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

SECTION 7.3 ENGINEERED SAFETY FEATURE SYSTEMS

REVIEW RESPONSIBILITIES

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

Secondary - Auxiliary and Power Conversion Systems Branch (APCSB)
Containment Systems Branch (CSB)
Reactor Systems Branch (RSB)

I. AREAS OF REVIEW

This standard review plan (SRP) covers the portion of the protection system used to initiate and control operation of the engineered safety feature systems and essential auxiliary supporting systems. This portion of the protection system is called the engineered safety feature actuation system (ESFAS).

Typical engineered safety feature (ESF) systems are:

Containment and Reactor Vessel Isolation Systems
Emergency Core Cooling Systems (ECCS)
Containment Heat Removal and Depressurization Systems
Pressurized Water Reactor (PWR) Auxiliary Feedwater Systems (See SRP 7.4 for review of the safe shutdown functions of this system)
Boiling Water Reactor (BWR) Standby Gas Treatment Systems
Containment Air Purification and Cleanup Systems
Containment Combustible Gas Control Systems

Typical essential auxiliary supporting systems are:

Electric Power Systems (See Chapter 8 for review plans for these systems)
Diesel Generator Fuel Storage and Transfer Systems
Instrument Air Systems
Heating, Ventilating, and Air Conditioning (HVAC) Systems for ESF Areas
Essential Service Water Systems

The descriptive information, functional control diagrams, piping and instrument diagrams, electrical schematics (operating license stage only), and physical arrangement drawings,

as presented in the applicant's safety analysis report (SAR), are reviewed. The objectives are to determine that the engineered safety feature actuation system satisfies applicable design criteria and will perform as intended during all plant operating conditions and accident conditions for which its function is required. The most significant difference between the review performed for a construction permit (CP) application and that performed for an operating license (OL) application is that the CP review can be based on a preliminary design. The depth of detailed information need only be "sufficient to provide reasonable assurance that the final design will conform to the design bases with adequate margin for safety (Ref. 1)." In addition, "a construction permit...will not constitute Commission approval of the safety of any design feature or specification unless the applicant specifically requests such approval and such approval is incorporated in the permit (Ref. 2)."

The review of the information presented and referenced in Section 7.3 of an SAR is primarily directed to the engineered safety feature actuation system (ESFAS), i.e., the instrumentation and controls used to initiate and control the operation of the engineered safety features. The scope of the EICSB review of Section 7.3 of an SAR includes:

1. The descriptive information, including single line diagrams (CP) and schematic diagrams (OL) pertaining to the ESFAS. The ESFAS includes all electric and electromechanical equipment involved in detecting a plant condition requiring operation of an ESF system and in initiating the operation of the ESF system.

2. The descriptive information pertaining to the instrumentation and control systems for those auxiliary supporting systems that are essential to the operation of either the ESFAS or the ESF systems.

3. The applicant's proposed design criteria for the ESFAS and the instrumentation and controls of essential auxiliary supporting systems.

4. The applicant's analysis of the adequacy of the proposed design criteria and design bases for the ESFAS and the instrumentation and controls of auxiliary supporting systems.

5. The applicant's analyses of how the design of the ESFAS and auxiliary supporting systems conform to the design criteria for these systems.

The RSB and the CSB review, for those ESF systems within their review responsibilities, the following aspects of ESFAS:

(1) The adequacy of the monitored variables, i.e., the suitability of parameters, such as pressure, for initiating operation of a given ESF system.

(2) The acceptability of the proposed trip set points.

The APCSB will advise EICSB of any corrections to the SAR descriptions of auxiliary supporting systems essential to ESF systems and of time intervals available to initiate operation of auxiliary supporting systems.

II. ACCEPTANCE CRITERIA

Acceptance criteria for the review areas of this plan are referenced in Table 7-1 (Ref. 3), which lists the general design criteria (GDC), industry standards, regulatory guides, and branch technical positions that are applicable to the ESFAS and the instrumentation and controls of essential auxiliary supporting systems. These documents either establish design requirements or describe acceptable methods of implementing design requirements. In each of these categories, some documents set forth mandatory design criteria and others describe acceptable methods of design.

The GDC and IEEE Std 279-1971 set forth requirements that must be met by all designs for the ESFAS. In addition, these are also used for essential auxiliary supporting system instrumentation and controls. One purpose of the review is to verify that the applicant has committed to designing the ESFAS and the essential auxiliary supporting system instrumentation and controls in accordance with these mandatory criteria.

The regulatory guides are not mandatory and only set forth acceptable methods of implementing the mandatory criteria. The branch technical positions are used when a particular design problem has an identified and acceptable solution; they also are not mandatory.

Industry standards that are not endorsed by regulatory guides or incorporated in regulations or technical positions, or that have not been previously used and accepted in the licensing process, must be reviewed before they can be accepted as a sole basis for approval of a design. They are useful as guidance for identifying the subjects of importance to be considered in the review of the ESFAS. In all cases, the primary basis for acceptance of an ESFAS design is conformance to the mandatory criteria of the regulations.

III. REVIEW PROCEDURES

This section describes the general procedures to be followed in reviewing the ESFAS. For simplicity, it is written for the ESFAS for a single ESF system comprised of two identical, redundant subsystems. The same procedure should be applied to each ESF system and to each essential auxiliary supporting system.

Background information of interest in the review of the ESFAS is found in a number of SAR sections. A list of these is given below for reference purposes. Most of these reference sections also provide background information for other review plans in Chapter 7.

Chapter 1 of the SAR: for familiarization with the general operation of the plant, both safety and non-safety aspects.

Chapter 3: for a general understanding of the principal architectural and engineering designs of those structures, components, equipment, and systems important to safety.

Section 3.1: for exceptions to criteria applicable to the ESFAS, and for structures suitable for housing ESFAS equipment.

Chapters 4 and 5: for an understanding of the reactor and the reactor coolant system and its interconnections with the ESF systems.

Chapter 6: for the design bases, design features, and functional performance requirements of the ESF system.

Chapter 7: for a detailed understanding of the design and operation of the ESFAS.

Chapter 9: for the design bases, design features, and functional performance requirements of essential auxiliary supporting systems.

Chapter 15: for the courses of accidents for which the ESF system provides protective functions, the effects of failures of the protective functions, and the assumptions and initial conditions that form the bases of the accident analyses.

Chapter 16: for the proposed limiting conditions for operation for the ESF and the ESFAS.

It should be noted that reference to the above sections of the SAR is made to gain an understanding of the purpose of the ESF and an understanding of how the ESF system and the ESFAS are designed and are supposed to function. No "evaluation" should be made of these sections, i.e., the SAR description is taken at face value

The next step is to evaluate the design against the requirements of IEEE Std 279-1971. This procedure is detailed in Appendix A to this plan. The procedures in Appendix A address only those design requirements that are specific in nature. For example, paragraph 4.9 of IEEE Std 279-1971 requires that the design include means for checking the availability of each system input sensor during operation. Appendix A outlines a straightforward procedure that can be used to determine whether or not this requirement is met.

Appendix A discusses the requirements of IEEE Std 279-1971 and how they are used in the review of the ESFAS and the essential auxiliary supporting systems instrumentation and controls. Although the primary emphasis is on the equipment comprising the ESFAS, the reviewer should consider the protective functions on a systems level. It serves little purpose to approve an ESFAS design unless that design is compatible with the ESF systems and auxiliary supporting systems and unless the design and the accident analyses are compatible. It is not sufficient to judge the adequacy of the ESFAS only on the basis that the design meets the specific requirements of IEEE Std 279-1971. It is also necessary to judge the functional relationship between the ESFAS and the ESF systems themselves.

Other requirements for the ESFAS and the instrumentation and controls of essential auxiliary supporting systems are listed in Table 7-1. Many of these requirements are

general in nature and this permits various designs to meet them. For example, GDC 20 requires, in part, that the protection system be designed to sense accident conditions and to initiate the operation of (ESF) systems important to safety. A cursory examination of the descriptive information would be sufficient to determine whether or not the ESFAS is designed to sense accident conditions and initiate the ESF systems. Such general requirements are not detailed here as to review procedures. Specific design features and approaches are described in the EICSB technical positions in Appendix 7-A to Chapter 7 of the review plans.

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 provided and that his review supports conclusions of the following type, to be included in the staff's safety evaluation report:

"7.3 Engineered Safety Feature Actuation Systems (ESFAS)

The engineered safety feature actuation systems include the instrumentation and controls used to detect a plant condition requiring operation of an engineered safety feature (ESF) system, to initiate action of the ESF, and to control its operation. The scope of review of the ESFAS for the _____ plant included single line diagrams (CP and OL) and schematic diagrams (OL) and descriptive information for the ESFAS and for those auxiliary supporting systems that are essential to the operation of either the ESFAS or the engineered safety feature systems themselves. The review has included the applicant's proposed design criteria and design bases for the ESFAS and the instrumentation and controls of auxiliary supporting systems, and his analysis of the adequacy of those criteria and bases. The review also has included the applicant's analyses of the manner in which the design of the ESFAS and 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 the engineered safety feature actuation systems and necessary auxiliary supporting systems 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 the engineered safety feature actuation systems conform to all applicable regulations, guides, branch technical positions, and industry standards and is acceptable."

V. REFERENCES

1. 10 CFR §50.34(a)(3)(iii), "Contents of Applications; Technical Information. Preliminary Safety Analysis Report."

2. 10 CFR §50.35(b), "Issuance of Construction Permits."

3. Standard Review Plan Table 7-1, "Acceptance Criteria for Controls."

4. Standard Review Plan Appendix 7-A, "Branch Technical Positions (EICSB)."

APPENDIX A

STANDARD REVIEW PLAN 7.3

USE OF IEEE STD 279 IN THE REVIEW OF THE ESFAS AND INSTRUMENTATION AND CONTROLS OF ESSENTIAL AUXILIARY SUPPORTING SYSTEMS

This appendix discusses the requirements of IEEE Std 279-1971, Section 4, as they are used in the review of the ESFAS and instrumentation and controls of essential auxiliary supporting systems.

1. Section 4.1 - This section requires that the ESFAS perform automatically and with precision and reliability. These requirements must be met over the full range of transient and steady-state conditions of the energy supply and environment during all plant conditions in which the applicant's accident analyses take credit for functions performed by the ESFAS. Other criteria which set forth similar requirements are: GDC 2, 4, 10, 13, 20, 21, and 29.

   a. Automatic initiation is required for all protective functions that must be started within a short time of the indicated need for the function. Although GDC 20 appears to require automatic initiation of all protective functions, initiation solely by manual means has been acceptable. However, automatic initiation is preferable for all protective functions, even though they are not needed (according to the accident analyses) for a relatively long time. Where the protective action is initiated solely by manual means, all the actions that need or may need to be performed by the operator during the time interval are reviewed, as are the applicant's basis for not providing automatic initiation. In this latter regard, the cost of automatic initiation is not, of itself, sufficient justification for using manual initiation. If the reviewer's judgement is that manual initiation is sufficiently reliable, then the equipment used by the operator to detect the need for the protection function, and to verify that the protective function has been completed, it must also meet all the requirements applicable to automatically initiated protective functions. See also Branch Technical Position (BTP) EICSB 20.

   b. The precision required in the ESFAS is at least that assumed in the accident analyses.

   c. There are no quantitative requirements established for the reliability of the ESFAS. The design is reviewed to identify any unusual or unique equipment that has not previously been used in nuclear plants. The "type testing" (as defined in IEEE Std 323-1974) that demonstrates such equipment is capable of performing its function is reviewed. The design is also reviewed to assure that no unnecessary interlocks, time delays, or other complexities are introduced in the ESFAS circuits. Where such features do exist, the applicant's design bases and performance analyses should be reviewed to determine that the reliability of the ESFAS is not significantly reduced by the inclusion of such features.

2. Section 4.2 - This is the most fundamental of all the requirements that the ESFAS must meet. It is inherent in other criteria such as GDC 21, 22, 24, 34, 35, 38, 41, 44, 54, 55, and 56.

In evaluating ESFAS conformance with this requirement, the reviewer must examine several different aspects of each single failure to determine its effect. The time of occurrence of the failure and the plant conditions prevailing at that time can significantly alter the effects of any single failure.

a. The first step in a single failure analysis is to identify components that are not seismic Category I, those that are not qualified for accident and post-accident environments, and those that serve both safety and non-safety systems and whose failure can affect the performance of or create the need for the EFSAS. Each of the non-qualified and non-safety grade systems and components are assumed to fail to function if failure adversely affects ESFAS performance and are assumed to function if functioning adversely affects ESFAS performance.

b. Next, the consequences of the events for which the ESFAS is designed to provide protective functions are examined. All failures that can be predicted to occur as a direct or consequential result of an event are assumed to occur if such failures adversely affect ESFAS performance. In general, lack of adequate environmental or seismic qualification testing is sufficient basis to assume a direct or consequential failure of equipment.

c. After assuming the failures of non-safety grade, non-qualified equipment and those failures caused by an event, any other single failure in the ESFAS or its auxiliary supporting systems is arbitrarily assumed and the resultant performance of the ESFAS is analyzed to assure that the minimum protective function will be performed.

d. In choosing the postulated failure to be analyzed, no distinction is made between active and passive components in electrical systems. Further, electrical equipment serving mechanical components that are not required to function in a given event is treated the same as electrical equipment serving "active" mechanical components, i.e., those that must function. (See also BTP EICSB 18.)

e. The meaning of redundancy is discussed in IEEE Std 379 and Regulatory Guide 1.53. Basically, to be considered redundant, there must be no communication, either directly or indirectly, between two systems that can perform the same function. Thus, two systems, each of which can perform a protective function, are not redundant (and therefore do not meet the single failure criterion) if the failure of one system affects in any way the performance of the other system. This includes starting (or not starting) one system by sensing the failure (or operation) of the other system.

3. Section 4.3 - There are at present no specific criteria to judge the quality of the equipment used in the ESFAS. However, Appendix B to 10 CFR Part 50 provides some guidance from which a judgment may be made of the quality of equipment required for the ESFAS.

4. Section 4.4 - Standard Review Plans 3.10 and 3.11 discuss the evaluation of equipment qualification. In reviewing the ESFAS, check that each component or module of the ESFAS has

been qualified for normal, accident, and post-accident environments at its installed location. This applies to all normal conditions but only to those accident conditions where the component or module provides a protective function.

5. Section 4.5 - This requirement is similar to Section 4.4 discussed above. No credit should be given for "safe" failure modes in meeting this requirement. For example, if the most probable effect of a given accident is a loss of energy supply to an ESFAS, it does not matter, in meeting this requirement, whether or not the loss of energy causes the ESFAS to perform its protective function. Even though GDC 23 requires that the ESFAS be designed to "fail-safe," acceptance of the ESFAS design should not be based on an accident causing a failure, even if that accident-induced failure accomplishes the protective function.

6. Section 4.6 - The requirement for channel independence applies to all portions of the ESFAS that are designated as redundant channels. Verification of compliance with this requirement and the recommendations of Regulatory Guide 1.75 and IEEE Std 384-1974 concentrates on points of interface between redundant ESFAS components and interfaces between the redundant portions of the ESFAS and non-safety grade systems. For example, switches common to redundant portions of the ESFAS are reviewed for physical independence between redundant switch sections and for the effects on redundant systems caused by a single malpositioned switch. Also reviewed are the functional performances of isolation devices to assure that no failure in non-safety circuits can disable safety functions.

7. Section 4.7 - The interaction of control systems and the ESFAS involves more than examining the electrical interconnection of control systems with the ESFAS. The functional performance of appropriate control systems must also be reviewed to determine whether their effect on plant conditions can indirectly affect the performance of the ESFAS or the ESF. For example, if a cooling water system is used to supply both safety and non-safety equipment, the controls for the cooling water system must be examined to determine whether failure could lead to insufficient cooling water being supplied to the ESF or the ESFAS during an accident. (Also see Branch Technical Position (BTP) EICSB 27.)

   Note that if failure of a system serving both safety and non-safety systems can lead to a condition requiring action by the safety system, then in addition to the failure creating the need for safety action, the ESFAS must be designed to withstand any other simultaneous single failure.

8. Section 4.8 - This requirement is self-explanatory. In addition, it must be verified that the measured variable is the variable that is used in the accident analyses.

9. Section 4.9 - The most common method used to verify the availability of the ESFAS input sensors is by cross checking between redundant channels that have readout available. When only two channels of readout are provided, evaluate the applicant's analysis of the effect of the operator choosing the incorrect readout as a basis for this action.

   Where non-indicating sensors are used, check the test procedure to see whether a bypass indication is provided when the sensor is disconnected from the process system.

10. Section 4.10 - The extent of test and calibration capability that is provided bears heavily on whether the design meets the single failure criterion.

    a. Any failure that is not detectable must be considered concurrently with any postulated, detectable, single failure.

    b. Periodic testing should duplicate, as closely as practical, the integrated performance required from the ESFAS, ESF systems, and their essential auxiliary supporting systems. If such a "system level" test can be performed only during shutdown, the testing done during power operation must be reviewed in detail. Check that "overlapping" tests do, in fact, overlap from one test segment to another. For example, closing a circuit breaker with the manual breaker control switch may not be adequate to test the ability of the ESFAS to close the breaker.

    c. Test frequencies are acceptable if identical to frequencies recently approved on other identical plants. Any changes made in design or test procedure are not an adequate basis for reducing test frequencies until after experience is gained and the results submitted for review.

    d. Test procedures that require disconnecting wires, installing jumpers, or other similar modifications of the installed equipment are not acceptable test procedures for use during power operation. Check that periodic tests conducted during power operation use only permanently installed test equipment. See also Regulatory Guide 1.22 and BTP EICSB 22, 24, and 25.

11. Section 4.11 - Verify that tests can be conducted without initiating a protective action at the system level, and that tests can be conducted without preventing the initiation of a protective action at the system level. In general, it is an operational rather than a safety problem if testing causes the initiation of a protective action. For those parts of the ESFAS with a degree of redundancy greater than one, testing should not require bypass of the channel level protective action. For one-out-of-two systems, one channel may be bypassed only if initiation of the protective action would disrupt plant operation and the other channel remains operable. In these cases, verify that an interlock is provided that prevents, even with a single failure in the interlock circuits, bypassing both channels and that the single bypass is indicated. See also Regulatory Guide 1.22 and BTP EICSB 24.

12. Section 4.12 - The requirement for automatic removal of operational bypasses means that the reactor operator shall have no role in such removal. The operator may be required to take action to prevent the unnecessary initiation of a protective action and this is acceptable. In no circumstances should a design be approved where action or inaction of the reactor operator is required to make available the protective actions needed in any operational or shutdown mode of the plant.

13. Section 4.13 - See Reg. Guide 1.47 and BTP EICSB 21 for an explanation of this requirement as it pertains to the ESFAS, ESF systems, and auxiliary supporting systems.

14. Section 4.14 - In practice, administrative control is used as the basis for assuring that access to the means for bypassing is limited to qualified plant personnel and that permission of the control room operator is obtained to gain access.

15. Section 4.15 - This requirement is similar to Section 4.12. The phrase "positive means" can be interpreted as either automatic or manual. In the case of manual means, the design must be such that no action or inaction on the part of the reactor operator will prevent the more restrictive set point from being available. It is acceptable for the design to be such that incorrect action or inaction by the operator will cause an unnecessary protective action or prevent placing the plant in an operating mode for which there is inadequate protection (as defined by the accident analyses). See BTP EICSB 12 for specific guidance on set point changes required with a reactor coolant pump out of service.

16. Section 4.16 - For the ESFAS, "completion of a protective action" must be defined by the applicant for each ESF system. This information should be supplied as part of the design basis information required by Section 3.0 of IEEE Std 279-1971.

    Generally, completion consists of starting or energizing the components in the ESF system. Verify that once initiated, the protective action will continue until terminated by deliberate actions of the operator and that operator action cannot prevent the initiation of the protective action when the ESFAS determines the need for that action. Exception: "pull-to-lock" control switches have been acceptable even though their manipulation could prevent the protective action from going to completion.

17. Section 4.17 - Regulatory Guide 1.62 describes an acceptable method of implementing the requirement for manual initiation of protective actions. For those designs that take no credit (in the accident analysis) for manual initiation of protective actions, conformance with Regulatory Guide 1.62 is an adequate basis for acceptance.

    For those protective actions which are initiated solely by manual means, there are no specific criteria to judge acceptance at present. In practice, the requirements of IEEE Std 279 are applied to all equipment used by the operator to detect the need for the protective action, to accomplish the protection action, and to confirm completion of the protective actions. However, it first should be established that automatic initiation need not or cannot be provided. Cost is not sufficient justification for the lack of automatic initiation. In judging the adequacy of any manual initiation features, the other tasks that the operator may be required to perform should be determined and then a judgment made as to whether it is reasonable to rely on the operator to perform all necessary actions. In most situations, automatic actuation, backed up by provisions for manual initiation or manual termination, is more reliable than manual initiation alone, no matter how much time is available to take the protective action.

18. Section 4.18 - See procedure above for Section 4.14.

19. Sections 4.19 and 4.20 - Other than the requirements for indication and identification of channel and system level protective actions, there are no specific implementation guidelines

by which to judge the adequacy of a design with respect to the requirements for status indication. Evaluate the applicant's discussion of how the ESFAS designs conform to these requirements. Acceptance is based on the reviewers's engineering judgement.

See also SRP 7.5 for a discussion of review procedures for safety-related display instrumentation.

20. Section 4.22 - This requirement is self-explanatory. The preferred identification method is color coding of components, cables, and cabinets. See also Regulatory Guide 1.75.

SRP 7.4