U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

SECTION 7.4 SAFE SHUTDOWN SYSTEMS

REVIEW RESPONSIBILITIES

Primary - Instrumentation and Control Systems Branch (ICSB)

Secondary - None

I. AREAS OF REVIEW

The areas reviewed in this section of the applicant's safety analysis report (SAR) include those instrumentation and control systems associated with systems used to achieve and maintain a safe shutdown condition of the plant. 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. Such features may involve individual component control for safe shutdown versus sytem level actuation for accident mitigation or system operating modes which involve considerations which differ for safe shutdown and accident mitigation. 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 the type of plant (pressurized water reactor, PWR; boiling water reactor, BWR; etc.) as well as on individual plant design features, and 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, it is necessary that reactivity control systems maintain a subcritical condition of the core and that residual heat removal systems operate to maintain adequate cooling of the core. For a precise definition of both shutdown conditions for a specific plant, see Chapter 16, "Technical Specifications," in the applicant's safety analysis report (SAR). Section 7.5 includes the information systems important to safety that provide information which is used for the manual control of systems required for safe shutdown.

The objective 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 will perform their safety functions during all plant conditions for which they are required.

The review performed for a construction permit application may be based on preliminary designs and the depth of information need only be sufficient to provide reasonable assurance that the final design will conform to the design bases and applicable criteria with an adequate margin for safety. The review performed for an operating license (OL) application is based upon detailed design information that confirms that the final design conforms to the design bases and applicable criteria. The depth of the review for an OL application should be sufficient to conclude that the requirements of the Commission regulations have been satisfied. The depth of the review for the balance of the criteria should be sufficient to conclude that the systems conform with the guidelines to the extent to support the findings of conformance to the regulations.

The review includes the process to sensor coupling, sensors, initiating circuitry, logic bypasses, interlocks, redundancy features, and actuated devices of those systems which provide the necessary instrumentation and control functions to achieve and maintain safe shutdown.

Typical systems required for safe shutdown are:

Auxiliary Feedwater Systems
Residual Heat Removal Systems
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
Essential Service Water and Component Cooling Water Systems

The scope of the ICSB review of Section 7.4 of an SAR includes:

1. The descriptive information, functional control diagrams, piping and instrument diagrams (CP), and electrical schematics (OL) pertaining to safe shutdown systems.

2. The acceptance criteria, guidelines, and design bases for the design of the systems required for safe shutdown (CP).

3. The applicant's analysis of conformance to the acceptance criteria, guidelines, and design bases for the systems required for safe shutdown (OL).

In addition, the ICSB will coordinate with branches that interface with the overall review of systems required for safe shutdown including the following:

The Power Systems Branch (PSB) evaluates the redundancy of power sources, the criteria for physical separation of redundant electrical equipment, cabling, and cable trays; criteria for providing control and motive power

to these systems and the provisions for sharing electrical systems between unit plants as part of its primary review responsibility for SRP Section 8.2, 8.3.1, and 8.3.2.

The Chemical Engineering Branch (CMEB) evaluates the conformance to the fire protection requirements with respect to remote shutdown capability as part of its primary review responsibility for SRP Section 9.5.1.

The Auxiliary Systems Branch (ASB) evaluates the adequacy of those auxiliary systems required for the proper operation of the systems required for safe shutdown as part of its primary review responsibility for SRP Chapters 9 and 10. These systems include compressed air, cooling water, boration, lighting, communications, heating, air conditioning, etc. The ASB review confirms the physical arrangement of components and structures related to the systems required for safe shutdown and their supporting systems, and determine that single events will not disable redundant systems.

The Containment Systems Branch (CSB) reviews the containment ventilation and atmosphere control systems provided to maintain required environmental conditions for electrical and instrumentation equipment associated with the systems for safe shutdown and located inside containment as part of its primary review responsibility for SRP Chapter 6.0.

The Equipment Qualifications Branch (EQB) reviews the seismic and environmental qualification of instrumentation and electrical systems as part of its primary review responsibility for SRP Sections 3.10 and 3.11. This includes the design criteria and testing methods and procedures employed in the seismic design and installation of Category I instrumentation and electrical equipment.

The Reactor Systems Branch (RSB) reviews the systems identified as required for safe shutdown, and confirms that the configuration and design bases of these systems are acceptable, and that all design parameters such as temperature, pressure, flow rate, and reactivity can be controlled within acceptable limits as part of its primary review responsibility for these systems in SRP Chapters 5 and 6.

The Human Factors Evaluation Branch (HFEB) evaluates the adequacy of the arrangement and location of instrumentation and controls required for safe shutdown, for situations where shutdown is to be accomplished from locations outside of the main control room as part of its primary review responsibility for SRP Chapter 18.0.

For those areas of review identified above as being reviewed as part of the primary review responsibility of other branches, the acceptance criteria necessary for the review and their methods of application are contained in the referenced SRP section of the corresponding primary branch.

II. ACCEPTANCE CRITERIA

The acceptance criteria and guidelines applicable to the 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 for these systems. The review of the systems required for safe shutdown in this section of the SAR confirms that these

systems conform to the requirements of the acceptance criteria and guidelines. The branch technical positions are used when a particular design problem and an acceptable solution have been identified.

Acceptance criteria for the review areas of this SRP section are:

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

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

3. General Design Criterion 13, "Instrumentation and Control."

4. General Design Criterion 19, "Control Room."

In addition to the acceptance criteria indicated above, the instrumentation and control systems are reviewed for conformance to the following acceptance criteria, applicable to systems required for safe shutdown, with regards to operability from onsite and offsite electrical power and with regards to single failure assumptions:

1. General Design Criterion 34, "Residual Heat Removal."

2. General Design Criterion 35, "Emergency Core Cooling."

3. General Design Criterion 38, "Containment Heat Removal."

Regulatory Guides, Branch Technical Position and industry standards that provide information, recommendations and guidance and in general describe a basis acceptable to the staff that may be used to implement the requirements of the Commission regulations identified above are given in SRP Section 7.1, Table 7-1 (Ref. 1) and SRP Appendix 7-A (Ref. 2).

III. REVIEW PROCEDURES

This subsection describes the general procedures to be followed in reviewing the systems required for safe shutdown. The bases for the evaluation of conformance to the requirements of the acceptance criteria and guidelines may be based upon referenced approved designs or a specific design review of the system as documented in the SAR. The category of referenced approved designs include topical reports, standard design approvals, and designs of systems which are identical to plants which have been reviewed and approved by the Staff. If any aspect of a design is not identical to that which is referenced, an evaluation must be made to address the adequacy of the differences and the conclusions included in the safety evaluation report.

Background information of interest in the review of the systems required for safe shutdown is found in a number of SAR sections. A list of these is given in SRP Section 7.3 for reference purposes. Most of these reference sections also provide background information for other SRP sections in Chapter 7. Reference to these sections of the SAR given in SRP Section 7.3 is made to gain an understanding of the purpose of the systems and an understanding of how the systems are designed and how they function. The main objective of the review of systems required for safe shutdown is to confirm that the design of these systems conform to the requirements of the acceptance criteria.

Review guidance for conformance to the GDC are provided in Appendix A of SRP Section 7.1 (Ref. 3). The review guidance includes references to the guidelines in regulatory guides and industry codes and standards where applicable. An audit review of the safe shutdown systems should be made to confirm that the systems conform to the guidelines to support the conclusions of conformance to the regulations.

The review confirms that the systems required for safe shutdown include the required redundancy; meet the single failure criterion; provide the required capacity and reliability to perform intended safety functions on demand; provide the capability to function during and after design basis events such as earthquakes and anticipated operational occurrences; provide 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 provide the capability to be tested during reactor operation.

A major portion of the systems required for safe shutdown are also used as engineered safety features 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 review is coordinated with RSB and ASB to confirm the acceptability of the redundancy and independence of systems required for safe shutdown.

The descriptive information, including the electrical one-line diagrams aid P&IDs (CP and OL) and electrical schematics (OL), should be reviewed to verify that the necessary redundancy is provided. This should include instrumentation channels used to sense vital parameters such as temperature, pressure, water level, etc.; the associated logic and actuated devices; and the motive and control power sources.

Conformance with the single failure criterion is verified by review of the same information as for redundancy. The guidance provided by IEEE Std 379 and Regulatory Guide (RG) 1.53 should be used for ascertaining that a given design is single failure proof. A particularly important but subtle point to check is one cited in position 4 of RG 1.53, wherein a single d-c source supplies control power for one channel of system logic and for the redundant actuator circuit.

Certain areas of review need close coordination between review branches in order to make a determination that a specific aspect of the design meets the applicable criteria. Seismic qualification of Class 1E equipment, flood protection of safety-related systems and components, and effects of high energy fluid line breaks inside containment or near safety-related equipment are the major areas for which branch coordination is essential in evaluating the acceptability of a given design feature.

RG 1.75 provides guidance for satisfying the acceptance criteria with respect to the identification of power and signal cables, cable trays, and instrument panels related to systems required for safe shutdown. The criteria for identification and separation of redundant systems discussed in RG 1.75 are presented in sufficient detail to make their application self-explanatory.

RGs 1.22, 1.47, and 1.68 provide the requirements that the design of systems required for safe shutdown should meet with regard to preoperational and periodic inservice testing. The primary review responsibility for the preoperational testing is with the PTRB. Periodic testing and downtime

restrictions are specified in the technical specifications. The review procedures for technical specifications are covered in SRP Chapter 16.0.

An important area to be reviewed is the remote or local control stations that are required by GDC 19 for the safe shutdown of the plant in case the main control room becomes uninhabitable. Plant designs should provide for control stations in locations removed from the main control room that may be used for manual control and alignment operations needed to achieve and maintain a hot shutdown and subsequently to be able to achieve a cold shutdown. Equipment required for safe shutdown should be operable from local control panels. Access to these local control panels should be under strict administrative controls. Communications between the local control panels/stations should be provided. The design of these control stations should provide appropriate readouts so that the operator can monitor the status of the shutdown. Typical readouts are steam generator level, steam generator pressure, pressurizer pressure, pressurizer level, reactor coolant temperature, and auxiliary feedwater flow.

The remote control stations and the equipment used to maintain safe shutdown should be designed to accommodate a single failure.* Equipment located at these stations which is required for safe shutdown should be capable of operating independently (without interaction) of the equipment in the main control room. The design should be such that a single failure will not prevent the capability for affecting safe shutdown from the remote control stations. The remote control stations 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. The remote control station equipment should be designed to the same standards as the corresponding equipment in the main control room. Control transfer devices should be located remote from the main control room and their use should initiate an alarm in the control room.

An important part of the review is the engineering drawing review at the OL stage. The drawing review should confirm that the design and layout meet the applicable criteria listed under subsection II. An applicant may choose to take exceptions to some of the guidelines in the branch technical positions,

*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 to SRP Section 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 shutdown 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 be uninhabitable. These events would not result in consequential damage or unavailability of systems required for safe shutdown.

regulatory guides, IEEE standards and propose alternate ways of meeting the General Design Criteria requirements (which are mandatory). Any exceptions to the criteria are evaluated on an individual case basis. Exceptions are judged on the basis of the proposed design providing an equivalent level of safety and conservatism.

A site visit should be performed before the evaluation findings are written for an OL. A site visit should include an audit verification that the design and layout criteria reviewed during the drawing review are implemented. An outline of topics for a site visit is provided in Appendix 7-B (Ref. 4) to SRP Chapter 7.

In certain instances, it will be the reviewer'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 nonuniform placement of emphasis are the introduction of new design features or the utilization in the design of design 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 Commission's regulations.

IV. EVALUATION FINDINGS

The reviewer verifies that sufficient information has been submitted and the review supports conclusions of the following type, to be included in the staff's safety evaluation report:

> The review of systems required for safe shutdown included the processor to sensor coupling sensors, initiating circuitry, logic elements, interlocks, redundancy features, and actuated devices, and that provide the instrumentation and control functions that prevent the reactor from returning to criticality and provide means for adequate residual heat removal from the core, containment, and other vital components and systems.
>
> The staff concludes that the systems required for safe shutdown are acceptable and meet the relevant requirements of General Design Criteria 2, 4, 13, 19, 34, 35, and 38. This conclusion is based on the following:
>
> We have conducted an audit review of these systems or conformance to guidelines of the regulatory guides and industry codes and standards applicable to these systems. In Section 7.1 of this SER we concluded that the applicant had adequately identified the guidelines applicable to these systems. Based upon our audit review of the system design for conformance to the guidelines we find that there is reasonable assurance that systems conform fully to the guidelines applicable to these systems.
>
> Our review has included the identification of those systems and components required for safe shutdown which are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments and missiles. Based upon our review we conclude that the applicant has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of this SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore we find that the identification of these systems

and components satisfies this aspect of the General Design Criterion (GDC) 2 and GDC 4.

Based on our review we conclude 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, we find 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 have 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, we conclude that the systems required for safe shutdown satisfy the requirements of GDC 19.

Our review of the instrumentation and controls required for safe shutdown has examined the dependence of these systems on the availability of essential auxiliary supports (EAS) systems. Based on our review and coordination with those having primary review responsibility for the EAS system, we conclude that the design of EAS systems are compatible with the functional performance requirements of these systems. Therefore, we find the interfaces between the design of safe shutdown systems and the design of EAS systems to be acceptable.

Our review of the instrumentation and control systems required for safe shutdown included conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures consistent with the General Design Criteria applicable to safe shutdown systems. We conclude 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.

The conclusions noted above for the systems required for safe shutdown are applicable to all portions of the system except for the following for which acceptance is based upon prior Commission review and approval as noted. (List applicable systems or topics and identify references)

V. IMPLEMENTATION

The following is intended to provide guidance to applicants and licensees regarding the NRC staff's plans for using this SRP section.

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

Implementation schedules for conformance to parts of the method discussed herein are contained in the referenced regulatory guides.

VI. REFERENCES

1. Standard Review Plan Section 7.1, Table 7-1, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety."

2. Standard Review Plan Appendix 7-A, "Branch Technical Positions (ICSB)."

3. Standard Review Plan Section 7.1, Appendix A, "Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety."

4. Standard Review Plan Appendix 7-B, "General Agenda, Station Site Visits."