U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

Appendix 8-A BRANCH TECHNICAL POSITIONS (PSB)

The PSB Branch Technical Positions (BTPs) represent guidelines intended to supplement the acceptance criteria established in Commission Regulations, guidelines presented in Regulatory Guides, and recommendations presented in applicable IEEE standards. As technical problems or questions of interpretation arise in the detailed reviews of plant designs, the staff must determine an acceptable resolution for each such case to complete its review of a particular application. Where the same technical problem or question of interpretation arises in several cases, the staff's determination on the point at issue is formalized in a BTP. The BTP is primarily an instruction to staff reviewers that outlines an acceptable approach to the particular issue and ensures a uniform treatment of the issue by staff reviewers. The approaches taken in the BTPs, like the approaches taken in regulatory guides, are not mandatory, but do provide defined, acceptable, and immediate solutions to some of the technical problems and questions of interpretation that arise in the review process. In some instances, regulatory guides may be developed from BTPs after sufficient experience in their use has accumulated. All PSB BTPs applicable to Chapter 8 of the Standard Review Plan have been included in this appendix for convenience. They are listed below:

BTP ICSB (PSB)*	Branch Technical Positions of the PSB
2	*Diesel-Generator Reliability Qualification Testing* (Deleted)
4	Requirements on Motor-Operated Valves in the ECCS Accumulator Lines
8	Use of Diesel-Generator Sets for Peaking
11	Stability of Offsite Power Systems
15	Reactor Coolant Pump Breaker Qualification (Deleted)
17	Diesel-Generator Protective Trip Circuit Bypasses (Deleted)
18	Application of the Single Failure Criterion to Manually-Controlled Electrically-Operated Valves
21	Guidance for Application of Regulatory Guide 1.47

*These BTPs are formerly EICSB BTPs which are now in the area of review responsibility of the Power Systems Branch (PSB). Their EICSB (now ICSB) number has been retained in order to provide continuity and correlation with completed reviews.

Rev. 2 - July 1981

BTP PSB

1 Adequacy of Shutdown Electronic Distribution System Voltages
2 Criteria for Alarms and Indications Associated with Diesel-Generator Unit Bypassed and Inoperable Status

BRANCH TECHNICAL POSITION 2 (PSB)
DIESEL-GENERATOR RELIABILITY QUALIFICATION TESTING
(BTP ICSB-2 (PSB) HAS BEEN SUPERCEEDED BY IEEE-387)

BRANCH TECHNICAL POSITION ICSB-4 (PSB)
REQUIREMENTS ON MOTOR-OPERATED VALVES IN THE ECCS ACCUMULATOR LINES

A. BACKGROUND

For many postulated loss-of-coolant accidents, the performance of the emergency core cooling system (ECCS) in pressurized water reactor plants depends upon proper functioning of the safety injection tanks (also referred to as "accumulators" or "flooding tanks" in some applications). In these plants, a motor-operated isolation valve (MOIV) and two check valves are provided in series between each safety injection tank and the reactor coolant (primary) system.

The MOIVs must be considered to be "operating bypasses" because, when closed, they prevent the safety injection tanks from performing the intended protective function. IEEE Std 279 has a requirement for "operating bypasses" which states that the bypasses of a protective function will be removed automatically whenever permissive conditions are not met. This Branch Technical Position provides specific guidance in meeting the intent of IEEE Std 279 for safety injection tank MOIVs.

It should be noted that BTP ICSB 18 (PSB), "Application of the Single Failure Criterion to Manually-Controlled Electrically-Operated Valves," also applies to these isolation valves and should be used in conjunction with this position.

B. BRANCH TECHNICAL POSITION

The following features should be incorporated in the design of MOIV systems for safety injection tanks to meet the intent of IEEE Std 279:

1. Automatic opening of the valves when either primary coolant system pressure exceeds a preselected value (to be specified in the technical specifications), or a safety injection signal is present. Both primary coolant system pressure and safety injection signals should be provided to the valve operator.

2. Visual indication in the control room of the open or closed status of the valve.

3. An audible and visual alarm, independent of item 2., above, that is actuated by a sensor on the valve when the valve is not in the fully-open position.

4. Utilization of a safety injection signal to remove automatically (override) any bypass feature that may be provided to allow an isolation valve to be closed for short periods of time when the reactor coolant system is at pressure (in accordance with provisions of the technical specifications).

C. REFERENCES

1. Arkansas 1, Unit 1, Safety Evaluation Report, January 23, 1973.

2. IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations."

3. BTP ICSB 18 (PSB), "Application of the Single Failure Criterion to Manually-Controlled Electrically-Operated Valves."

BRANCH TECHNICAL POSITION ICSB-8 (PSB)
USE OF DIESEL-GENERATOR SETS FOR PEAKING

A. BACKGROUND

General Design Criterion 17 requires that provisions be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, loss of the main generator, loss of power from the grid, or loss of standby power supplies. Additionally, IEEE Std 308 requires that the preferred (offsite) and standby power supplies shall not have a common failure mode. Common failure mode is defined as "a mechanism by which a single design basis event can cause redundant equipment to be inoperable." Although IEEE Std 308 does not preclude the use of emergency diesels for nonsafety purposes, the staff concludes that the potential for common failure modes should preclude interconnection of onsite and offsite power sources except for short periods for the purpose of load testing.

Review of the use of emergency diesel-generator sets for peaking service leads to the conclusion that the required frequent interconnection of the preferred and standby power supplies increases the probability of their common failure.

B. BRANCH TECHNICAL POSITION

General Design Criterion 17 and IEEE Std 308 should be interpreted as prohibiting the use of plant emergency power diesel-generator sets for purposes other than that of supplying standby power when needed. In particular, emergency power diesel-generator sets should not be used for peaking service.

C. REFERENCES

IEEE STD 308, "Criteria for Class 1E Systems for Nuclear Power Generating Stations."

BRANCH TECHNICAL POSITION ICSB-11 (PSB)
STABILITY OF OFFSITE POWER SYSTEMS

A. BACKGROUND

The staff has traditionally required each applicant to perform stability studies for the electrical transmission grid which would be used to provide the offsite power sources to the plant. The basic requirement is that loss of the largest operating unit on the grid will not result in loss of grid stability and availability of offsite power to the plant under consideration. In some cases, such as plants on the island of Puerto Rico, the plant is connected to an isolated power system of limited generating capacity. These kinds of isolated power systems are inherently less stable than equivalent systems with supporting grid interties. It is also obvious that limited systems are more vulnerable to natural disasters such as tornadoes or hurricanes.

B. BRANCH TECHNICAL POSITION

1. The staff has concluded, from a review of appropriate reliability data, that power systems with supporting grid interties meet the grid availability criterion with some margin. This conclusion is applicable to the review of most plants located on the U.S. mainland.

2. There is also strong indication that an isolated system large enough to justify inclusion of a nuclear unit will also meet this criterion. However, as a conservative approach, the staff will examine the available generating capacity of a system, including interties if available, to withstand outage of the largest unit. If the available capacity is judged marginal to provide adequate stability of the grid, additional measures should be taken. These may include provisions for additional capability and margin for the onsite power system beyond the normal requirements, or other measures as may be appropriate in a particular case. The additional measures to be taken should be determined on an individual case basis.

C. REFERENCES

None.

BRANCH TECHNICAL POSITION ICSB-15 (PSB)
REACTOR COOLANT PUMP BREAKER QUALIFICATION
(BTP ICSB-15 (PSB) has been Deleted)

BRANCH TECHNICAL POSITION ICSB-17 (PSB)
DIESEL-GENERATOR PROTECTIVE TRIP CIRCUIT BYPASSES

BTP ICSB-17 (PSB) has been Superceeded by
Position 7 of Regulatory Guide 1.9 (Revision 2)

BRANCH TECHNICAL POSITION ICSB 18 (PSB)
APPLICATION OF THE SINGLE FAILURE CRITERION TO MANUALLY-CONTROLLED ELECTRICALLY-OPERATED VALVES

A. BACKGROUND

Where a single failure in an electrical system can result in loss of capability to perform a safety function, the effect on plant safety must be evaluated. This is necessary regardless of whether the loss of safety function is caused by a component failing to perform a requisite mechanical motion, or by a component performing an undesirable mechanical motion.

This position establishes the acceptability of disconnecting power to electrical components of a fluid system as one means of designing against a single failure that might cause an undesirable component action. These provisions are based on the assumption that the component is then equivalent to a similar component that is not designed for electrical operation, e.g., a valve that can be opened or closed only by direct manual operation of the valve. They are also based on the assumption that no single failure can both restore power to the electrical system and cause mechanical motion of the components served by the electrical system. The validity of these assumptions should be verified when applying this position.

B. BRANCH TECHNICAL POSITION

1. Failures in both the "fail to function" sense and the "undesirable function" sense of components in electrical systems including valves and other fluid system components should be considered in designing against a single failure, even though the valve or other fluid system component may not be called upon to function in a given safety operational sequence.

2. Where it is determined that failure of an electrical system component can cause undesired mechanical motion of a valve or other fluid system component and this motion results in loss of the system safety function, it is acceptable, in lieu of design changes that also may be acceptable, to disconnect power to the electric systems of the valve or other fluid system component. The plant technical specifications should include a list of all electrically-operated valves, and the required positions of these valves, to which the requirement for removal of electric power is applied in order to satisfy the single failure criterion.

3. Electrically-operated valves that are classified as "active" valves, i.e., are required to open or close in various safety system operational sequences, but are manually-controlled, should be operated from the main control room. Such valves may not be included among those valves from which power is removed in order to meet the single failure criterion unless: (a) electrical power can be restored to the valves from the main control room, (b) valve operation is not necessary for at least ten minutes following occurrence of the event requiring such operation, and

(c) it is demonstrated that there is reasonable assurance that all necessary operator actions will be performed within the time shown to be adequate by the analysis. The plant technical specifications should include a list of the required positions of manually-controlled, electrically-operated valves and should identify those valves to which the requirement for removal of electric power is applied in order to satisfy the single failure criterion.

4. When the single failure criterion is satisfied by removal of electrical power from valves described in 2. and 3., above, these valves should have redundant position indication in the main control room and the position indication system should, itself, meet the single failure criterion.

5. The phrase "electrically-operated valves" includes both valves operated directly by an electrical device (e.g., a motor-operated valve or a solenoid-operated valve) and those valves operated indirectly by an electrical device (e.g., an air-operated valve whose air supply is controlled by an electrical solenoid valve).

C. REFERENCES

None.

BRANCH TECHNICAL POSITION ICSB-21
GUIDANCE FOR APPLICATION OF REGULATORY GUIDE 1.47

A. BACKGROUND

The guidance of Regulatory Guide 1.47 needs further detailing as to methods of providing an acceptable design for the bypass and inoperable status indicators for engineered safety feature (ESF) systems. The purpose of this Branch Technical Position is to provide supplemental guidance for implementation of the guidance of Regulatory Guide 1.47.

B. BRANCH TECHNICAL POSITION

The design criteria for bypass and inoperable status indication systems for ESF should reflect the importance of providing accurate information for the operator and reducing the possibility for the indicating equipment to affect adversely the monitored safety systems. In developing the design criteria, the following should be considered:

1. The bypass indicators should be arranged to enable the operator to determine the status of each safety system and determine whether continued reactor operation is permissible.

2. When a protective function of a shared system can be bypassed, indication of that bypass condition should be provided in the control room of each affected unit.

3. Means by which the operator can cancel erroneous bypass indications, if provided, should be justified by demonstrating that the postulated cases of erroneous indications cannot be eliminated by another practical design.

4. Unless the indication system is designed in conformance with criteria established for safety systems, it should not be used to perform functions that are essential to safety. Administrative procedures should not require immediate operator action based solely on the bypass indications.

5. The indication system should be designed and installed in a manner which precludes the possibility of adverse effects on plant safety systems. Failure or bypass of a protective function should not be a credible consequence of failures occurring in the indication equipment, and the bypass indication should not reduce the required independence between redundant safety systems.

6. The indication system should include a capability of assuring its operable status during normal plant operation to the extent that the indicating and annunciating function can be verified.

C. REFERENCES

1. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

BRANCH TECHNICAL POSITION PSB-1

ADEQUACY OF STATION ELECTRIC DISTRIBUTION SYSTEM VOLTAGES

A. BACKGROUND

Events at the Millstone station have shown that adverse effects on the Class 1E loads can be caused by sustained low grid voltage conditions when the Class 1E buses are connected to offsite power. These low voltage conditions will not be detected by the loss of voltage relays (loss of offsite power) whose low voltage pickup setting is generally in the range of .7 per unit voltage or less.

The above events also determined that imporper voltage protection logic can itself cause adverse effects on the Class 1E systems and equipment such as spurious load shedding of Class 1E loads from the standby diesel generators and spurious separation of Class 1E systems from offsite power due to normal motor starting transients.

A more recent event at Arkansas Nuclear One (ANO) station and the subsequent analysis performed disclosed the possibility of degraded voltage conditions existing on the Class 1E buses even with normal grid voltages, due to deficiencies in equipment between the grid and the Class 1E buses or by the starting transients experienced during certain accident events not originally considered in the sizing of these circuits.

B. BRANCH TECHNICAL POSITION

1. In addition to the undervoltage scheme provided to detect loss of offsite power at the Class 1E buses, a second level of undervoltage protection with time delay should also be provided to protect the Class 1E equipment; this second level of undervoltage protection shall satisfy the following criteria:

   a) The selection of undervoltage and time delay setpoints shall be determined from an analysis of the voltage requirements of the Class 1E loads at all onsite system distribution levels;

   b) Two separate time delays shall be selected for the second level of undervoltage protection based on the following conditions:

      1) The first time delay should be of a duration that established the existance of a sustained degraded voltage condition (i.e., something longer than a motor starting transient). Following this delay, an alarm in the control room should alert the operator to the degraded condition. The subsequent occurrence of a safety injection actuation signal (SIAS) should immediately separate the Class 1E distribution system from the offsite power system.

      2) The second time delay should be of a limited duration such that the permanently connected Class 1E loads will not be damaged. Following this delay, if the operator has failed to restore

adequate voltages, the Class 1E distribution system should be automatically separated from the offsite power system. Bases and justification must be provided in support of the actual delay chosen.

c) The voltage sensors shall be designed to satisfy the following applicable requirements derived from IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations":

1) Class 1E equipment shall be utilized and shall be physically located at and electrically connected to the Class 1E switchgear.

2) An independent scheme shall be provided for each division of the Class 1E power system.

3) The undervoltage protection shall include coincidence logic on a per bus basis to preclude spurious trips of the offsite power source;

4) The voltage sensors shall automatically initiate the disconnection of offsite power sources whenever the voltage set point and time delay limits (cited in item 1.b.2 above) have been exceeded;

5) Capability for test and calibration during power operation shall be provided.

6) Annunciation must be provided in the control room for any bypasses incorporated in the design.

d) The Technical Specifications shall include limiting conditions for operations, surveillance requirements, trip setpoints with minimum and maximum limits, and allowable values for the second-level voltage protection sensors and associated time delay devices.

2. The Class 1E bus load shedding scheme should automatically prevent shedding during sequencing of the emergency loads to the bus. The load shedding feature should, however, be reinstated upon completion of the load sequencing action. The technical specifications must include a test requirement to demonstrate the operability of the automatic bypass and reinstatement features at least once per 18 months during shutdown.

In the event an adequate basis can be provided for retaining the load shed feature during the above transient conditions, the setpoint value in the Technical Specifications for the first level of undervoltage protection (loss of offsite power) must specify a value having maximum and minimum limits. The basis for the setpoints and limits selected must be documented.

3. The voltage levels at the safety-related buses should be optimized for the maximim and minimum load conditions that are expected throughout the anticipated range of voltage variations of the offsite power sources by appropriate adjustment of the voltage tap settings of the intervening transformers. The tap settings selected should be based on an analysis

of the voltage at the terminals of the Class 1E loads. The analyses performed to determine minimum operating voltages should typically consider maximum unit steady state and transient loads for events such as a unit trip, loss-of-coolant accident, startup or shutdown; with the offsite power supply (grid) at minimum anticipated voltage and only the offsite source being considered available. Maximum voltages should be analyzed with the offsite power supply (grid) at maximum expected voltage concurrent with minimum unit loads (e.g. cold shutdown, refueling). A separate set of the above analyses should be performed for each available connection to the offsite power supply.

4. The analytical techniques and assumptions used in the voltage analyses cited in item 3 above must be verified by actual measurement. The verification and test should be performed prior to initial full-power reactor operation on all sources of offsite power by:

   a) loading the station distribution buses, including all Class 1E buses down to the 120/208 v level, to at least 30%;

   b) recording the existing grid and Class 1E bus voltages and bus loading down to the 120/208 volt level at steady state conditions and during the starting of both a large Class 1E and non-Class 1E motor (not concurrently);

      Note: to minimize the number of instrumented locations, (recorders) during the motor starting transient tests, the bus voltages and loading need only be recorded on that string of buses which previously showed the lowest analyzed voltages from item 3 above.

   c) using the analytical techniques and assumptions of the previous voltage analyses cited in item 3 above, and the measured existing grid voltage and bus loading conditions recorded during conduct of the test, calculate new set of voltages for all the Class 1E buses down to the 120/208 volt level;

   d) compare the analytically derived voltage values against the test results.

   With good correlation between the analytical results and the test results, the test verification requirement will be met. That is, the validity of the mathematical model used in performance of the analyses of item 3 will have been established; therefore, the validity of the results of the analyses is also established. In general the test results should not be more than 3% lower than the analytical results; however, the difference between the two when subtracted from the voltage levels determined in the original analyses should never be less than the Class 1E equipment rated voltages.

C. REFERENCES

1. General Design Criterion 17, "Electric Power Systems."

2. IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Stations."

3. Millstone Unit No. 2, Safety Evaluation Supporting Amendment No. 16 to License No. DPR-65.

4. NRC Summary of Meeting for Arkansas Nuclear One Incident of September 16, 1978, dated February 9, 1979.

Branch Technical Position PSB-2

CRITERIA FOR ALARMS AND INDICATIONS ASSOCIATED WITH DIESEL-GENERATOR UNIT BYPASSED AND INOPERABLE STATUS

1. BACKGROUND

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," describes an acceptable method for complying with the requirements of IEEE 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," with respect to indicating the bypass or inoperable status of portions of the protection system, systems actuated or controlled by the protection system, and auxiliary or supporting systems that must be operable for the protection system and the system it actuates to perform their safety-related functions. This appendix gives more specific guidance on meeting the provisions of Regulatory Guide 1.47 as they pertain to diesel-generator units. Diesel-generator units, as defined in Regulatory Guide 1.108, "Periodic Testing of Diesel Generator Units Used as Onsite Electric Power Systems at Nuclear Power Plants," consist of the engine, generator, combustion air system, cooling water system up to the supply, fuel supply system, lubricating oil system, starting energy sources, autostart controls, manual controls, and diesel-generator breaker.

Operating experience has shown that there have been incidents where diesel-generator units failed to respond to an automatic start signal because control switches or lockout and shutdown relays (which require manual reset) were left in the shutdown condition without control room operators being aware of their status. The principal reasons for this lack of awareness were the (a) sharing of annunciator stations for both disabling and nondisabling alarm conditions; (b) wording on annunciator windows for disabling conditions that did not specifically say a diesel-generator unit was unavailable for an automatic emergency start; and (c) disabling conditions that were not annunciated in the control room.

In order that the operator can act appropriately to supply emergency power when required in the operation of diesel-generator units, it is esential that he has accurate and sufficient information about the status of the units (e.g., is a unit under test; is a unit locked out for repair, maintenance, or otherwise unavailable) on which to base his decisions.

2. BRANCH TECHNICAL POSITION

2.1 Diesel-generator unit bypass or deliberately induced inoperability status should be automatically indicated in the control room where the bypass or deliberately induced inoperable condition can be expected to occur more frequently than once per year and can render the unit unavailable to respond to an automtic or operator-initiated emergency start signal (e.g., nonreset, mode switch position, loss of control voltage, low starting air pressure). Manually induced indication may be desirable and is permitted for diesel-generator unit bypass or deliberately induced inoperability status for those conditions expected to occur less frequently than once per year.

2.2 All status indication should be sufficiently precise to prevent misinterpretation. Further, disabling or bypass indicators should be separate from nondisabling indicators and should be physically arranged to enable the operator to clearly determine the status of each diesel-generator unit. An acceptable design would include a separate alarm for each disabling condition or a single shared alarm with reflash capability. The alarms should be displayed in the control room and at the diesel-generator unit for all disabling conditions, with wording that indicates that the diesel-generator unit is incapable of responding to an automatic start signal.

2.3 When a shared diesel-generator unit can be bypassed, indication of that bypass condition should be provided in the control room of each affected unit.

2.4 The indication system should be designed and installed in a manner that precludes the possibility of adverse effects on the diesel-generator units. Failures in the indication equipment should not result in diesel-generator unit failure or bypass of the diesel-generator unit, and the bypass indication should not reduce the required independence between redundant diesel-generator units.

2.5 The indication system should include a capability of ensuring its operable status during normal plant operation to the extent that the indicating and annunciating function can be verified.

3. REFERENCES

a. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

b. IE Circular 77-16, "Emergency Diesel Generator Electrical Trip Lock-Out Features," December 13, 1977.

c. Branch Technical Position ICSB, "Guidance for Application of Regulatory Guide 1.47," Appendix 8-A to Standard Review Plan Section 8.1, Standard Review Plan Section 7.