NUREG-0800
(Formerly NUREG-75/087)

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.4. Safe Shutdown Systems

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for those instrumentation and control 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 which are unique to safe shutdown and not directly related to accident mitigation. The features within the scope of 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 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 which are not classified as ESF systems. The specific arrangement of these systems depends on (1) the type of plant (pressurized water reactor, boiling water reactor, etc.), (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 essential auxiliary supporting systems are reviewed by other branches in accordance with the SRP sections which address these systems.

There are two kinds of shutdown conditions: hot shutdown and cold shutdown. In either case, 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 both shutdown conditions for a specific plant, see Chapter 16, "Technical Specifications," in the applicant/licensee's 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 instrumentation and controls provided as part of an alternative or dedicated shutdown capability needed for compliance with GDC 3, "Fire Protection."

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.

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 Office of Nuclear Reactor Regulation (NRR) 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 HICB and other branches.

Typical systems required for safe shutdown are:

- Auxiliary feedwater systems,
- Residual heat removal systems, and
- Boric acid transfer systems.

Typical essential auxiliary supporting (EAS) systems are:

- Electric power systems,
- Diesel generator fuel storage and transfer systems,
- Instrument air systems,
- Heating, ventilation, and air conditioning (HVAC) systems for areas containing systems required for safe shutdown, and
- Essential service water and component cooling water systems.

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 Office of Nuclear Reactor Regulation (NRR) 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 HICB and other branches.

Voice communication between safe shutdown control areas is reviewed by HICB as part of its primary review responsibility for SRP Section 9.5.2.

II. Acceptance Criteria

The acceptance criteria and guidelines applicable to the I&C systems required for safe shutdown are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified as applicable to these systems. The review of the systems required for safe shutdown confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

1. Acceptance criteria for the review of the safe shutdown I&C systems are based on meeting the relevant requirements of the following regulations

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For post-accident monitoring systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by Generic Letters.

(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena."

General Design Criterion 4, "Environmental and Missile Design Bases."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

General Design Criterion 34, "Residual Heat Removal."

General Design Criterion 35, "Emergency Core Cooling."

General Design Criterion 38, "Containment Heat Removal."

2. Additional acceptance criteria applicable to safe shutdown systems proposed for design certification under 10 CFR 52 include

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Function."

3. Additional acceptance criteria applicable to safe shutdown systems proposed as part of combined license applications under 10 CFR 52 include

10 CFR 52.79(c), "ITAAC in Combined License Applications."

Section 7.1, Table 7-1 and Appendix 7.1-A list the requirements, standards, regulatory guides, and branch technical positions (BTP) that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff to implement the relevant requirements of the NRC regulations identified above.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any instrumentation and control system. This part of section 7.4 highlights specific topics that should be emphasized in the review of safe shutdown systems.

The review should include an evaluation of the safe shutdown systems design against the guidance of ANSI/IEEE Std 279, or Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"), depending upon the applicant/licensee's commitment regarding these design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address specific design requirements.

Appendices 7.1-B and 7.1-C discuss ANSI/IEEE Std 279 and IEEE Std 603, respectively, 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 on a 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 of the design meeting the specific requirements of ANSI/IEEE Std 279 or IEEE Std 603.

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 which are unique to safe shutdown, in addition to those systems required for safe shutdown which are not classified as ESF systems.

The safe shutdown systems review should address the topics identified as applicable by Table 7-1. 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.

- The review confirms that I&C required for safe shutdown (where appropriate based on their safety function):

  – Provides the required redundancy,

  – Meets the single-failure criterion,

  – Provides the required capacity and reliability to perform intended safety functions on demand,

  – Provides the capability to function during and after design-basis events such as earthquakes and anticipated operational occurrences,

  – Provides the capability to 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

  – Provides the capability to be tested during reactor operation.

- Single-failure criterion — The remote control stations and the equipment used to maintain safe shutdown should be designed to accommodate a single failure. See Appendix 7.1-B item 3 or Appendix 7.1-C item 4.[1]

- Independence — See Appendix 7.1-B item 7 and 8 and Appendix 7.1-C item 11 and 24.

- Use of digital systems — See Appendix 7.0-A.

- Periodic testing — See Appendix 7.1-B item 11 or see Appendix 7.1-C items 12 and 27.

- Remote shutdown capability — 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 (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 steam generator level, steam generator pressure, pressurizer pressure, pressurizer level, reactor coolant temperature, and

[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 upon 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 which could force the evacuation of the control room and result in a need to effect safe shutdown remote from the control room. Branch Technical Position CMEB 9.5.-1 establishes the bases for safe shutdown with respect to fire protection. Specifically, fire damage limits as they impact on 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 to fires. The evaluation of conformance to the BTP is addressed in SRP Section 9.5.1. Therefore, the application of the single-failure criterion to remote shutdown is only applicable for other events which could cause the control room to become uninhabitable. These events would not result in consequential damage or unavailability of systems required for safe shutdown.

auxiliary feedwater flow. Typical parameters for BWR displays are reactor vessel water level and pressure and high pressure core injection system flow.

The remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions which 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. Since 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.

- 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.

In certain instances, it will be the Staff's judgment that, for a specific case under review, emphasis should be placed on specific aspects of the design, while other aspects of the design need not receive the same emphasis and in-depth review. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the NRC's regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the safety evaluation report (SER):

The NRC staff concludes that the design of the safe shutdown systems and the safe shutdown initiation of the essential auxiliary support (EAS) 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 upon 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 information systems important to safety are appropriately isolated from safety systems, including the safety portions of the information systems. Therefore, the Staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 5.55a(h) and the requirements of GDC 24.

The review included the identification of those systems and components for the safe shutdown systems which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon 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 instrumentation and controls have been provided to maintain variables and systems which 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.

Instrumentation and controls 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 instrumentation and controls 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 instrumentation and control 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 General Design Criteria 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 dependence of these systems on the available essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of EAS systems, the Staff concludes that the design of the safe shutdown systems is compatible with the functional requirements of EAS systems.

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 Reg. 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.

Note: the following findings apply only to applications under 10 CFR 52.

The safe shutdown systems design appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the safe shutdown systems satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the safe shutdown systems examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the safe shutdown systems satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the safe shutdown systems [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the safe shutdown systems satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The safe shutdown systems contain the following elements which differ significantly from evolutionary changes from light water reactor designs of plants which have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience] the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the safe shutdown systems satisfy the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant/licensee, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the safe shutdown systems design to satisfy the requirements of 10 CFR 52.47(a)(2).

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 upon prior NRC review and approval as noted [List applicable system or topics and identify references].

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

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

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

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, 1996.

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