



U.S. NUCLEAR REGULATORY COMMISSION  
**STANDARD REVIEW PLAN**  
OFFICE OF NUCLEAR REACTOR REGULATION

SECTION 7.4

SYSTEMS REQUIRED FOR SAFE SHUTDOWN

REVIEW RESPONSIBILITIES

Primary - Electrical, Instrumentation and Control Systems Branch (EICSB)

Secondary - Reactor Systems Branch (RSB)  
Containment Systems Branch (CSB)  
Auxiliary and Power Conversion Systems Branch (APCSB)  
Mechanical Engineering Branch (MEB)  
Quality Assurance Branch (QAB)I. AREAS OF REVIEW

The systems reviewed under this plan are those instrumentation and control systems associated with parts of the nuclear steam supply system (NSSS) used to achieve and maintain a safe shutdown condition of the plant. The specific arrangement of these parts of both the primary and secondary loops of the NSSS 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. There are two kinds of shutdown conditions; hot shutdown and cold shutdown. A hot shutdown is a stable condition of the reactor achieved shortly after a programmed or emergency shutdown (scram) of the plant has taken place. A cold shutdown is a stable condition of the plant achieved after the residual heat removal process has brought the primary coolant temperature below 200°F. 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).

Examples of systems required for achieving and maintaining a safe shutdown are the auxiliary feedwater system, the residual heat removal system, and the boric acid transfer system (for PWR's).

The review of the instrumentation and control systems associated with the various parts of the NSSS required for safe shutdown, along with the equipment required for their proper alignment from the main control room or from other locations outside the control room, is the responsibility of the EICSB. The review includes the sensors, initiating circuitry, logic bypasses,

---

**USNRC STANDARD REVIEW PLAN**

Standard review plans are prepared for the guidance of the Office of Nuclear Reactor Regulation staff responsible for the review of applications to construct and operate nuclear power plants. These documents are made available to the public as part of the Commission's policy to inform the nuclear industry and the general public of regulatory procedures and policies. Standard review plans are not substitutes for regulatory guides or the Commission's regulations and compliance with them is not required. The standard review plan sections are keyed to Revision 2 of the Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. Not all sections of the Standard Format have a corresponding review plan.

Published standard review plans will be revised periodically, as appropriate, to accommodate comments and to reflect new information and experience.

Comments and suggestions for improvement will be considered and should be sent to the U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, Washington, D.C. 20555.

---

11/24/75

interlocks, redundancy features, and actuated devices of those systems and auxiliaries which provide the necessary instrumentation and control functions. The EICSB review should confirm that the systems required for safe shutdown, as defined above, and their supporting systems will perform design functions as required for plant shutdown and conform to all applicable acceptance criteria.

The descriptive information contained in the SAR, including single line diagrams, electrical schematics, piping and instrumentation diagrams (P&ID's), and physical arrangement diagrams are reviewed to ascertain that the systems required for safe shutdown meet the acceptance criteria listed in Section II of this plan. For a construction permit (CP) review, a commitment to meet these criteria, together with a preliminary design, can suffice in cases where the design of these systems has not been completed. For an operating license (OL) review, however, the actual design and its implementation should be verified to meet these criteria.

The EICSB review includes the following specific items:

1. The redundancy of power sources, logic, and instrumentation provided for the operation and status monitoring of systems required for safe shutdown. This requires the review of the descriptive information contained in the SAR, functional diagrams, electrical schematics, and P&ID's.
2. The ability of systems required for safe shutdown to function after sustaining a single failure. This requires the review of the descriptive information and diagrams as in (1) above, and in addition the drawings showing the physical layout of the instrumentation, control equipment, and cabling, the design criteria for physical separation of redundant electrical equipment and cabling, the design criteria for providing control and motive power to these systems, the control arrangements for controlled electrically-operated valves, and provisions for sharing of electrical systems between units in multi-unit plants.
3. The criteria for design of instrumentation and electrical equipment, cabling, cable trays, and structures housing parts of the systems required for safe shutdown.
4. The environmental qualification of the electrical and instrumentation equipment and cabling.
5. The online testability of the systems and indication of bypassed or inoperable status of the systems required for safe shutdown.

The APCS should evaluate the adequacy of those auxiliary systems required for the proper operation of the systems required for safe shutdown. These include systems concerned with compressed air requirements, reactor coolant chemistry, boron concentration, lighting, air conditioning, etc. In particular, the APCS should determine that the piping, ducting, and valving of redundant vital auxiliary supporting systems meet the single failure criterion. In addition, the APCS should review 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 these systems.

The CSB should review the containment ventilation and atmosphere control systems provided to maintain required environmental conditions for electrical and instrumentation equipment associated with the systems required for safe shutdown and located inside containment.

The MEB review should confirm that the seismic qualification of instrumentation and electrical systems is acceptable. 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 RSB should review the systems identified as required for safe shutdown, and confirm that the configuration and design bases of these systems are correct, and that all design parameters such as temperature, pressure, flow rate, and reactivity can be controlled within acceptable limits. This information should be provided to the EICSB. For situations where shutdown is to be accomplished from locations outside of the main control room, the RSB review should establish the adequacy of needed systems and any differences in system alignment or operation that are required to achieve and maintain safe shutdown.

The QAB review should verify that the quality assurance program proposed by the applicant includes the systems required for safe shutdown.

## II. ACCEPTANCE CRITERIA

The design materials, qualifications testing, and surveillance of systems required for safe shutdown are covered by several general design criteria (GDC), IEEE standards, regulatory guides, and branch technical positions. A list of applicable criteria, standards, guides, and technical positions is given in Table 7-1 and Appendix 7-A, attached to the standard review plans for Chapter 7.

The instrumentation and control systems required for safe shutdown are acceptable when it is determined that these systems satisfy the following requirements:

1. They have the required redundancy.
2. They meet the single failure criterion.
3. They have the required capacity and reliability to perform intended safety functions on demand.
4. They are capable of functioning during and after certain design basis events such as earthquakes, accidents, and anticipated operational occurrences.
5. They are testable during reactor operation.

The criteria listed in Table 7-1 are utilized as the bases for determining that these requirements are met. How these criteria are applied during the review process is discussed in Section III of this plan. The applicability of the acceptance criteria to the review of the systems required for safe shutdown is as follows:

1. System Redundancy Requirements

GDC 26, 33, 34, and IEEE Std 279 specify the requirements that systems required for safe shutdown, among others, must meet with regard to all operating conditions (such as loss of offsite power), so that they can perform their safety function assuming a single failure. If a determination is made that the systems required for safe shutdown meet the requirements of these criteria, they are acceptable in this regard. Electrical and physical independence requirements as discussed in Standard Review Plans (SRP) 7.2 and 7.3 should be met.

2. Conformance with the Single Failure Criterion

IEEE Std 279, IEEE Std 379, and Regulatory Guide 1.53 provide recommendations and guidance for meeting the single failure criterion. Regarding the application of the single failure criterion to the design of manually-controlled electrically-operated valves, the acceptability of proposed designs is based on Branch Technical Position EICSB 18.

3. Identification of Cables, Cable Trays, and Instrument Panels

The method used for identifying power and signal cables and cable trays as safety-related equipment, and the identification scheme used to distinguish between redundant cables, cable trays, and instrument panels should be in accordance with the recommendations of Sections 5.1.2 and 5.6.3 of Regulatory Guide 1.75, "Physical Independence of Electric Systems," and Section 4.2.2 of IEEE Std 279. Color coding is a preferred method of identification.

4. Vital Supporting Systems

The instrumentation, control, and electric equipment associated with the auxiliary systems that support the systems required for safe shutdown should meet the same acceptance criteria as for the systems they support.

5. System Testing, Quality Assurance, and Surveillance

GDC 1, 21, IEEE Std 279, IEEE Std 336, and Regulatory Guides 1.22, 1.47, and 1.68 contain the applicable acceptance criteria with regard to preoperation and periodic testing, quality assurance, and design provisions for indicating the availability of systems required for safe shutdown and essential auxiliary supporting systems.

For the areas of review identified in Section I as responsibilities of other branches, the applicable acceptance criteria are included in the corresponding review plans.

III. REVIEW PROCEDURES

The main objectives of the review of systems required for safe shutdown are to determine that the design of these systems includes the required redundancy; meets the single

failure criterion; provides the required capacity and reliability to perform intended safety functions on demand; and provides the capability to function during and after design basis events such as earthquakes and anticipated operational occurrences.

For a CP review, the descriptive information contained in the preliminary safety analysis report (PSAR), including the design bases and their justification with regard to the acceptance criteria, electrical single line drawings, and P&ID's are reviewed to determine that the basic design features and the commitments made provide assurance that the final design will meet the acceptance criteria. During the OL stage of review, it is verified that the acceptance criteria are met through review of the final electrical and instrumentation drawings and the physical layout drawings, and a site visit, during which a spot-check verification of the design is performed. In order to verify that the acceptance criteria are satisfied, the review is performed in accordance with the following specific procedures.

A major portion of the systems required for safe shutdown are also used as engineered safety feature (ESF) systems, as discussed in SRP 7.3. A major portion of the systems required for safe shutdown are also used as engineered safety feature (ESF) systems, as discussed in SRP 7.3. This plan includes the safe shutdown systems configurations which are not part of ESF systems or result from a realignment of ESF systems. The RSB and APCSB confirm the acceptability of the proposed configuration and the redundancy required for systems required for safe shutdown as specified in GDC 26, 33, 34. The descriptive information, including the electrical one-line diagrams and P&ID's (for CP and OL reviews) and electrical schematics (for the OL review) 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 as specified by IEEE Std 279 and Regulatory Guide 1.53 is verified by review of the same information as for redundancy and may be done, to some extent by necessity, at the same time. The guidance provided by Regulatory Guide 1.53 is excellent 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 Regulatory Guide 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 primary and secondary review branches in order to make a determination that a specific aspect of the design meets the applicable criteria. Seismic qualification of Class IE 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.

For a multi-unit plant where electrical systems are shared, thus resulting in more and complex interaction modes, a fault-tree and decision-tree analysis may be required from the applicant to show that a single failure or a single event resulting in multiple failures will not result in unacceptable consequences with respect to the capability of

systems required for safe shutdown to perform safety functions when required. Additional guidance with regard to the single failure criterion as it relates to shared electric power systems is given in the review plans for Chapter 8.

For the case of manually-controlled electrically-operated valves in these systems, the acceptability of the proposed design is based on satisfying Branch Technical Position EICSB 18. This position basically states that it is acceptable to disconnect electric power to a safety-related valve as means of removing the possibility of an active failure of that valve.

Regulatory Guide 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 Regulatory Guide 1.75 are presented in sufficient detail to make their application self-explanatory.

GDC 1, 21, 22, and 23, IEEE Std 279, IEEE Std 336, and Regulatory Guides 1.22, 1.47, and 1.68 provide the requirements that the design of systems required for safe shutdown must meet with regard to preoperational and periodic inservice testing. The primary review responsibility for the preoperational testing is with the QAB. Periodic testing and downtime restrictions are specified in the technical specifications. The review procedures for technical specifications are covered in SRP 7.1.

Another 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. 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, 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 as to prevent a single failure in the main control room or the cable spreading room from defeating the capability for affecting safe shutdown from the remote control stations, and vice versa. The remote control station equipment should be designed to the same standards as the corresponding equipment in the main control room, including appropriate IEEE criteria. Control transfer devices should be located away from the main control room and cable spreading areas, and their actuation should cause 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:

1. Verify that a complete set of drawings has been submitted that includes logic diagrams, P&IDs, and location layout drawings for these systems.
2. Verify that the submitted drawings represent the actual system designs and layouts for the particular plant, and that those drawings submitted as "typical" of a system are so identified.
3. Verify that the design and layout meet the applicable criteria listed under Section II of this plan.

The environmental qualification of components and cabling of systems required for safe shutdown should be the same as for the ESF systems discussed in SRP 7.3.

An applicant may choose to take exceptions to some of the acceptance criteria in the branch technical positions, guides, IEEE standards (other than IEEE Std 279, which is a mandatory requirement) and propose alternate ways of meeting the GDC 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.

In general, the applicant will have design criteria that supplement or clarify the mandatory criteria. In the evaluation of such criteria, the reviewer can use the guidance listed above to determine whether the applicant's design criteria are adequate.

For the purpose of the EICSB review, no distinction should be made between the design criteria for systems required for safe shutdown and the criteria for the instrumentation and controls for essential auxiliary supporting systems.

Certain system designs and design features are submitted on a generic basis in the form of topical reports. Reference to a topical report is an acceptable alternative to submitting information in an application for a CP or an OL. Generally, topical reports pertain to standardized systems and qualification tests. If a referenced topical report has been accepted after staff review, the subjects of the report should not be reviewed again in connection with a particular application. If the referenced topical report has not been reviewed up to the time of the application review, it should be reviewed and treated in the same manner as the SAR itself. It may be necessary to assure conformance to requirements by getting additional information and justifications from the applicant. If the topical report has been rejected, then the applicant should be so advised and requested to submit information or design changes that are acceptable.

References other than topical reports should be obtained from the library or other sources, or the applicant asked to supply a copy.

A site visit and inspection should be performed before the evaluation findings are written for an OL. A site inspection should include a spot-check verification that the design and layout criteria reviewed during the drawing review are actually implemented at the hardware assembly stage. A site visit should be coordinated with the licensing project manager and the regional office that has jurisdiction over the geographic area in which the plant is located. Specific items to be considered include:

1. Separation and identification of redundant safety-related instrumentation channels, cabling, cable trays, and instrument rack terminations.
2. Separation of actuating switches in control panels for redundant safety-related equipment such as inboard and outboard isolation valves, coolant pumps, diesel-generator sets, etc.
3. Testability provisions and calibration procedures for instrumentation channels required for safe shutdown.
4. Adequacy of local control panels for remote shutdown, especially with regard to sufficient monitoring channels and actuating devices that the operators would need to perform and maintain a safe shutdown.

For a full outline of topics for a site visit, see Appendix 7-B to this Chapter.

In certain instances, it will be the reviewer's judgement 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 placement of emphasis are the introduction of new design features or the utilization in the design of design features previously reviewed and found acceptable.

#### 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 includes the sensors, initiating circuitry, logic elements, interlocks, redundancy features, actuated devices, and auxiliaries 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 scope of review of systems required for safe shutdown for the plant included single line diagrams (CP and OL) and schematic diagrams (OL) and descriptive information for these systems and for auxiliary systems essential for their operation. The review has included the applicant's proposed design criteria, design bases, and analyses. The review has also included the applicant's analyses of the manner in which the design of these systems and their auxiliary supporting systems conform to the proposed design criteria.



"The basis for acceptance in the staff review has been conformance of the applicant's designs, design criteria, and design bases for systems required for safe shutdown and essential supporting auxiliaries to the Commission's regulations as set forth in the general design criteria, and to applicable regulatory guides, branch technical positions, and industry standards. These are listed in Table 7-1.

"The staff concludes that the design of systems required for safe shutdown conforms to the applicable regulations, guides, technical positions, and industry standards and is acceptable."

V. REFERENCES

1. Standard Review Plan Table 7-1, "Acceptance Criteria for Controls."
2. Standard Review Plan Appendix 7-A, "Branch Technical Positions (EICSB)."
3. Standard Review Plan Appendix 7-B, "General Agenda, Station Site Visits."

11/24/75

SRP 7.5