shutdown systems is compatible with the functional requirements of auxiliary supporting features and other auxiliary features systems.

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.

2. Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the staff concludes that the computer systems meet the guidance of Regulatory Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the staff finds that the computer-based safe shutdown systems satisfy the requirements of GDC 1.

3. 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.

4. Note: the following conclusion is applicable to all applications.

   The conclusions noted above for the safe shutdown 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].

5. 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.

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 submitted 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. Regulatory Guide 1.189, "Fire Protection for Operating Nuclear Power Plants," Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2006.
