NUREG-1432
Vol. 2

Standard Technical Specifications
Combustion Engineering Plants

Bases (Sections 2.0–3.3)

Draft Report for Comment

Issued by the
U.S. Nuclear Regulatory Commission

Office of Nuclear Reactor Regulation

January 1991

NUREG-1432, Vol. 2
Draft

STANDARD TECHNICAL SPECIFICATIONS
COMBUSTION ENGINEERING PLANTS

JANUARY 1991

NUREG-1432
Vol. 2

Standard Technical Specifications
Combustion Engineering Plants

Bases (Sections 2.0-3.3)

Draft Report for Comment

Issued by the
U.S. Nuclear Regulatory Commission

Office of Nuclear Reactor Regulation

January 1991

AVAILABILITY NOTICE

Availability of Reference Materials Cited in NRC Publications

Most documents cited in NRC publications will be available from one of the following sources:

1. The NRC Public Document Room, 2120 L Street, NW, Lower Level, Washington, DC 20555

2. The Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082

3. The National Technical Information Service, Springfield, VA 22161

Although the listing that follows represents the majority of documents cited in NRC publications, it is not intended to be exhaustive.

Referenced documents available for inspection and copying for a fee from the NRC Public Document Room include NRC correspondence and internal NRC memoranda; NRC Office of Inspection and Enforcement bulletins, circulars, information notices, inspection and investigation notices; Licensee Event Reports; vendor reports and correspondence; Commission papers; and applicant and licensee documents and correspondence.

The following documents in the NUREG series are available for purchase from the GPO Sales Program: formal NRC staff and contractor reports, NRC-sponsored conference proceedings, and NRC booklets and brochures. Also available are Regulatory Guides, NRC regulations in the Code of Federal Regulations, and Nuclear Regulatory Commission Issuances.

Documents available from the National Technical Information Service include NUREG series reports and technical reports prepared by other federal agencies and reports prepared by the Atomic Energy Commission, forerunner agency to the Nuclear Regulatory Commission.

Documents available from public and special technical libraries include all open literature items, such as books, journal and periodical articles, and transactions. Federal Register notices, federal and state legislation, and congressional reports can usually be obtained from these libraries.

Documents such as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings are available for purchase from the organization sponsoring the publication cited.

Single copies of NRC draft reports are available free, to the extent of supply, upon written request to the Office of Information Resources Management, Distribution Section, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at the NRC Library, 7920 Norfolk Avenue, Bethesda, Maryland, and are available there for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from the American National Standards Institute, 1430 Broadway, New York, NY 10018.

PREFACE

This DRAFT NUREG presents the results of the Nuclear Regulatory Commission (NRC) staff review of the Combustion Engineering Owners Group (CEOG) proposed new Standard Technical Specifications (STS). These new STS were developed based on the criteria in the interim Commission Policy Statement on Technical Specification Improvements for Nuclear Power Reactors, dated February 6, 1987.

The new STS will be used as bases for developing improved plant-specific technical specifications by individual nuclear power plant owners that have PWRs designed by Combustion Engineering (CE). The NRC staff is issuing this draft new STS for a 30 working-day comment period. Following the comment period, the NRC staff will analyze comments received, finalize the new STS, and issue them for plant-specific implementation.

Comments should be submitted no later than March 15, 1991, in accordance with the following guidance: The exact wording of each proposed change should be marked in pen and ink on copies of all the affected pages of DRAFT NUREG-1432, "Standard Technical Specifications, Combustion Engineering Plants." Each proposed change should be numbered. Each proposed change should be accompanied with a separate technical justification, cross referenced to the applicable proposed change on the marked up pages.

Submit written comments to: David L. Meyer, Chief, Regulatory Publications Branch, Division of Freedom of Information and Publications Services, Office of Administration, U. S. Nuclear Regulatory Commission, Washington, DC 20555. Hand deliver comments to: 7920 Norfolk Avenue, Bethesda, Maryland, between 7:45 a.m. and 4:15 p.m. on Federal workdays.

(continued)

B 2.0 SAFETY LIMITS

B 2.1.1 Reactor Core Safety Limits (SLs) (Analog)

BASES

BACKGROUND

GDC 10 (Ref. 1) requires that specified acceptable fuel design limits are not exceeded during steady-state operation, normal operation transients, or anticipated operational occurrences (AOOs). This is accomplished with a departure from nucleate boiling (DNB) design basis, which corresponds to a 95% probability at a 95% confidence level that DNB will not occur and by requiring that fuel-centerline temperature stays below the melting temperature.

The restrictions of this SL prevent overheating of the fuel and cladding and possible cladding perforation, that would result in the release of fission products to the reactor coolant. Overheating of the fuel is prevented by maintaining the steady-state peak linear heat rate (LHR) below the level at which centerline fuel melting occurs. Overheating of the fuel cladding is prevented by restricting fuel operation to within the nucleate boiling regime, where the heat-transfer coefficient is large and the cladding-surface temperature is slightly above the coolant-saturation temperature.

Centerline fuel melting occurs when the local LHR or power peaking, in a region of the fuel is high enough to cause the fuel-centerline temperature to reach the melting point of the fuel. Expansion of the pellet upon centerline melting may cause the pellet to stress the cladding to the point of failure, allowing an uncontrolled release of activity to the reactor coolant.

Operation above the boundary of the nucleate boiling regime could result in excessive cladding temperature because of the onset of DNB and the resultant sharp reduction in heat-transfer coefficient. Inside the steam film, high-cladding temperatures are reached and a cladding-water (zirconium-water) reaction may take place. This chemical reaction results in oxidation of the fuel cladding to a structurally weaker form. This weaker form may also lose its integrity, resulting in an uncontrolled release of activity to the reactor coolant.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The proper functioning of the Reactor Protection System (RPS) and steam generator (SG) safety valves prevents violation of the reactor core SLs.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation and AOOs. The reactor core SLs are established to preclude violation of the following fuel design criteria:

a. There must be at least 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB (this is referred to hereafter as the 95/95 DNB criterion); and

b. The hot fuel pellet in the core must not experience centerline fuel melting.

The RPS setpoints (Ref. 2), in combination with all the LCOs, is designed to prevent any anticipated combination of transient conditions for Reactor Coolant System (RCS) temperature, pressure, and THERMAL POWER level that would result in a DNB of less than the DNB limit and preclude the existence of flow instabilities.

Automatic enforcement of these reactor core SLs is provided by the trip setpoints for the following functions:

a. High pressurizer-pressure reactor trip;

b. Variable high-power reactor trip;

c. Power rate of change—high reactor trip;

d. Reactor coolant flow—low reactor trip;

e. SG safety valves;

f. SG pressure—low reactor trip;

g. SG water level—low reactor trip; and

h. Axial power distribution—high reactor trip.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The limitation that the average enthalpy in the hot leg be less than or equal to the enthalpy of saturated liquid also ensures that the ΔT measured by instrumentation, (used in the RCS design as a measure of the core power) is proportional to core power.

The SL represents a design requirement for establishing the RPS trip setpoints identified previously. LCO 3.2.1, "Linear Heat Rate (LHR)," and LCO 3.2.5, Axial Shape Index, or the assumed initial conditions of the safety analyses (as indicated in the FSAR, Ref. 2) provide more restrictive limits to ensure that the SLs are not exceeded.

SAFETY LIMITS

The curves provided in Figure 2.1.1-1 shows the loci of points of THERMAL POWER, pressurizer pressure, and highest operating loop cold leg temperature, for which the minimum departure from nucleate boiling ratio (DNBR) is not less than the safety analysis limit, and that fuel centerline temperature remains below melting, or that the average enthalpy in the hot leg is less than or equal to the enthalpy of saturated liquid, or the exit quality is within the limits defined by the DNBR correlation.

APPLICABILITY

SL 2.1.1 only applies in MODES 1 and 2 because these are the only modes in which the reactor is critical. Automatic protection functions are required to be OPERABLE during MODES 1 and 2 to ensure operation within the reactor core SLs. The SG safety valves or automatic protection actions serve to prevent RCS heatup to the reactor core SL conditions or to initiate a reactor trip function (which forces the unit into MODE 3). Setpoints for the reactor trip functions are specified in LCO 3.3.1 and LCO 3.3.2.

In MODES 3, 4, 5, and 6, Applicability is not required, since the reactor is not generating significant THERMAL POWER.

(continued)

(continued)

BASES (continued)

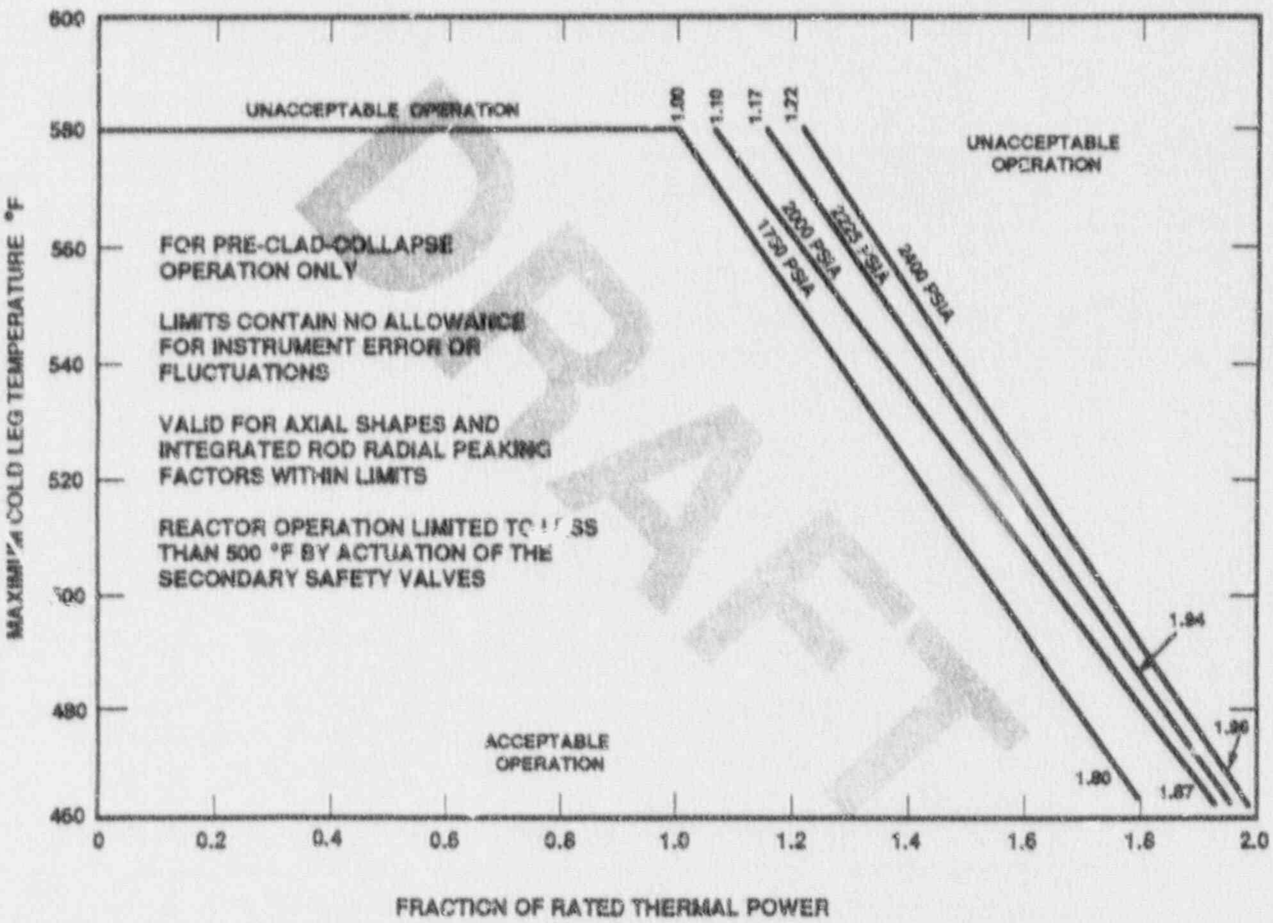

Figure 2.1.1-1
Reactor Core Thermal Margin Safety Limit

BASES (continued)

SAFETY LIMIT VIOLATIONS

2.2.1

If SL 2.1.1 is violated, the requirement to go to MODE 3 places the plant in a MODE in which this SL is not applicable.

The allowed Completion Time of 1 hour recognizes the importance of bringing the plant to a mode of operation where this SL is not applicable. Also, the Completion Time of 1 hour ensures that the probability of an accident occurring during this period is minimal.

2.2.3

If SL 2.1.1 is violated, the NRC Operations Center must be notified within 1 hour. This is in accordance with 10 CFR 50.72 (Ref. 3).

2.2.4

If SL 2.1.1 is violated, the appropriate senior management of the nuclear plant and the utility shall be notified within 24 hours. This 24-hour period provides time for the plant operators and staff to take the appropriate immediate action and assess the condition of the plant before reporting to the senior management.

2.2.5

If SL 2.1.1 is violated, a Licensee Event Report shall be prepared and submitted within 30 days to the NRC, the senior management of the nuclear plant, and the utility Vice-President—Nuclear Operations. This requirement is in accordance with 10 CFR 50.73 (Ref. 4).

2.2.6

If SL 2.1.1 is violated, restart of the unit shall not commence until authorized by the NRC. This requirement ensures the NRC that all necessary reviews, analyses, and actions are completed before the unit begins its restart to normal operation.

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," 1988.

2. [Unit Name] FSAR, Section [ ], "[Title]."

3. Title 10, Code of Federal Regulations, Part 50.72, "Immediate Notification Requirements for Operating Nuclear Power Reactors."

4. Title 10, Code of Federal Regulations, Part 50.73, "Licensee Event Report System."

B 2.0 SAFETY LIMITS

B 2.1.2 Reactor Coolant System (RCS) Pressure Safety Limit (SL) (Analog)

BASES

BACKGROUND

The SL on RCS pressure protects the integrity of the RCS against overpressurization. In the event of fuel-cladding failure, fission products are released into the reactor coolant. The RCS then serves as the primary barrier in preventing the release of fission products into the atmosphere. By establishing an upper limit on RCS pressure, continued RCS integrity is ensured. According to 10 CFR 50, Appendix A, GDC 14, "Reactor Coolant Pressure Boundary," and GDC 15, "Reactor Coolant System Design" (Ref. 1), the reactor coolant pressure boundary (RCPB) design conditions are not exceeded during normal operation and anticipated operational occurrences (AOOs). Also, according to GDC 28 (Ref. 1), "Reactivity Limits," reactivity accidents including rod ejection, do not result in damage to the RCPB greater than limited local yielding.

The design pressure of the RCS is 2500 psia. During normal operation and AOOs, the RCS pressure is kept from exceeding the design pressure by more than 10%, in accordance with Section III of the American Society of Mechanical Engineers (ASME) Code (Ref. 2). As an assurance of system integrity, all RCS components are hydrostatically tested at 125% of design as specified in the ASME Code requirements prior to initial operation, when there is no fuel in the core. If repairs or replacements that would require a full hydrostatic test of the RCS are necessary, the fuel must be completely offloaded before the RCS exceeds the maximum pressure specified in this SL. Removing fuel from the vessel precludes fission products from entering the reactor coolant.

Overpressurization of the RCS could result in a breach of the RCPB. If this occurs in conjunction with a fuel-cladding failure, fission products could enter the containment atmosphere, raising concerns relative to limits on radioactive releases specified in 10 CFR 100, "Reactor Site Criteria."

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The RCS pressurizer safety valves, the main steam safety valves (MSSVs), and the reactor high-pressure trip have settings established to ensure that the RCS pressure SL will not be exceeded.

The RCS pressurizer safety valves are sized to prevent system pressure from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code for Nuclear Power Plant Components (Ref. 2). The transient that establishes the required relief capacity, and hence the valve-size requirements and lift settings, is a [complete loss of external load without a direct reactor trip.] During the transient, no control actions are assumed except that the safety valves on the secondary plant are assumed to open when the steam pressure reaches the secondary plant safety valve settings and nominal feedwater supply is maintained.

The Reactor Protection System (RPS) trip setpoints (Ref. 3), together with the settings of the MSSVs (Ref. 4), provide pressure protection for normal operation and AOOs. In particular, the reactor high-pressure trip setpoint is specifically set to provide protection against overpressurization (Ref. 5). Safety analyses for both the high-pressure trip and the RCS pressurizer safety valves are performed using conservative assumptions relative to pressure-control devices.

More specifically, no credit is taken for operation of the following:

a. Pressurizer power-operated relief valves (PORVs);

b. Steam line relief valve;

c. Steam Dump System;

d. RCS;

e. Pressurizer Level Control System; or

f. Pressurizer spray valve.

(continued)

BASES (continued)

SAFETY LIMITS

The maximum transient pressure allowable in the RCS pressure vessel under the ASME Code, Section III, is 110% of design pressure. The maximum transient pressure allowable in the RCS piping, valves, and fittings under [USAS, Section B31.1, Ref. 6] is 120% of design pressure. The most limiting of those two allowances is the 110% of design pressure; therefore, the SL on maximum allowable RCS pressure is established at 2735 psig.

APPLICABILITY

SL 2.1.2 applies in MODES 1 through 5 because it is conceivable to approach or exceed this SL in these MODES due to overpressurization events. The SL is not applicable in MODE 6 because the reactor vessel head closure bolts are not fully tightened, making it impossible to pressurize the RCS.

SAFETY LIMIT VIOLATIONS

2.2.2.1

If the RCS pressure SL is violated when the reactor is in MODE 1 or 2, the requirement is to restore compliance within 15 minutes and be in MODE 3 within 1 hour.

If the RCS pressure SL is violated in MODE 1 or 2, the reactor vessel temperature would be well above the transition temperature at which reactor vessel metal goes from being ductile to being nonductile. Given that the reactor vessel metal is ductile, a pressure increase above 100% of design pressure does not challenge RCS integrity as much as it would if the reactor vessel were in a non-ductile state; therefore, 15 minutes to restore pressure implies immediacy.

The allowed Completion Time of 1 hour recognizes the importance of reducing power level to a mode of operation where the potential for challenges to safety systems is minimized.

2.2.2.2

If the RCS pressure SL is exceeded in MODE 3, 4, or 5, RCS pressure must be restored to within the SL value within 5 minutes.

(continued)

(continued)

BASES (continued)

SAFETY LIMIT VIOLATIONS (continued)

Exceeding the RCS pressure SL in MODE 3, 4, or 5 is more severe than exceeding this SL in MODE 1 or 2, since the reactor vessel temperature may be lower and the vessel material consequently less ductile. As such, pressure must be reduced to less than the SL within 5 minutes. This action does not require reducing MODES, since this would require reducing temperature, which would compound the problem by adding thermal gradient stresses to the existing pressure stress.

2.2.3

If the RCS pressure SL is violated, the NRC Operations Center must be notified within 1 hour. This is in accordance with 10 CFR 50.72 (Ref. 7).

2.2.4

If the RCS pressure SL is violated, the appropriate senior management of the nuclear plant and the utility shall be notified within 24 hours. This 24-hour period provides time for the plant operators and staff to take the appropriate immediate action and to assess the condition of the plant before reporting to the senior management.

2.2.5

If the RCS pressure SL is violated, a Licensee Event Report shall be prepared and submitted within 30 days to the NRC, the senior management of the nuclear plant, and the utility Vice-President—Nuclear Operations. This requirement is in accordance with 10 CFR 50.73 (Ref. 8).

2.2.6

If the RCS pressure SL is violated, restart of the unit shall not commence until authorized by the NRC. This requirement ensures the NRC that all necessary reviews, analyses, and actions are completed before the unit begins its restart to normal operation.

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 14, "Reactor Coolant Pressure Boundary"; General Design Criterion 15, "Reactor Coolant System Design"; and General Design Criterion 28, "Reactivity Limits."

2. American Society of Mechanical Engineers Boiler and Pressure Vessel Code, Section III, "Nuclear Power Plant Components," Article NB-7000, "Protection Against Overpressure."

3. [Unit Name] FSAR, Section [ ], "[Title]."

4. [Unit Name] FSAR, Section [ ], "[Title]."

5. [Unit Name] FSAR, Section [ ], "[Title]."

6. USAS B31.1, Standard Code for Pressure Piping, American Society of Mechanical Engineers, 1967.

7. Title 10, Code of Federal Regulations, Part 50.72, "Immediate Notification Requirements for Operating Nuclear Power Reactors."

8. Title 10, Code of Federal Regulations, Part 50.73, "Licensee Event Report System."

B 2.0 SAFETY LIMITS

B 2.1.1 Reactor Core Safety Limits (SLs) (Digital)

BASES

BACKGROUND

GDC 10 (Ref. 1) requires that specified acceptable fuel design limits are not exceeded during steady-state operation, normal operational transients, and anticipated operational occurrences (AOOs). This is accomplished with a departure from nucleate boiling (DNB) design basis that corresponds to a 95% probability at a 95% confidence level that DNB will not occur and by requiring that fuel-centerline temperature stays below the melting temperature.

The restrictions of this SL prevent overheating of the fuel and cladding and possible cladding perforation, that would result in the release of fission products to the reactor coolant. Overheating of the fuel is prevented by maintaining the steady-state, peak linear heat rate (LHR) below the level at which centerline fuel melting occurs. Overheating of the fuel cladding is prevented by restricting fuel operation to within the nucleate boiling regime where the heat-transfer coefficient is large and the cladding-surface temperature is slightly above the coolant-saturation temperature.

Centerline fuel melting occurs when the local LHR, or power peaking, in a region of the fuel is high enough to cause the fuel-centerline temperature to reach the melting point of the fuel. Expansion of the pellet upon centerline melting may cause the pellet to stress the cladding to the point of failure, allowing an uncontrolled release of activity to the reactor coolant.

Operation above the boundary of the nucleate boiling regime could result in excessive cladding temperature because of the onset of DNB and the resultant sharp reduction in the heat-transfer coefficient. Inside the steam film, high-cladding temperatures are reached and a cladding-water (zirconium-water) reaction may take place. This chemical reaction results in oxidation of the fuel cladding to a structurally weaker form. This weaker form may lose its integrity, resulting in an uncontrolled release of activity to the reactor coolant.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The proper functioning of the Reactor Protection System (RPS) and steam generator (SG) safety valves prevents violation of the reactor core SLs.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation and AOOs. The reactor core SLs are established to preclude violation of the following fuel design criteria:

a. There must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience DNB (this is referred to hereafter as the 95/95 DNB criterion); and

b. The hot fuel pellet in the core must not experience centerline fuel melting.

The RPS setpoints, in combination with all LCOs, are designed to prevent any anticipated combination of transient conditions for Reactor Coolant System (RCS) temperature, pressure, and THERMAL POWER level that would result in a departure from nuclear boiling ratio (DNBR) of less than the DNBR limit and preclude the existence of flow instabilities.

Automatic enforcement of these reactor core SLs is provided by trip setpoints for the following functions:

a. High pressurizer pressure reactor trip;

b. Low pressurizer pressure reactor trip;

c. Linear power level—high reactor trip;

d. SG pressure—low reactor trip;

e. Core protection calculators reactor trip;

f. SG safety valves;

g. SG level—low reactor trip;

h. SG level—high reactor trip;

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

i. Reactor coolant flow—low reactor trip; and

j. Control element assembly calculators reactor trip.

The limitation that the average enthalpy in the hot leg be less than or equal to the enthalpy of saturated liquid also ensures that the ΔT measured by instrumentation (used in the protection system design as a measure of the core power) is proportional to core power.

The SL represents a design requirement for establishing the protection system trip setpoints identified previously. LCO 3.2.1, "Linear Heat Rate (LHR)," and LCO 3.2.4, "Departure from Nucleate Boiling Ratio (DNBR)," or the assumed initial conditions of the safety analyses (as indicated in the FSAR, Ref. 2), provide more restrictive limits to ensure that the SLs are not exceeded.

SAFETY LIMITS

SL 2.1.1.1 and SL 2.1.1.2 ensure that the minimum DNBR is not less than the safety analyses limit and that fuel centerline temperature remains below melting, or that the average enthalpy in the hot leg is less than or equal to the enthalpy of saturated liquid, or that the exit quality is within the limits defined by the DNBR correlation.

The minimum value of the DNBR during normal operation and design basis AOOs is limited to [1.19] based on a statistical combination of CE-1 CHF correlation and engineering factor uncertainties and is established as an SL. Additional factors such as rod bow and spacer grid size and placement will determine the limiting safety system settings (LSSS) required to ensure that the SL is maintained. Maintaining the dynamically adjusted peak LHR to ≤ 21 kW/ft ensures that fuel-centerline melt will not occur during normal operating conditions or design AOOs.

APPLICABILITY

SL 2.1.1.1 and SL 2.1.1.2 only apply in MODES 1 and 2 because these are the only MODES in which the reactor is critical. Automatic protection functions are required to be OPERABLE during MODES 1 and 2 to ensure operation within the reactor core SLs. The SG safety valves or automatic

(continued)

(continued)

DRAFT

BASES (continued)

APPLICABILITY (continued)

protection actions serve to prevent RCS heatup to the reactor core SL conditions or to initiate a reactor trip function (which forces the unit into MODE 3). Setpoints for the reactor trip functions are specified in LCO 3.3.1 and LCO 3.3.2.

In MODES 3, 4, 5, and 6, Applicability is not required, since the reactor is not generating significant THERMAL POWER.

SAFETY LIMIT VIOLATIONS

2.2.1

If SL 2.1.1.1 or SL 2.1.1.2 is violated, the requirement to go to MODE 3 places the plant in a MODE in which this SL is not applicable.

The allowed Completion Time of 1 hour recognizes the importance of bringing the plant to a MODE where this SL is not applicable. Also, the Completion Time of 1 hour ensures that the time period of operation outside of the safety analyses is minimal.

2.2.3

If SL 2.1.1.1 or SL 2.1.1.2 is violated, the NRC Operations Center must be notified within 1 hour. This is in accordance with 10 CFR 50.72 (Ref. 3).

2.2.4

If SL 2.1.1.1 or SL 2.1.1.2 is violated, the appropriate senior management of the nuclear plant and the utility shall be notified within 24 hours. This 24-hour period provides time for the plant operators and staff to take the appropriate immediate action and assess the condition of the plant before reporting to the senior management.

2.2.5

If SL 2.1.1.1 or SL 2.1.1.2 is violated, a Licensee Event Report shall be prepared and submitted within 30 days to the NRC, the senior management of the nuclear plant, and the

(continued)

(continued)

BASES (continued)

SAFETY LIMIT VIOLATIONS (continued)

utility Vice-President—Nuclear Operations. This requirement is in accordance with 10 CFR 50.73 (Ref. 4).

2.2.6

If SL 2.1.1.1 or SL 2.1.1.2 is violated, restart of the unit shall not commence until authorized by the NRC. This requirement ensures the NRC that all necessary reviews, analyses, and actions are completed before the unit begins its restart to normal operation.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," 1988.
2. [Unit Name] FSAR, Section [ ], "[Title]."
3. Title 10, Code of Federal Regulations, Part 50.72, "Immediate Notification Requirements for Operating Nuclear Power Reactors."
4. Title 10, Code of Federal Regulations, Part 50.73, "Licensee Event Report System."

B 2.0 SAFETY LIMITS

B 2.1.2 Reactor Coolant System (RCS) Pressure Safety Limit (SL) (Digital)

BASES

BACKGROUND

The SL on RCS pressure protects the integrity of the RCS against overpressurization. In the event of fuel-cladding failure, fission products are released into the reactor coolant. The RCS then serves as the primary barrier in preventing the release of fission products into the atmosphere. By establishing an upper limit on RCS pressure, continued RCS integrity is ensured. According to 10 CFR 50, Appendix A, GDC 14, "Reactor Coolant Pressure Boundary," and GDC 15, "Reactor Coolant System Design" (Ref. 1), the reactor coolant pressure boundary (RCPB) design conditions are not exceeded during normal operation and anticipated operational occurrences (AOOs). Also, according to GDC 28 (Ref. 1), "Reactivity Limits," reactivity accidents including rod ejection, do not result in damage to the RCPB greater than limited local yielding.

The design pressure of the RCS is 2500 psia. During normal operation and AOOs, the RCS pressure is kept from exceeding the design pressure by more than 10%, in accordance with Section III of the American Society of Mechanical Engineers (ASME) Code (Ref. 2). As an assurance of system integrity, all RCS components are hydrostatically tested at 125% of design pressure as specified in the ASME Code requirements prior to initial operation, when there is no fuel in the core. If repairs or replacements that would require a full hydrostatic test of the RCS are necessary, the fuel must be completely offloaded before the RCS exceeds the maximum pressure specified in this SL. Removing fuel from the vessel precludes fission products from entering the reactor coolant.

Overpressurization of the RCS could result in a breach of the RCPB. If this occurs in conjunction with a fuel-cladding failure, fission products could enter the containment atmosphere, raising concerns relative to limits on radioactive releases specified in 10 CFR 100, "Reactor Site Criteria."

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The RCS pressurizer safety valves, the main steam safety valves (MSSVs), and the reactor high-pressure trip have settings established to ensure that the RCS pressure SL will not be exceeded.

The RCS pressurizer safety valves are sized to prevent system pressure from exceeding the design pressure by more than 10%, in accordance with Section III of the ASME Code for Nuclear Power Plant Components (Ref. 2). The transient that establishes the required relief capacity, and hence the valve-size requirements and lift settings, is a [complete loss of external load without a direct reactor trip.] During the transient, no control actions are assumed except that the safety valves on the secondary plant are assumed to open when the steam pressure reaches the secondary plant safety valve settings and nominal feedwater supply is maintained.

The Reactor Protection System (RPS) trip setpoints (Ref. 3), together with the settings of the MSSVs (Ref. 4), provide pressure protection for normal operation and AOOs. In particular, the reactor high-pressure trip setpoint is specifically set to provide protection against overpressurization (Ref. 5). Safety analyses for both the high-pressure trip and the RCS pressurizer safety valves are performed using conservative assumptions relative to pressure-control devices.

More specifically, no credit is taken for operation of the following:

a. Pressurizer power-operated relief valves (PORVs);

b. Steam line relief valve;

c. Steam Dump System;

d. Reactor Control System;

e. Pressurizer Level Control System; or

f. Pressurizer spray valve.

(continued)

BASES (continued)

SAFETY LIMITS

The maximum transient pressure allowable in the RCS pressure vessel under the ASME Code, Section III, is 110% of design pressure. The maximum transient pressure allowable in the RCS piping, valves, and fittings under [USAS, Section B31.1, Ref. 6] is 120% of design pressure. The most limiting of these two allowances is the 110% of design pressure; therefore, the SL on maximum allowable RCS pressure is established at 2735 psig.

APPLICABILITY

SL 2.1.2 applies in MODES 1 through 5 because it is conceivable to approach or exceed this SL in these modes due to overpressurization events. The SL is not applicable in MODE 6 because the reactor vessel head closure bolts are not fully tightened, making it impossible to pressurize the RCS.

SAFETY LIMIT VIOLATIONS

2.2.2.1

If the RCS pressure SL is violated when the reactor is in MODE 1 or 2, the requirement is to restore compliance within 15 minutes and be in MODE 3 within 1 hour.

If the RCS pressure SL is violated in MODE 1 or 2, the reactor vessel temperature would be well above the transition temperature, at which reactor vessel metal goes from being ductile to being nonductile. Given that the reactor vessel metal is ductile, a pressure increase above 100% of design pressure does not challenge RCS integrity as much as it would if the reactor vessel were in a non-ductile state; therefore, 15 minutes to restore pressure implies immediacy.

The allowed Completion Time of 1 hour recognizes the importance of reducing power level to a mode of operation where the potential for challenges to safety systems is minimized.

2.2.2.2

If the RCS pressure SL is exceeded in MODE 3, 4, or 5, RCS pressure must be restored to within the SL value within 5 minutes.

(continued)

(continued)

BASES (continued)

SAFETY LIMIT VIOLATIONS (continued)

Exceeding the RCS pressure SL in MODE 3, 4, or 5 is more severe than exceeding this SL in MODE 1 or 2, since the reactor vessel temperature may be lower and the vessel material consequently less ductile. As such, pressure must be reduced to less than the SL within 5 minutes. This action does not require reducing MODES, since this would require reducing modes since this would require reducing temperature, which would compound the problem by adding thermal gradient stresses to the existing pressure stress.

2.2.3

If the RCS pressure SL is violated, the NRC Operations Center must be notified within 1 hour. This is in accordance with 10 CFR 50.72 (Ref. 7).

2.2.4

If the RCS pressure SL is violated, the appropriate senior management of the nuclear plant and the utility shall be notified within 24 hours. This 24-hour period provides time for the plant operators and staff to take the appropriate immediate action and to assess the condition of the plant before reporting to the senior management.

2.2.5

If the RCS pressure SL is violated, a Licensee Event Report shall be prepared and submitted within 30 days to the NRC, the senior management of the nuclear plant, and the utility Vice-President—Nuclear Operations. This requirement is in accordance with 10 CFR 50.73 (Ref. 8).

2.2.6

If the RCS pressure SL is violated, restart of the unit shall not commence until authorized by the NRC. This requirement ensures the NRC that all necessary reviews, analyses, and actions are completed before the unit begins its restart to normal operation.

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 14, "Reactor Coolant Pressure Boundary"; General Design Criterion 15, "Reactor Coolant System Design"; and General Design Criterion 28, "Reactivity Limits."

2. American Society of Mechanical Engineers Boiler and Pressure Vessel Code, Section III, "Nuclear Power Plant Components," Article NB-7000, "Protection Against Overpressure."

3. [Unit Name] FSAR, Section [ ], "[Title]."

4. [Unit Name] FSAR, Section [ ], "[Title]."

5. [Unit Name] FSAR, Section [ ], "[Title]."

6. USAS B 31.1, Standard Code for Pressure Piping, American Society of Mechanical Engineers, 1967.

7. Title 10, Code of Federal Regulations, Part 50.72, "Immediate Notification Requirements for Operating Nuclear Power Reactors."

8. Title 10, Code of Federal Regulations, Part 50.73, "Licensee Event Report System."

B 3.0 APPLICABILITY

B 3.0 Limiting Conditions for Operation (LCO) Applicability

BASES

LCO 3.0.1, LCO 3.0.2, LCO 3.0.3, LCO 3.0.4, and LCO 3.0.5	LCO 3.0.1, LCO 3.0.2, LCO 3.0.3, LCO 3.0.4, and LCO 3.0.5 establish the general requirements applicable to all specifications unless otherwise stated. This includes specifications regarding the programs in Section 5.7.4, "Programs and Manuals," as well as LCOs contained in Sections 3.1 through 3.9.
LCO 3.0.1	LCO 3.0.1 establishes the requirement to meet LCOs when the unit is in the MODES or other specified Conditions of the Applicability statement of each specification.
LCO 3.0.2	LCO 3.0.2 establishes that upon discovery of a failure to meet an LCO, the associated ACTIONS shall be met. The Completion Time of each Required Action for an ACTIONS Condition is applicable from the point in time it is discovered that an inoperable situation exists (i.e., that the LCO is not met) associated with a Condition. Following this discovery, the associated Condition is entered. The Required Actions establish those remedial measures that must be taken within specified Completion Times when the requirements of an LCO are not met. Concurrent entry into all applicable ACTIONS Conditions is a requirement to be followed in each specification. The Required Action(s) of each Condition entered must be completed within the specified Completion Time(s). There are two basic types of Required Actions. The first type of Required Action has an associated time limit in which the entered Condition must be corrected. This time limit is the Completion Time to place required equipment in operation, or to restore an inoperable system or component to OPERABLE status, or to restore variables to within specified limits. If this type of Required Action is not completed within the specified Completion Time, a shutdown may be required to place the facility in a MODE or Condition

(continued)

(continued)

BASES (continued)

LCO 3.0.2
(continued)

in which the specification no longer applies. (Whether stated as a Required Action or not, correction of the entered condition is the first action that is to be considered upon entering ACTIONS.) The second type of Required Action specifies the remedial measures that permit continued operation of the facility that is not further restricted by the Completion Time. In this case, conformance to the Required Actions provides an acceptable level of safety for continued operation. This type of Required Action is common throughout the Technical Specifications (TS).

This specification establishes that performance of the Required Actions within the specified Completion Times constitutes compliance with the TS. It also establishes, however, that completing the performance of the Required Actions is not required when an LCO is met within the associated Completion Time, unless otherwise stated in the individual specifications. This is equivalent to stating that correction of an ACTIONS Condition prior to the expiration of the specified Completion Time(s) makes it unnecessary to continue or complete the performance of the associated Required Action(s).

This specification is written for the more general case in which more than one of the stated Conditions are concurrently applicable. As each Condition is resolved, the Required Action(s) for that Condition no longer need be performed.

A Condition once entered or once applicable is resolved either by completing corrective measures such that it no longer exists or by placing the facility outside the Applicability of the LCO.

The nature of some Required Actions necessitates that, once begun, their performance must be completed even though the associated Conditions are resolved. The individual LCO's ACTIONS specify the Required Actions where this is the case. An example of this is in LCO 3.8.1, "AC Sources—Operating."

The above discussion about not having to complete the performance of Required Actions once the corresponding Conditions have been resolved also applies to the category

(continued)

(continued)

BASES (continued)

LCO 3.0.2 (continued)

of Conditions that state, "Required Actions and associated Completion Times not met."

Usually, the Required Action for a Condition of this type is to go to an inapplicable MODE or other specified Condition. The performance of such a shutdown Required Action may be suspended if the LCO Required Action that was not performed is completed or if the LCO is restored. If the shutdown had proceeded to the point where a MODE change had occurred, however, returning to the previously applicable MODE or specified Condition is not allowed by LCO 3.0.4, unless otherwise specified.

It is possible in some LCOs (but unlikely) to enter and exit two or more ACTION's Conditions repeatedly, in such a manner that facility operation could continue indefinitely without ever having restored the LCO (i.e., the facility is always in at least one of the Conditions). Because of the risk associated with extended facility operation with certain LCOs unmet, Specification 1.3 limits such operation to the longer of the specified Completion Times for the Conditions that are concurrently entered. This limitation does not apply to Conditions where the associated Required Actions, if met, permit continued operation for an unlimited period of time.

The Completion Times of the Required Actions are also applicable when a system or component is removed from service intentionally. The reasons for intentionally relying on the ACTIONS include, but are not limited to, performance of surveillances, preventive maintenance, corrective maintenance, or investigation of operational problems. Entering ACTIONS for these reasons must be done in a manner that does not compromise safety. It is not intended that intentional entry into ACTIONS be made for operational convenience. Intentional entry into ACTIONS Conditions with shutdown Required Actions (i.e., Actions requiring a change in MODE) is strongly discouraged and should be considered only in extreme circumstances. This is to limit routine voluntary removal of redundant equipment from service in lieu of other alternatives that would not result in redundant equipment being inoperable. Individual specifications may specify a time limit for performing an SR when equipment is removed from service or bypassed for testing. In such a case, the Completion Times of the

(continued)

(continued)

BASES (continued)

LCO 3.0.2 (continued)

Required Actions are applicable when this time limit expires, if the SR has not been completed. When a change in MODE or other specified Condition is required to comply with Required Actions, the facility may enter a MODE or other specified condition in which a new specification becomes applicable. Upon the new specification becoming applicable, immediately enter all ACTIONS Conditions that apply, unless otherwise specified. The Completion Times of the associated Required Actions would apply from the point in time that the new specification became applicable.

LCO 3.0.3

LCO 3.0.3 establishes the Required Actions that must be implemented when an LCO is not met;

a. An associated Required Action and Completion Time is not met and no other Condition applies; or

b. The condition of the facility is not specifically addressed by the associated ACTIONS. This means that no combination of Conditions stated in the ACTIONS can be made that exactly corresponds to the actual condition of the facility. Sometimes, possible combinations of Conditions are such that going to LCO 3.0.3 is warranted; in such cases, the ACTIONS specifically state a Condition corresponding to such combinations and also that LCO 3.0.3 be entered immediately.

This specification delineates the time limits for placing the facility in a safe MODE or other specified condition when operation cannot be maintained within the limits for safe operation as defined by the LCO and its ACTIONS. It is not to be used as an operational convenience that permits routine voluntary removal of redundant systems or components from service in lieu of other alternatives that would not result in redundant systems or components being inoperable. Intentional entry into LCO 3.0.3 for operational convenience constitutes noncompliance with the TS. Under suitable circumstances, intentional entry into LCO 3.0.3 for corrective action or repairs may be justified, but prior notification of the NRC should be considered.

(continued)

(continued)

BASES (continued)

LCO 3.0.3 (continued)

After entering LCO 3.0.3, 1 hour is allowed to prepare for an orderly shutdown before initiating a change in facility operation. This includes time to permit the operator to coordinate the reduction in electrical generation with the load dispatcher to ensure the stability and availability of the electrical grid. The time limits specified to reach higher-numbered MODES of operation permit the shutdown to proceed in a controlled and orderly manner that is well within the specified maximum cool-down rate and within the capabilities of the facility, assuming that only the minimum required equipment is OPERABLE. This reduces thermal stresses on components of the Reactor Coolant System (RCS) and the potential for a plant upset that could challenge safety systems under conditions to which this specification applies. The use and interpretation of specified times to complete the actions of LCO 3.0.3 shall be consistent with the discussion of Specification 1.3, "Completion Times."

A facility shutdown required in accordance with LCO 3.0.3 may be terminated and LCO 3.0.3 exited if any of the following occurs:

a. The LCO is now met;

b. Remedial measures have restored the facility to an LCO Condition for which the Required Actions have now been performed, where such ACTIONS permit operation in that Condition for either a limited or unlimited period of time; or

c. Remedial measures have restored the facility to a Condition for which the Completion Times of the Required Action(s) have not expired. For example, while in MODE 1, one of the two Iodine Cleanup System trains is declared inoperable. The corresponding Condition for one inoperable train is entered and 7 days are allowed to restore the train to OPERABLE status. Then, the second train is declared inoperable at a time 24 hours into the Completion Time. Since no ACTIONS Condition is provided for both trains being inoperable, LCO 3.0.3 must be entered. If one of the trains is made OPERABLE while still in MODE 1, for example at time 30 hours (6 hours into LCO 3.0.3), then the shutdown may be halted and operation can

(continued)

(continued)

BASES (continued)

LCO 3.0.3 (continued)

continue in the Condition of one train being inoperable. In this example, that would mean operation for another 5 days, 18 hours. If the train is restored to OPERABLE status after going to MODE 2, 3, 4, operation could continue only in the MODE that the facility is in when LCO 3.0.3 is exited. This is because LCO 3.0.4 does not permit MODE changes when the LCO is not met.

The time limits of Specification 3.0.3 allow 37 hours for the facility to be in MODE 5 when a shutdown is required during MODE 1 operation. If the facility is in a higher-numbered MODE of operation when a shutdown is required, the time limit for reaching the next higher-numbered MODE applies. If a higher-numbered MODE is reached in less time than allowed, however, the total allowable time to reach MODE 5, or other applicable MODE, is not reduced. For example, if MODE 3 is reached in 2 hours, then the time allowed to reach MODE 4 is the next 11 hours, because the total time to reach MODE 4 is not reduced from the allowable limit of 13 hours. Therefore, if remedial measures are completed that would permit a return to MODE 1, a penalty is not incurred by having to reach a higher-numbered MODE of operation in less than the total time allowed.

In MODES 1, 2, 3, and 4, LCO 3.0.3 provides Required Actions for Conditions not stated in other Specifications. The requirements of LCO 3.0.3 do not apply in MODES 5 and 6 because the facility is already in the most restrictive Condition in which LCO 3.0.3 would require the facility to be placed. The requirements of LCO 3.0.3 do not apply in other specified Conditions of the Applicability (unless in MODE 1, 2, 3, or 4) because the ACTIONS of individual specifications sufficiently define the remedial measures to be taken. [This must be verified by review of all LCOs when finalized.]

The exceptions to LCO 3.0.3 are provided in instances where requiring a facility shutdown, in accordance with LCO 3.0.3, would not provide appropriate remedial measures for the associated condition of the facility. These exceptions are addressed in the individual Specifications.

(continued)

(continued)

BASES (continued)

LCO 3.0.3 (continued)

The requirement to be in MODE 4 in 13 hours is plant specific and depends on the ability to cool the pressurizer and degas.

LCO 3.0.4

LCO 3.0.4 establishes limitations on changes in MODES or other specified Conditions in the Applicability when an LCO is not met. It precludes placing the facility in a different MODE or other specified Condition when the following exists:

a. The requirements of an LCO in the MODE or other specified Condition to be entered are not met; and

b. Continued noncompliance with these requirements would eventually result in a shutdown to comply with the Required Actions.

Compliance with Required Actions that permit continued operation of the facility for an unlimited period of time in an applicable MODE or other specified Condition provides an acceptable level of safety for continued operation. Therefore, in such cases, entry into a MODE or other Condition specified in the Applicability is made in accordance with the provisions of the Required Actions. The provisions of this specification should not be interpreted as endorsing the failure to exercise good practice in restoring systems or components to OPERABLE status before facility startup.

The provisions of LCO 3.0.4 shall not prevent changes in MODES or other specified Conditions in the Applicability that are required to comply with ACTIONS.

Exceptions to LCO 3.0.4 are stated in the individual specifications. Exceptions may apply to all the ACTIONS or to a specific Required Action of a specification. While entering or changing MODES or other specified conditions during operation of the facility in an ACTIONS Condition, as permitted by LCO 3.0.4 or where an exception to LCO 3.0.4 is stated, the ACTIONS define the remedial measures that must be taken. Surveillances do not have to be performed on the associated inoperable equipment (or on variables outside the specified limits), as permitted by SR 3.0.1. Therefore, a

(continued)

(continued)

BASES (continued)

LCO 3.0.4 (continued)

MODE change in this situation does not violate SR 3.0.4 for those Surveillances that do not have to be performed due to the associated inoperable equipment, etc. SRs must, however, be met to demonstrate OPERABILITY prior to declaring the affected equipment OPERABLE (or variable within limits) and the associated LCOs met.

LCO 3.0.5

Special tests and operations are required at various times over the facility's life to demonstrate performance characteristics, to perform maintenance activities, and to perform special evaluations. Because TS normally preclude these tests and operations, special test exceptions (STEs) allow specified requirements to be changed or suspended under controlled conditions. STEs are included in applicable sections of the specifications. Unless otherwise specified, all other TS requirements remain unchanged and in effect as applicable. This will ensure that all appropriate requirements of the MODE or other specified Condition not directly associated with or required to be changed or suspended to perform the special test or operation will remain in effect.

The Applicability of an STE LCO represents a Condition not necessarily in compliance with the normal requirements of the TS. Compliance with STE LCOs is optional.

A special test may be performed either under the provisions of the appropriate STE LCO or the other applicable TS requirements. If it is desired to perform the special test under the provisions of the STE LCO, the requirements of the STE LCO shall be followed. This includes the SRs specified in the STE LCO.

Some of the STE LCOs require that one or more of the LCOs for normal operation be met (i.e., meeting the STE LCO requires meeting the specified normal LCOs). The Applicability, ACTIONS, and SRs of the specified normal LCOs, however, are not required to be met in order to meet the STE LCO when it is in effect. This means that, upon failure to meet a specified normal LCO, the associated ACTIONS of the STE LCO apply, in lieu of the ACTIONS of the normal LCO. Exceptions to the above do exist. There are instances when the Applicability of the specified normal LCO

(continued)

(continued)

BASES (continued)

LCO 3.0.5 (continued)

must be met, where its ACTIONS must be taken, where certain of its Surveillances must be performed, or where all of these requirements must be met concurrently with the requirements of the STE LCO.

Unless the SRs of the specified normal LCOs are suspended or changed by the special test, those SRs that are necessary to meet the specified normal LCOs must be met prior to performing the special test. During the conduct of the special test, those Surveillances need not be performed unless specified by the ACTIONS or SRs of the STE LCO.

ACTIONS for STE LCOs provide appropriate remedial measures upon failure to meet the STE LCO. Upon failure to meet these ACTIONS, suspend the performance of the special test and enter the ACTIONS for all LCOs that are then not met. Entry into LCO 3.0.3 may possibly be required, but this determination should not be made by considering only the failure to meet the ACTIONS of the STE LCO.

B 3.0 APPLICABILITY

B 3.0 Surveillance Requirement (SR) Applicability

BASES

SR 3.0.1, SR 3.0.2, SR 3.0.3, and SR 3.0.4	SR 3.0.1, SR 3.0.2, SR 3.0.3, and SR 3.0.4 establish the general requirements applicable to all specifications unless otherwise stated. This includes specifications regarding the programs in Section 5.7.4, "Programs and Manuals," as well as specifications contained in Sections 3.1 through 3.9.
SR 3.0.1	SR 3.0.1 establishes the requirement that SRs must be met during the MODES or other specified Conditions in the Applicability of the LCO, unless otherwise specified in the individual SRs. This specification ensures that Surveillances are performed to verify the OPERABILITY of systems and components, and that variables are within specified limits. Failure to meet an SR within the specified Frequency, in accordance with SR 3.0.2, constitutes a failure to meet an LCO.

Systems and components are assumed to be OPERABLE when the associated SRs have been met. Nothing in this specification, however, is to be construed as implying that systems or components are OPERABLE when:

a. The systems or components are known to be inoperable, although SRs are being met; or

b. The requirements of the Surveillance(s) are known not to be met between required performances of the Surveillance(s).

Surveillances do not have to be performed when the facility is in a MODE or other specified Condition for which the associated LCO is not applicable, unless otherwise specified. The SRs associated with a special test exception (STE) are only applicable when the STE is used as an allowable exception to the requirements of a specification.

(continued)

(continued)

BASES (continued)

SR 3.0.1 (continued)

Surveillances, including Surveillances invoked by Required Actions, do not have to be performed on inoperable equipment because the ACTIONS define the remedial measures that apply. SRs have to be met in accordance with SR 3.0.2 prior to returning equipment to OPERABLE status.

Upon completion of maintenance, appropriate post-maintenance testing (which usually includes Surveillance testing) is required to declare equipment OPERABLE. Post-maintenance testing may not be possible in the MODE or Condition that the facility is in when the maintenance is completed because the necessary facility parameters have not been established. In these situations, proceeding to the appropriate applicable MODE or other specified Condition may be allowed as an exception to SR 3.0.4, provided that such an exception is stated in the requirements of the affected equipment's LCO. Such exceptions to SR 3.0.4 are permitted, provided that the post-maintenance and Surveillance testing to demonstrate OPERABILITY of the equipment has been satisfactorily completed to the extent possible and provided that the equipment is not otherwise suspected of being incapable of performing its intended function. Once the necessary facility parameters have been established, completion of the excepted tests must be accomplished to demonstrate OPERABILITY of the equipment.

SR 3.0.2

SR 3.0.2 establishes the requirements for meeting the specified Frequency for SRs, the Required Actions that call for the performance of a Surveillance, and any Required Action with a Completion Time that requires the periodic performance of an action on a "once per..." interval.

SR 3.0.2 permits a 25% extension of the interval specified in the Frequency or periodic Completion Time. This provides flexibility to Surveillance scheduling by providing the opportunity for consideration of plant operating conditions that may not be suitable for conducting the Surveillance (e.g., transient conditions or other ongoing Surveillance or maintenance activities).

(continued)

(continued)

BASES (continued)

SR 3.0.2 (continued)

The 25% extension does not significantly degrade the assurance of reliability obtained by performing the Surveillance at its specified Frequency. This recognizes that the most probable result of any particular Surveillance being performed is the verification of conformance with the SRs. The exceptions to SR 3.0.2 are those Surveillances for which the 25% extension of the interval specified in the Frequency does not apply. These exceptions are stated in the individual specifications. An example of where SR 3.0.2 does not apply is a Surveillance with a Frequency of "in accordance with 10 CFR 50, Appendix J, and approved exemptions." The requirements of regulations take precedence over the Technical Specifications (TS). The TS cannot extend a test interval specified in the regulations. Therefore, there would be a Note in the Frequency stating, "Provisions of SR 3.0.2 are not applicable."

As stated in SR 3.0.2, the 25% extension also does not apply to the initial portion of a periodic Completion Time. The initial performance of the Required Action, whether it is a particular Surveillance or some other remedial action, is considered a single action with a single Completion Time. One reason for not allowing the 25% extension to this Completion Time is that such an action usually verifies that no loss of function has occurred by checking the status of redundant or diverse components or accomplishes the function of the inoperable equipment in an alternative manner to ensure that specified limits or conditions of the LCO are met.

The previous Standard Technical Specifications (STS) also contained a specification that permitted the 25% extension, but restricted the combined time interval for any three consecutive Surveillance intervals to 3.25 times the specified interval. Generic Letter 89-14 (Ref. 1) encouraged licensees to request license amendments to remove the 3.25 restriction, because the NRC staff concluded that the removal would result in a greater benefit to safety. This line-item improvement to the STS did not extend the Applicability of the 25% extension to intervals associated with LCO Required Actions (including Required Actions to perform Surveillances) specified for periodic performance. The NRC staff subsequently concluded, however, that extending the applicability of the 25% extension to

(continued)

(continued)

BASES (continued)

SR 3.0.2 (continued)

periodic Completion Times, as SR 3.0.2 does, was also justified because the reasons for doing so were essentially the same as the reasons that originally justified the 25% extension (i.e., flexibility for scheduling the performance of Surveillances, etc.). Extending periodic Completion Time intervals for performing Surveillances or repetitive remedial actions specified by ACTIONS can result in a benefit to safety when the performance is due at a time that is not suitable because of plant operating conditions, for example.

The provisions of SR 3.0.2 are not intended to be used repeatedly merely as an operational convenience to extend Surveillance intervals or periodic Completion Time intervals beyond those specified.

SR 3.0.3

SR 3.0.3 establishes the option to defer declaring affected equipment inoperable or an affected variable outside the specified limits when a Surveillance has not been completed within the specified Frequency. A delay period of up to 24 hours applies from the point in time that it is discovered that the Surveillance has not been performed, in accordance with SR 3.0.2, and not at the time that the specified Frequency was not met. This 24-hour delay period was approved by the NRC as a line-item improvement to the STS in Generic Letter 87-09 (Ref. 2). The length of the delay period in SR 3.0.3 differs from the 24-hour allowance in the generic letter. SR 3.0.3 limits it to 24 hours or the specified Surveillance interval, whichever is shorter. Although the 24-hour allowance is not applicable to all the cases apparently provided for in the generic letter, the intent of the generic letter was to only allow the specified Surveillance interval in which to complete a missed Surveillance when the Frequency is less than 24 hours.

This delay period provides an adequate time limit to complete Surveillances that have been missed. This delay period provides the opportunity to complete a Surveillance that otherwise could not be completed before compliance with ACTIONS would be required and when compliance with such ACTIONS would then preclude completion of the Surveillance.

(continued)

(continued)

BASES (continued)

SR 3.0.3 (continued)

The basis for this delay period includes consideration of facility conditions, adequate planning, availability of personnel, the time required to perform the Surveillance, and the safety significance of the delay in completing the Surveillance. The delay period is considered appropriate for balancing the risk associated with delaying completion of the Surveillance for this period against the risk associated with the potential for a plant transient and challenge to safety systems when the alternative is a shutdown to comply with ACTIONS before the Surveillance can be completed.

SR 3.0.3 differs from the position taken in Generic Letter 87-09 in one other respect. Unlike the generic letter, SR 3.0.3 authorizes the delay-period option for performance of missed Surveillances without respect to the duration of the Completion Time associated with the LCO Condition that would otherwise be entered.

When a Surveillance with a Frequency based not on time intervals, but upon specified facility Conditions or operational situations, is discovered not to have been performed when specified, SR 3.0.3 allows the full 24-hour delay period in which to perform the Surveillance.

An additional application of SR 3.0.3 is to establish a time limit for completion of Surveillances that become applicable as a consequence of MODE changes imposed by Required Actions, when such Surveillances could not be completed prior to entering the applicable MODE or other specified Condition either because there was insufficient time or because plant conditions were not suitable for performance of the Surveillance.

The provisions of SR 3.0.3 exist because it is recognized that the most probable result of the performance of a particular Surveillance is the verification of conformance with the SRs and that a facility shutdown entails some risk that ought to be avoided unless a shutdown is actually warranted. Implementation of the provisions of SR 3.0.3, however, does not imply that a violation of SR 3.0.1 has not occurred, except in situations where SRs become applicable as a consequence of MODE changes imposed by Required Actions, as described above.

(continued)

(continued)

BASES (continued)

SR 3.0.3 (continued)

Failure to comply with specified Frequencies for SRs is expected to be an infrequent occurrence. Use of the delay period established by SR 3.0.3 is optional and is expected only under extreme circumstances.

If a Surveillance is not completed within the allowed delay period, the equipment is considered inoperable or the variable is considered outside the specified limits and the Completion Times of the Required Actions for the applicable LCO Conditions begin immediately upon expiration of the delay period. If a Surveillance is failed within the delay period, then the equipment is inoperable, or the variable is outside the specified limits and the Completion Times of the Required Actions for the applicable LCO Conditions begin immediately upon the failure of the Surveillance.

Completion of the Surveillance within the delay period allowed by this specification, or within the Completion Time of the ACTIONS, restores compliance with SR 3.0.1.

SR 3.0.4

SR 3.0.4 establishes the requirement that all SRs associated with an LCO and all applicable Section 5.7.4 program requirements must be met before entry into a MODE or other specified Condition in the Applicability of the LCO. Thus, prior to entry into an applicable MODE or other specified Condition, all of the SRs associated with all of the LCOs applicable in that MODE or Condition must be met.

This specification ensures that requirements on system and component OPERABILITY and variable limits that are necessary for safe operation of the facility are met before entry into an applicable MODE or other specified Condition to which the requirements apply. This specification applies to changes in MODES or other specified Conditions in the Applicability associated with facility shutdown as well as startup.

The provisions of SR 3.0.4 shall not prevent changes in MODES or other specified Conditions in the Applicability that are required to comply with ACTIONS.

(continued)

(continued)

BASES (continued)

SR 3.0.4 (continued)

Exceptions to SR 3.0.4 are needed in several situations. Because the concerns of each situation are not the same, the conditions under which the exceptions are permitted are different. Briefly, these situations are as follows:

a. When there is insufficient time to complete a Surveillance prior to the associated LCO becoming applicable as a result of complying with ACTIONS, the provisions of SR 3.0.3 apply; and

b. When an individual exception to SR 3.0.4 is stated in the individual specification:

   1. if the Surveillance is required to be performed, after entry into an applicable MODE or other specified Condition, because the specified Surveillance interval expired, and there is no other reason to suspect that the affected equipment (or variable) is inoperable (or outside limits), then a Completion Time of 12 hours is specified.

      Unless otherwise stated, performance of the Surveillance is not required if the specified Surveillance interval has not expired.

   2. if the Surveillance is required by the specified Frequency to be performed every time the LCO becomes applicable, then, unless an alternative Completion Time is specified, the 12-hour limit applies.

   3. if the Surveillance must be performed for the additional purpose of restoring the affected equipment (or variable) to OPERABLE status (or to within limits), upon entering an applicable MODE or other specified Condition, the associated ACTIONS of the LCO must be entered, unless specified otherwise in the individual specification. The ACTIONS specify the Completion Time allowed.

A more detailed discussion of these situations follows.

(continued)

(continued)

BASES (continued)

SR 3.0.4 (continued)

If unable to complete a Surveillance prior to its becoming applicable because Required Actions in an LCO affected changes in MODES or other specified Conditions, then upon entering the applicable MODE or other specified Condition, a delay period within which to complete the Surveillance is allowed, as specified in SR 3.0.3. This use of the provisions of SR 3.0.3 is an exception to SR 3.0.4 that applies only when an exception to SR 3.0.4 is not provided in the individual specification, as discussed below. The exception of SR 3.0.3 is not intended to be used consecutively with exceptions to SR 3.0.4 stated in the individual specifications.

Individual exceptions to SR 3.0.4 are usually stated with the SRs. These exceptions are provided to permit performance of Surveillance testing that otherwise would be prevented by compliance with SR 3.0.4. The prerequisite conditions for such a Surveillance (usually specified in the Surveillance test procedure) require entry into an applicable MODE or specified Condition in order to perform or complete the Surveillance test. If an exception to SR 3.0.4 is stated in an individual specification, a Completion Time of 12 hours, which begins upon entering the prerequisite MODE or Condition, is specified by SR 3.0.4 for performing the Surveillance when the specified Surveillance interval has expired (including the 25% extension), unless otherwise specified. It is expected that the performance of such Surveillances will commence soon after entry into the prerequisite MODE or other specified Condition. Use of the entire 12-hour Completion Time interval is expected to occur infrequently. The 12 hours provide sufficient operational flexibility, so the 25% extension allowed by SR 3.0.2 is not needed and therefore does not apply.

This 12-hour Completion Time applies when there is no reason to conclude that the affected equipment is inoperable, or the variable is outside specified limits other than the expiration of the Surveillance interval specified by the Frequency. If still within the Surveillance interval, the Surveillance is still considered to be met and does not have to be performed solely because its LCO becomes Applicable. The 12-hour Completion Time also applies to those Surveillances that are specified to be performed only one time after the prerequisite conditions have been established (i.e., Surveillances that do not have a periodic Frequency

(continued)

(continued)

BASES (continued)

SR 3.0.4 (continued)

specified). If 12 hours is not an appropriate Completion Time for a Surveillance that has an exception to SR 3.0.4 stated in the individual specification, then the stated exception to SR 3.0.4 specifies an alternative Completion Time, which should be followed. If an alternative Completion Time is not specified, then the 12-hour Completion Time applies. In the event the Surveillance is failed, compliance with the ACTIONS of the LCO is required.

The 2-hour Completion Time does not apply when performance of the Surveillance is necessary to establish the affected equipment's OPERABILITY as follows:

a. The equipment was declared inoperable for reasons other than the surveillance interval expired.

b. It is necessary to establish that the affected variable is restored to within limits after the variable was known to be outside limits.

In such situations, prior to entering a MODE or other specified Condition in the Applicability of the LCO, appropriate measures must be taken to provide reasonable assurance that the affected equipment or variable is able to meet the requirements of the Surveillance. For example, post-maintenance testing of equipment may not demonstrate OPERABILITY of the equipment with as much assurance as the Surveillance testing does, but it could be an appropriate measure to provide assurance that the Surveillance will be passed. In some cases, appropriate measures could include partial or complete performance of the Surveillance using suitably revised acceptance criteria, if necessary.

It must be emphasized that entry into an applicable MODE or specified Condition, when the affected equipment is known to be inoperable or when the affected variable is known to be outside specified limits, is not permitted by any exception to SR 3.0.4 that is stated in an individual specification. There must first be a reasonable expectation that performance of the Surveillance will establish that the equipment is OPERABLE or that the variable is within specified limits. At the time the associated LCO becomes applicable (because of entry into an applicable MODE or specified Condition from a non-applicable MODE or Condition), the ACTIONS of the LCO must be entered for the

(continued)

(continued)

BASES (continued)

SR 3.0.4 (continued)

Condition corresponding to the affected equipment or variable being inoperable or outside specified limits. The SR must be met and the entered Conditions corrected prior to expiration of the specified Completion Time. Any associated Required Actions other than the Action to restore the equipment to OPERABLE status or to return the variable to within the specified limits must be accomplished within the specified Completion Times until the entered Condition is corrected. In the event the Surveillance is failed, compliance with the ACTIONS of the LCO is required. The Completion Time clock (that began when the LCO became applicable and is associated with the Required Action to correct the entered Condition) does not reset upon failure of the Surveillance.

REFERENCES

1. NRC Generic Letter 89-14, "Line-Item Improvements in Technical Specifications - Removal of 3.25 Limit on Extending Surveillance Intervals," August 21, 1989.

2. NRC Generic Letter 87-09, "Sections 3.0 and 4.0 of the Standard Technical Specifications (STS) on the Applicability of Limiting Conditions for Operation and Surveillance Requirements," June 4, 1987.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM)—T_{avg} > 200°F (Analog)

BASES

BACKGROUND

The Reactivity Control System must be redundant and capable of holding the reactor core subcritical when shut down under cold conditions (GDC 26, Ref. 1). Maintenance of the SDM ensures that postulated reactivity events will not damage the fuel. SDM requirements provide sufficient reactivity margin to ensure that acceptable fuel design limits will not be exceeded for normal shutdown and anticipated operational occurrences (AOOs). As such, in MODES 1 and 2 the SDM defines the degree of subcriticality that would be obtained immediately following the insertion or scram of all control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn. In MODES 3, 4, and 5, the SDM specified continues to provide for adequate shutdown capability and acceptable fuel design limits for potential accidents initiated from shutdown conditions.

The system design requires that two independent Reactivity Control Systems be provided, and that one of these systems be capable of maintaining the core subcritical under cold conditions. These requirements are provided by the use of movable CEAs and soluble boric acid in the Reactor Coolant System (RCS). The CEA System can compensate for the reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full-load to no-load. In addition, the CEAs, together with the Boration System, provide the SDM during power operation and are capable of making the core subcritical rapidly enough to prevent exceeding acceptable fuel damage limits, assuming that the CEA of highest reactivity worth remains fully withdrawn.

The soluble Boron System can compensate for fuel depletion during operation and all xenon burnout reactivity changes, and maintain the reactor subcritical under cold conditions.

During power operation, SDM control is ensured by operating with the shutdown CEAs fully withdrawn and the regulating CEAs within the limits of LCO 3.1.7. When in the shutdown and refueling MODES, the SDM requirements are met by adjustments to the RCS boron concentration.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Ref. 2) establishes a SDM that ensures that specified acceptable fuel design limits are not exceeded for normal operation and AOOs with the assumption of the highest worth CEA stuck out on scram.

The acceptance criteria for the SDM are that specified acceptable fuel design limits are maintained by ensuring that:

a. The reactor can be made subcritical from all operating conditions and transients and Design Basis Event (DBEs);

b. The reactivity transients associated with postulated accident conditions are controllable within acceptable limits (departure from nucleate boiling ratio (DNBR), fuel centerline temperature limit AOOs, and ≤ 280 cal/gm energy deposition for the CEA ejection accident); and

c. The reactor will be maintained sufficiently subcritical to preclude inadvertent criticality in the shutdown condition.

The most limiting accident for the SDM requirements are based on a main steam line break (MSLB) as described in the accident analysis (Ref. 2). The increased steam flow resulting from a pipe break in the main steam system causes an increased energy removal from the affected steam generator, and consequently the RCS. This results in a reduction of the reactor coolant temperature. The resultant coolant shrinkage causes a reduction in pressure. In the presence of a negative moderator temperature coefficient, this cooldown causes an increase in core reactivity. As RCS temperature decreases, the severity of an MSLB decreases until the MODE 5 value is reached. The most limiting MSLB, with respect to potential fuel damage before a reactor trip occurs, is a guillotine break of a main steam line inside containment initiated at the end of core life. The positive reactivity addition from the moderator temperature decrease will terminate when the affected steam generator boils dry, thus terminating RCS heat removal and cooldown. Following the MSLB, a post-trip return to power may occur; however, no

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

fuel damage occurs as a result of the post-trip return to power and the THERMAL POWER does not violate the Safety Limit requirement of SL 2.1.1.

In addition to the limiting MSLB transient, the SDM requirement must also protect against:

a. Inadvertent boron dilution;

b. An uncontrolled CEA withdrawal from a subcritical or low power condition;

c. Startup of an inactive reactor coolant pump (RCP); and

d. CEA ejection.

Each of these events is discussed below.

In the boron dilution analysis, the required SDM defines the reactivity difference between an initial subcritical boron concentration and the corresponding critical boron concentration. These values, in conjunction with the configuration of the RCS and the assumed dilution flow rate, directly affect the results of the analysis. This event is most limiting at the beginning of core life when critical boron concentrations are highest.

The withdrawal of CEAs from subcritical or low power conditions adds reactivity to the reactor core, causing both the core power level and heat flux to increase with corresponding increases in reactor coolant temperatures and pressure. The withdrawal of CEAs also produces a time dependent redistribution of core power.

Depending on the system initial conditions and reactivity insertion rate, the uncontrolled CEA withdrawal transient is terminated by either a high power trip, or a high pressurizer pressure trip. In all cases, power level, RCS pressure, linear heat rate, and the DNBR do not exceed allowable limits.

The startup of an inactive RCP will not result in a "cold water" criticality even if the maximum difference in temperature exists between the steam generator and the core. The maximum positive reactivity addition that can occur due

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

to an inadvertent RCP start is less than half the minimum required SDM. An idle RCP cannot, therefore, produce a return to power from the hot standby condition.

SDM satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed from the control room, SDM is considered an initial condition process variable because it is periodically monitored to provide assurance that the unit is operating within the bounds of accident analysis assumptions.

LCO

The accident analysis has shown that the required SDM is sufficient to avoid unacceptable consequences to the fuel or RCS as a result of the events addressed above. Shutdown boron concentration requirements assume the highest worth CEA is stuck in the fully withdrawn position to account for a postulated inoperable or untrippable CEA prior to reactor shutdown.

The MSLB (Ref. 2) and the boron dilution (Ref. 3) accidents are the most limiting analyses that establish the SDM value of the LCO. For MSLB accidents, if the LCO is violated, there is a potential to exceed the DNBR limit and to exceed 10 CFR 100 limits. For the boron dilution accident, if the LCO is violated, then the minimum required time assumed for operator action to terminate dilution may no longer be applicable.

SDM is a core physics design condition that can be ensured during operation through CEA positioning (regulating and shutdown CEA) and through the soluble boron concentration. To ensure that SDM is behaving as anticipated so that the acceptance criteria are met, the SDM is evaluated during surveillance SR 3.1.1.1, and appropriate actions are taken as necessary when the SDM is not within the required limit.

APPLICABILITY

In MODES 1, 2, 3, and 4, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analyses discussed above. In

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

MODE 5, SDM is addressed by LCO 3.1.2. In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1, "Boron Concentration."

ACTIONS

A.1

If the SDM requirements are not met, boration must be initiated immediately. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. Boration will be continued until SDM is within the limit.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique DBA that must be satisfied. It is imperative to raise the boron concentration of the RCS as soon as possible.

Therefore, the operator should begin boration with the best source available for the plant conditions. Some of the possible sources of boron originate from either the boric acid storage tank (BAST), whose minimum concentration of boron is [11600] ppm, or the borated water storage tank (BWST), whose minimum concentration of boron is [2270] ppm. These sources include:

a. Makeup flow through makeup pumps from makeup tank: Makeup pumps are rated at [300] gpm at [2400] psig. Boron concentration of the makeup tank varies with the time in life and the concentration in the RCS;

b. Makeup flow through makeup pumps from BWST: Makeup pumps are rated at [300] gpm at [2400] psig;

c. Makeup flow through makeup pumps from BAST: Makeup pumps are rated at [300] gpm at [2400] psig;

d. High pressure injection through makeup pumps from BWST: Makeup pumps are rated at [500] gpm at [600] psig;

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

e. Decay heat flow through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig;

f. Low pressure injection through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig; and

g. Boric acid through boric acid pumps from BAST: Boric acid pumps are rated at [25] gpm at [100] psig.

In determining the boration flow rate, it should be remembered that the most difficult time in core life to increase the RCS boron concentration is at beginning of cycle, when the boron concentration may approach or exceed [2000] ppm.

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

In MODES 1 and 2, SDM is verified by observing that the requirements of LCO 3.1.6, "Shutdown CEA Insertion Limit," and LCO 3.1.7, "Regulating CEA Insertion Limit," are met. However, in the event that a CEA is known to be untrippable, SDM verification must account for the worth of the untrippable CEA as well as another CEA of maximum worth.

In MODES 3, 4, and 5, the SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration;

b. CEA positions;

c. RCS average temperature;

d. Fuel burnup based on gross thermal energy generation;

e. Xenon concentration;

f. Samarium concentration; and

g. Isothermal Temperature Coefficient (ITC).

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

Using the ITC accounts for Doppler reactivity in this calculation because the reactor is subcritical and the fuel temperature will be changing at the same rate as the RCS. The Frequency of 24 hours is based on the generally slow change in required boron concentration, and also allows sufficient time for the operator to collect the required data, which includes performing a boron concentration analysis, and complete the calculation.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 26, "Reactivity Control System Redundancy and Capability."
2. [Unit Name] FSAR, Section [ ], "[Title]."
3. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 SHUTDOWN MARGIN (SDM)—$T_{avg} \leq 200°F$ (Analog)

BASES

BACKGROUND

The reactivity control system must be redundant and capable of holding the reactor core subcritical when shut down under cold conditions (GDC 26) (Ref. 1). Maintenance of the SDM ensures that postulated reactivity events will not damage the fuel. SDM requirements provide sufficient reactivity margin to assure that acceptable fuel design limits will not be exceeded for normal shutdown and anticipated operational occurrences (AOOs). As such, in MODES 1 and 2 the SDM defines the degree of subcriticality that would be obtained immediately following the insertion or scram of all control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn. In MODES 3, 4, and 5, the SDM specified continues to provide for adequate shutdown capability and acceptable fuel design limits for potential accidents initiated from shutdown conditions.

The system design requires that two independent Reactivity Control Systems be provided, and that one of these systems be capable of maintaining the core subcritical under cold conditions. These requirements are provided by the use of movable CEAs and soluble boric acid in the Reactor Coolant System (RCS). The CEA System can compensate for the reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full-load to no-load. In addition, the CEAs, together with the Boration System, provide the SDM during power operation and are capable of making the core subcritical rapidly enough to prevent exceeding the acceptable fuel damage limits, assuming that the CEA of highest reactivity worth remains fully withdrawn.

The soluble Boron System can compensate for fuel depletion during operation and all xenon burnout reactivity changes, as well as maintain the reactor subcritical under cold conditions.

During power operation, SDM control is ensured by operating with the shutdown CEAs fully withdrawn and the regulating

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

CEAs within the limits of LCO 3.1.7. When in the shutdown and refueling MODES, the SDM requirements are met by adjustments to the RCS boron concentration.

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Ref. 2) establishes a SDM that ensures that specified acceptable fuel design limits are not exceeded for normal operation and AOOs with the assumption of the highest-worth CEA stuck out on scram. Specifically, for MODE 5 the primary safety analysis that relies on the SDM limits is the boron dilution analysis.

The acceptance criteria for the SDM are that the specified acceptable fuel design limits are maintained by ensuring that:

a. The reactor can be made subcritical from all operating conditions and transients and Design Basis Events (DBEs);

b. The reactivity transients associated with postulated accident conditions are controllable within acceptable limits (departure from nucleate boiling ratio (DNBR), fuel centerline temperature limits for AOOs, and $\leq$ 280 cal/gm energy deposition for the CEA ejection accident); and

c. The reactor will be maintained sufficiently subcritical to preclude inadvertent criticality in the shutdown condition.

An inadvertent boron dilution is a moderate frequency incident as defined in Reference 2. The core is initially subcritical with all CEAs inserted. A Chemical and Volume Control System malfunction occurs, which causes unborated water to be pumped to the RCS via three charging pumps.

During the event a minimum flow of [3000] gal/min will be circulated through the RCS by the Shutdown Cooling (SDC) System, complete mixing of boron within the RCS is assumed. A cold (200°F) RCS volume — excluding the pressurizer, surge line, and the SDC System — of [10,060] ft^3 is assumed. Excluding the pressurizer, surge line, and SDC System

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

increases the severity of the dilution. At the SDC flow rate, an equivalent RCS volume will be circulated in approximately 30 minutes. The reactivity change rate associated with boron concentration changes is within the capabilities of operator recognition and control.

The high neutron flux alarm on the startup channel instrumentation will alert the operator of the boron dilution with a minimum of 15 minutes remaining before the core becomes critical. The event can then be terminated by either:

a. Turning off the charging pumps;

b. Turning off the primary makeup pump;

c. Isolating the reactor makeup water supply;

d. Isolating the volume control tank; or

e. Actuating safety injection.

SDM satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed from the control room, SDM is considered an initial condition process variable because it is periodically monitored to provide assurance that the unit is operating within the bounds of accident analysis assumptions.

LCO

The accident analysis has shown that the required SDM is sufficient to avoid unacceptable consequences to the fuel or RCS as a result of the events addressed above.

The boron dilution (Ref. 2) accident initiated in MODE 5 is the most limiting analysis that establishes the SDM value of the LCO. For the boron dilution accident, if the LCO is violated, then the minimum required time assumed for operator action to terminate dilution may no longer be applicable.

SDM is a core physics design condition that is evaluated during SR 3.1.2.1, and appropriate actions are taken as necessary when the SDM is not within the required limit.

(continued)

BASES (continued)

APPLICABILITY

In MODE 5, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analysis discussed above. In MODES 1, 2, 3, and 4, the SDM requirements are given in LCO 3.1.1, shutdown MARGIN — $T_{avg} > 200°F$." In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1, "Boron Concentration."

ACTIONS

A.1

If the SDM requirements are not met, boration must be initiated immediately. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. Boration will be continued until SDM is within the limit.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique design basis event that must be satisfied. It is imperative to raise the boron concentration of the RCS as soon as possible.

Therefore, the operator should begin boration with the best source available for the plant conditions. Some of the possible sources of boron originate from either the Boric Acid Storage Tank (BAST), whose minimum concentration of boron is [11600] ppm, or the Borated Water Storage Tank (BWST), whose minimum concentration of boron is [2270] ppm. These sources include:

a. Makeup flow through makeup pumps from makeup tank: Makeup pumps are rated at [300] gpm at [2400] psig (boron concentration of the makeup tank varies with the time in life and the concentration in the RCS);

b. Makeup flow through makeup pumps from BWST: Makeup pumps are rated at [300] gpm at [2400] psig;

c. Makeup flow through makeup pumps from BAST: Makeup pumps are rated at [300] gpm at [2400] psig;

d. High pressure injection through makeup pumps from BWST: Makeup pumps are rated at [500] gpm at [600] psig;

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

e. Decay heat flow through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig;

f. Low pressure injection through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig; and

g. Boric acid through boric acid pumps from BAST: Boric acid pumps are rated at [25] gpm at [100] psig.

In determining the boration flow rate, it should be remembered that the most difficult time in core life to increase the RCS boron concentration is at beginning of cycle (BOC), when the boron concentration may approach or exceed [2000] ppm.

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1

In MODE 5, the SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration;

b. CEA positions;

c. RCS average temperature;

d. Fuel burnup based on gross thermal energy generation;

e. Xenon concentration;

f. Samarium concentration; and

g. Isothermal Temperature Coefficient (ITC).

Using the ITC accounts for Doppler reactivity in this calculation because the reactor is subcritical and the fuel temperature will be changing at the same rate as that of the RCS.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)	The Frequency of 24 hours is based on the generally slow change in required boron concentration and also allows sufficient time for the operator to collect the required data, including a boron concentration analysis, and complete the calculation.
REFERENCES	1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 26, "Reactivity Control system Redundancy and Capability." 2. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Reactivity Balance (Analog)

BASES

BACKGROUND

Per GDCs 26, 28, and 29 (Ref. 1), reactivity shall be controllable such that subcriticality is maintained under cold conditions and acceptable fuel design limits are not exceeded during normal operation and anticipated operational occurrences. Therefore, reactivity balance is used as a measure of the predicted versus measured core reactivity during power operation. The periodic confirmation of core reactivity is necessary to ensure that safety analyses of design basis transients and accidents remain valid. A large reactivity difference could be the result of unanticipated changes in fuel, control element assembly (CEA) worth, or operation at conditions not consistent with those assumed in the predictions of core reactivity and could potentially result in a loss of SHUTDOWN MARGIN (SDM) or violation of acceptable fuel design limits. Comparing predicted versus measured core reactivity validates the nuclear methods used in the safety analysis and supports the SDM demonstrations (LCO 3.1.1) in assuring the reactor can be brought safely to cold, subcritical conditions.

When the reactor core is critical or in normal power operation, a reactivity balance exists and the net reactivity is zero. A comparison of predicted and measured reactivity is convenient under such a balance since parameters are being maintained relatively stable under steady-state power conditions. The positive reactivity inherent in the core design is balanced by the negative reactivity of the control components, thermal feedback, neutron leakage, and materials in the core that absorb neutrons, such as burnable absorbers producing zero net reactivity. Excess reactivity can be inferred from the boron letdown curve (or critical boron curve), which provides an indication of the soluble boron concentration in the Reactor Coolant System (RCS) versus cycle burnup. Periodic measurement of the RCS boron concentration for comparison with the predicted value with other variables fixed such as CEA height, temperature, pressure, and power provides a convenient method of ensuring that core reactivity is within design expectations, and that the calculation models used to generate the safety analysis are

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

adequate. In order to achieve the required fuel cycle energy output, the uranium enrichment, in the new fuel loading and in the fuel remaining from the previous cycle, provides excess positive reactivity beyond that required to sustain steady-state operation throughout the cycle. When the reactor is critical at RATED THERMAL POWER (RTP) and moderator temperature, the excess positive reactivity is compensated by burnable absorbers (if any), CEAs, whatever neutron poisons (mainly xenon and samarium) are present in the fuel, and the RCS boron concentration.

When the core is producing THERMAL POWER, the fuel is being depleted and excess reactivity is decreasing. As the fuel depletes, the RCS boron concentration is reduced to decrease negative reactivity and maintain constant THERMAL POWER. The boron letdown curve is based on steady-state operation at RTP. Therefore, deviations from the predicted boron letdown curve may indicate deficiencies in the design analysis, deficiencies in the calculational models, or abnormal core conditions, and must be evaluated.

APPLICABLE SAFETY ANALYSES

Accurate prediction of core reactivity is either an explicit or implicit assumption in the accident analysis evaluations. Every accident evaluation (Ref. 2) is, therefore, dependent upon accurate evaluation of core reactivity. In particular, SDM and reactivity transients, such as CEA withdrawal accidents or CEA ejection accidents, are very sensitive to accurate prediction of core reactivity. These accident analysis evaluations rely on computer codes which have been qualified against available test data, operating plant data, and analytical benchmarks. Monitoring reactivity balance provides additional assurance that the nuclear methods provide an accurate representation of the core reactivity.

Design calculations and safety analysis are performed for each fuel cycle for the purpose of predetermining reactivity behavior and the RCS boron concentration requirements for reactivity control during fuel depletion.

The comparison between measured and predicted initial core reactivity provides a normalization for calculational models used to predict core reactivity. If the measured and

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

predicted RCS boron concentrations for identical core conditions at beginning of cycle (BOC) do not agree, then the assumptions used in the reload cycle design analysis or the calculation models used to predict soluble boron requirements may not be accurate. If reasonable agreement between measured and predicted core reactivity exists at BOC, then the prediction may be normalized to the measured boron concentration. Thereafter, any significant deviations in the measured boron concentration from the predicted boron letdown curve that develop during fuel depletion may be an indication that the calculation model is not adequate for core burnups beyond BOC, or that an unexpected change in core conditions has occurred.

The normalization of predicted RCS boron concentration to the measured value is typically performed after reaching RTP following startup from a refueling outage, with the CEAs in their normal positions for power operation. The normalization is performed at BOC conditions so that core reactivity relative to predicted values can be continually monitored and evaluated as core conditions change during the cycle.

Reactivity balance provides an additional assurance that SDM is maintained within the limits. Thus, reactivity balance satisfies Criterion 2 or the NRC Interim Policy Statement.

LCO

This Specification is provided to ensure that core reactivity behaves as expected in the long term, and to ensure that significant reactivity anomalies will be investigated.

The reactivity balance limit is established to ensure plant operation is maintained within the assumptions of the safety analyses. Large differences between actual and predicted core reactivity may indicate that the assumptions of the design basis transient and accident analyses are no longer valid, or that the uncertainties in the nuclear method are larger than expected. A limit on the reactivity balance of ± 1% Δk/k has been established based on engineering

(continued)

(continued)

BASES (continued)

LCO (continued)

judgment. A 1% deviation in reactivity from that predicted is larger than expected for normal operation and should therefore be evaluated.

When measured core reactivity is within 1% Δk/k of the predicted value at steady-state thermal conditions, the core is considered to be operating within acceptable design limits. Since deviations from the limit are normally detected by comparing predicted and measured steady-state RCS critical boron concentrations, the difference between measured and predicted values would be approximately 100 ppm (depending on the boron worth) before the limit is reached. These values are well within the uncertainty limits for analysis of boron concentration samples, so that spurious violations of the limit due to uncertainty in measuring the RCS boron concentration are unlikely.

APPLICABILITY

In MODE 1, most of the CEAs are withdrawn and steady-state operation is typically achieved. Under these conditions, the comparison between predictions and measurements provides an effective measure of the reactivity balance. In MODE 2, CEAs are typically being withdrawn during a startup. In MODES 3, 4, and 5, all CEAs are fully inserted and therefore the reactor is in the least reactive state where monitoring core reactivity is not necessary. In MODE 6, fuel loading results in a continually changing core reactivity. Boron concentration requirements (LCO 3.9.1) ensure that fuel movements are performed within the bounds of the safety analysis, and an SDM demonstration is required during the first startup following operations which could have altered core reactivity (e.g., fuel movement or CEA replacement or shuffling).

ACTIONS

A.1 and A.2

Should an anomaly develop between measured and predicted core reactivity, an evaluation of the core design and safety analysis is performed.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

In practice, smaller deviations in core reactivity (greater than 0.5% Δk/k) are generally cause for concern, and evaluation of both core conditions and the core design are performed to determine the cause of the deviation.

When a reactivity deviation is noted, the evaluation of core conditions typically includes the following steps:

a. Core conditions and the input to calculational models are verified to be consistent;

b. Shutdown capability from both the CEAs and the boron injection system is determined to be adequate;

c. A core power distribution map is obtained to evaluate peaking factors;

d. OPERABILITY of all CEAs is verified; and

e. Physical changes in the fuel or boron content of the RCS are considered.

An evaluation of the core design and safety analysis typically includes the following steps:

a. Reactivity worth calculations of boron, the CEAs, xenon, and samarium are reviewed;

b. The moderator and fuel temperature coefficient calculations are reviewed and verified to be within the bounds of the safety analysis;

c. The fuel depletion calculations are reviewed to determine that the calculated core burnup is appropriate; and

d. The calculation models are reviewed to verify that they are adequate for representation of the core conditions.

Reactivity anomalies are generally investigated when they are small, so that the evaluations are in progress before the 1% Δk/k reactivity limit for a deviation is reached, and corrective measures may be defined. The required

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Completion Time of 72 hours is based on operating experience and the low probability of a Design Basis Accident (DBA) occurring during this period. Also, it allows sufficient time to assess the physical condition of the reactor and complete an evaluation of the core design and safety analysis.

Following evaluations of the core design and safety analysis, the cause of the reactivity anomaly may be resolved. If the cause of the reactivity anomaly is a mismatch in core conditions at the time of RCS boron concentration sampling, then a recalculation of the RCS boron concentration requirements may be performed to demonstrate that core reactivity is behaving as expected. If an unexpected physical change in the condition of the core has occurred, it must be evaluated and corrected, if possible. If the cause of the reactivity anomaly is in the calculation technique, then the calculational models must be revised to provide more accurate predictions. If any of these results are demonstrated and it is concluded that the reactor core is acceptable for continued operation, then the boron letdown curve may be renormalized, and power operation may continue. If operational restrictions or additional SRs are necessary to ensure the reactor core is acceptable for continued operation, then they must be defined.

B.1

The unit must be placed in a MODE in which the LCO does not apply if the core reactivity cannot be restored to within the 1% $\Delta k/k$ limit by the methods discussed in Required Action A.1 and A.2 and the associated Completion Time. This is done by placing the unit in at least MODE 3 within 6 hours. If the SDM for MODE 3 is not met, then boration required by SR 3.1.1.1 would occur. The allowed Completion Time is reasonable based on operating experience related to the time required to reach the required plant conditions from full power in an orderly manner and without challenging plant systems.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1

Core reactivity is verified by periodic comparisons of measured and predicted RCS boron concentrations. The comparison is made considering that other core conditions are fixed or stable including CEA position, moderator temperature, fuel temperature, fuel depletion, xenon concentration, and samarium concentration. The surveillance is performed prior to entering MODE 1 as an initial check on core conditions and design calculations at BOC. A Note is included in the SR to indicate that the normalization of predicted core reactivity to the measured value must take place within the first 60 effective full power days (EFPDs) after each fuel loading. This allows sufficient time for core conditions to reach steady state, but prevents operation for a large fraction of the fuel cycle without establishing a benchmark for the design calculations. The required subsequent Frequency of 31 EFPDs after the initial 60 EFPDs after entering MODE 1 is acceptable based on the slow rate of core changes due to fuel depletion and the presence of other indicators (Quadrant Power Tilt Ratio, etc.) for prompt indication of an anomaly. Another Note is included in SR to indicate that the provisions or SR 3.0.4 are not applicable for this SR for entering MODE 2.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 26, "Reactivity Control System Redundancy and Capability"; General Design Criterion 28, "Reactivity Limits"; General Design Criterion 29, "Protection Against Anticipated Operational Occurrences."

2. [Unit Name] FSAR, Section [ ], "[Accident Analysis]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Moderator Temperature Coefficient (MTC) (Analog)

BASES

BACKGROUND

Per GDC 11 (Ref. 1), the reactor core and its interaction with the reactor system coolant must be designed for inherently stable power operation, even in the possible event of an accident. In particular, the net reactivity feedback in the system must compensate for any unintended or rapid reactivity increases.

The MTC relates a change in core reactivity to a change in reactor coolant temperature (a positive MTC means that reactivity increases with increasing moderator temperature; conversely, a negative MTC means that reactivity decreases with increasing moderator temperature). The reactor is designed to operate with a negative MTC over the largest possible range of fuel cycle operation. Therefore, a coolant temperature increase will cause a reactivity decrease, so that the coolant temperature tends to return toward its initial value. Reactivity increases that cause a coolant temperature increase will thus be self-limiting, and stable power operation will result. The same characteristic is true when the MTC is positive and coolant temperature decreases occur.

MTC values are predicted at selected burnups during the safety evaluation analysis and are confirmed to be acceptable by measurements. Both initial and reload cores are designed so that the beginning of cycle (BOC) MTC is less than zero when THERMAL POWER is [95]% of RATED THERMAL POWER (RTP) or greater. The actual value of the MTC is dependent on core characteristics, such as fuel loading and reactor coolant soluble boron concentration. The core design may require additional fixed distributed poisons (lumped burnable poison assemblies) to yield a MTC at BOC within the range analyzed in the plant accident analysis. The end of cycle (EOC) MTC is also limited by the requirements of the accident analysis. Fuel cycles designed to achieve high burnups or with changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

subcritical conditions, a large fraction of core power may be produced through the effects of subcritical neutron multiplication.

MTC values are bounded in reload safety evaluations assuming steady-state conditions at BOC and EOC. A middle of cycle (MOC) measurement is conducted at conditions when the RCS boron concentration reaches approximately 300 ppm. The measured value may be extrapolated to project the EOC value, in order to confirm reload design predictions.

The MTC satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed and controlled from the control room, MTC is considered an initial condition process variable because of its dependence on boron concentration.

LCO

LCO 3.1.4 requires the MTC to be within specified limits of the CORE OPERATING LIMITS REPORT (COLR) (Ref. 5) to ensure the core operates within the assumptions of the accident analysis. During the reload core safety evaluation, the MTC is analyzed to determine that its values remain within the bounds of the original accident analysis during operation. The limit of [+0.9E-4] (%Δk/k)/F on a positive MTC when THERMAL POWER is less than [95]% of RTP ensures that core overheating accidents will not violate the accident analysis assumptions. The requirement for a negative MTC when THERMAL POWER is [95]% of RTP or greater ensures that core operation will be stable. The negative MTC limit for EOC specified in the COLR ensures that core overcooling accidents will not violate the accident analysis assumptions.

MTC is a core physics parameter determined by the fuel and fuel cycle design and cannot be easily controlled once the core design is fixed. During operation, therefore, the Conditions of the LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on a MTC provide confirmation that the MTC is behaving as anticipated so that the acceptance criteria are met.

(continued)

BASES (continued)

APPLICABILITY

In MODE 1, the limits on the MTC must be maintained to assure that any accident initiated from THERMAL POWER operation will not violate the design assumptions of the accident analysis. In MODE 2, the limits must also be maintained to ensure startup and subcritical accidents (such as the uncontrolled CEA or group withdrawal) will not violate the assumptions of the accident analysis. In MODES 3, 4, 5, and 6, this LCO is not applicable, since no Design Basis Accidents (DBAs) using the MTC as an analysis assumption are initiated from these MODES. However, the variation of the MTC with temperature in MODES 3, 4, and 5, for DBAs initiated in MODES 1 and 2, is accounted for in the subject accident analysis. The variation of the MTC with temperature assumed in the safety analysis is accepted as valid once the BOC and MOC measurements are used for normalization.

ACTIONS

A.1

MTC is a function of the fuel and fuel cycle design and cannot be controlled directly once their designs have been implemented in the core. If MTC exceeds its limits, the reactor must be placed in MODE 3 with a minimum SHUTDOWN MARGIN. This eliminates the potential for violation of the accident analysis bounds. The associated Completion Time of 6 hours is reasonable considering the probability of an accident occurring during the time period which would require a MTC value within the LCO limits and the length of time required to reach MODE 3 conditions from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

The SRs for measurement of the MTC at the beginning and middle of each fuel cycle provide for confirmation of the limiting MTC values. The MTC changes smoothly from most positive (least negative) to most negative value during fuel cycle operation as the RCS boron concentration is reduced to compensate for fuel depletion. The requirement for measurement prior to operation above 5% of RTP satisfies the confirmatory check on the most positive (least negative) MTC

(continued)

(continued)

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Moderator Temperature Coefficient (MTC) (Analog)

BASES

BACKGROUND

Per GDC 11 (Ref. 1), the reactor core and its interaction with the reactor system coolant must be designed for inherently stable power operation, even in the possible event of an accident. In particular, the net reactivity feedback in the system must compensate for any unintended or rapid reactivity increases.

The MTC relates a change in core reactivity to a change in reactor coolant temperature (a positive MTC means that reactivity increases with increasing moderator temperature; conversely, a negative MTC means that reactivity decreases with increasing moderator temperature). The reactor is designed to operate with a negative MTC over the largest possible range of fuel cycle operation. Therefore, a coolant temperature increase will cause a reactivity decrease, so that the coolant temperature tends to return toward its initial value. Reactivity increases that cause a coolant temperature increase will thus be self-limiting, and stable power operation will result. The same characteristic is true when the MTC is positive and coolant temperature decreases occur.

MTC values are predicted at selected burnups during the safety evaluation analysis and are confirmed to be acceptable by measurements. Both initial and reload cores are designed so that the beginning of cycle (BOC) MTC is less than zero when THERMAL POWER is [95]% of RATED THERMAL POWER (RTP) or greater. The actual value of the MTC is dependent on core characteristics, such as fuel loading and reactor coolant soluble boron concentration. The core design may require additional fixed distributed poisons (lumped burnable poison assemblies) to yield a MTC at BOC within the range analyzed in the plant accident analysis. The end of cycle (EOC) MTC is also limited by the requirements of the accident analysis. Fuel cycles designed to achieve high burnups or with changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The acceptance criteria for the specified MTC are:

a. The MTC values must remain within the bounds of those used in the accident analysis (Ref. 2); and

b. The MTC must be such that inherently stable power operations result during normal operation and during accidents such as overheating and overcooling events.

Reference 2 contains analyses of accidents that result in both overheating and overcooling of the reactor core. MTC is one of the controlling parameters for core reactivity in these accidents. Both the most positive value and most negative value of the MTC are important to safety, and both values must be bounded. Values used in the analyses consider worst-case conditions, such as very large soluble boron concentrations, to ensure the accident results are bounding (Ref. 3).

Accidents that cause core overheating (either decreased heat removal or increased power production) must be evaluated for results when the MTC is positive. Reactivity accidents that cause increased power production include the control element assembly (CEA) withdrawal transient from either zero or full THERMAL POWER. The limiting overheating event relative to plant response is based on the maximum difference between core power and steam generator heat removal during a transient. The most limiting event with respect to a positive MTC is a [CEA withdrawal accident from zero power, also referred to as a startup accident (Ref. 4)].

Accidents that cause core overcooling must be evaluated for results when the MTC is most negative. The event which produces the most rapid cooldown of the Reactor Coolant System (RCS) and is therefore the most limiting event with respect to the negative MTC is a steam line break (SLB) event. Following the reactor trip for the postulated EOC SLB event, the large moderator temperature reduction combined with the large negative MTC may produce reactivity increases that are as much as the shutdown reactivity. When this occurs, a substantial fraction of core power is produced with all CEAs inserted except the most reactive one. Even if the reactivity increase produces slightly

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

subcritical conditions, a large fraction of core power may be produced through the effects of subcritical neutron multiplication.

MTC values are bounded in reload safety evaluations assuming steady-state conditions at BOC and EOC. A middle of cycle (MOC) measurement is conducted at conditions when the RCS boron concentration reaches approximately 300 ppm. The measured value may be extrapolated to project the EOC value, in order to confirm reload design predictions.

The MTC satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed and controlled from the control room, MTC is considered an initial condition process variable because of its dependence on boron concentration.

LCO

LCO 3.1.4 requires the MTC to be within specified limits of the CORE OPERATING LIMITS REPORT (COLR) (Ref. 5) to ensure the core operates within the assumptions of the accident analysis. During the reload core safety evaluation, the MTC is analyzed to determine that its values remain within the bounds of the original accident analysis during operation. The limit of [+0.9E-4] (%Δk/k)/F on a positive MTC when THERMAL POWER is less than [95]% of RTP ensures that core overheating accidents will not violate the accident analysis assumptions. The requirement for a negative MTC when THERMAL POWER is [95]% of RTP or greater ensures that core operation will be stable. The negative MTC limit for EOC specified in the COLR ensures that core overcooling accidents will not violate the accident analysis assumptions.

MTC is a core physics parameter determined by the fuel and fuel cycle design and cannot be easily controlled once the core design is fixed. During operation, therefore, the Conditions of the LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on a MTC provide confirmation that the MTC is behaving as anticipated so that the acceptance criteria are met.

(continued)

BASES (continued)

APPLICABILITY

In MODE 1, the limits on the MTC must be maintained to assure that any accident initiated from THERMAL POWER operation will not violate the design assumptions of the accident analysis. In MODE 2, the limits must also be maintained to ensure startup and subcritical accidents (such as the uncontrolled CEA or group withdrawal) will not violate the assumptions of the accident analysis. In MODES 3, 4, 5, and 6, this LCO is not applicable, since no Design Basis Accidents (DBAs) using the MTC as an analysis assumption are initiated from these MODES. However, the variation of the MTC with temperature in MODES 3, 4, and 5, for DBAs initiated in MODES 1 and 2, is accounted for in the subject accident analysis. The variation of the MTC with temperature assumed in the safety analysis is accepted as valid once the BOC and MOC measurements are used for normalization.

ACTIONS

A.1

MTC is a function of the fuel and fuel cycle design and cannot be controlled directly once their designs have been implemented in the core. If MTC exceeds its limits, the reactor must be placed in MODE 3 with a minimum SHUTDOWN MARGIN. This eliminates the potential for violation of the accident analysis bounds. The associated Completion Time of 6 hours is reasonable considering the probability of an accident occurring during the time period which would require a MTC value within the LCO limits and the length of time required to reach MODE 3 conditions from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

The SRs for measurement of the MTC at the beginning and middle of each fuel cycle provide for confirmation of the limiting MTC values. The MTC changes smoothly from most positive (least negative) to most negative value during fuel cycle operation as the RCS boron concentration is reduced to compensate for fuel depletion. The requirement for measurement prior to operation above 5% of RTP satisfies the confirmatory check on the most positive (least negative) MTC

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

value. The requirement for measurement within 7 days after reaching 40 effective full power days and $\frac{2}{3}$ core burnup satisfies the confirmatory check of the most negative MTC value. The measurement is performed at any THERMAL POWER so that the projected EOC MTC may be evaluated before the reactor actually reaches the EOC condition. MTC values may be extrapolated and compensated to permit direct comparison to the specified MTC limits.

The SR is modified by a Note that states SR 3.0.4 is not applicable for entering MODE 2. Although this surveillance is applicable in MODE 2, the reactor must be critical before the surveillance can be completed. Therefore, entry into MODE 2 prior to accomplishing the surveillance is necessary.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 11, "Reactor Inherent Protection."
2. [Unit Name] FSAR, Section [ ], "[Title]."
3. [Unit Name] FSAR, Section [ ], "[Title]."
4. [Unit Name] FSAR, Section [ ], "[Title]."
5. [Unit Name] Core Operating Limits Report, "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Control Element Assembly (CEA) Alignment (Analog)

BASES

BACKGROUND

The OPERABILITY of the shutdown and regulating CEAS are initial assumptions in all safety analyses which assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analysis, which directly affects core power distributions and assumptions of available SHUTDOWN MARGIN (SDM).

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," GDC 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Plants" (Ref. 2).

Mechanical or electrical failures may cause a CEA to become inoperable or to become misaligned from its group. CEA inoperability or misalignment may cause increased power peaking due to the asymmetric reactivity distribution and a reduction in the total available CEA worth for reactor shutdown. Therefore CEA alignment and OPERABILITY are related to core operation in design power peaking limits and the core design requirement of a minimum SDM.

Limits on CEA alignment and OPERABILITY have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking and SDM limits are preserved.

CEAs are moved by their control element drive mechanisms (CEDMs). Each CEA drive mechanism moves its CEA 1 step (approximately [$\frac{3}{4}$] inches) at a time but at varying rates (steps per minute) depending on the signal output from the Rod Control System.

The CEAs are arranged into groups that are radially symmetric. Therefore, movement of the CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

reactor trip. The regulating CEAs also provide reactivity (power level) control during normal operation and transients. Their movement may be automatically controlled by the Reactor Regulating System.

The axial position of shutdown and regulating CEAs is indicated by two separate and independent systems, which are the Plant Computer CEA Position Indication System and the Reed Switch Position Indication System.

The Plant Computer CEA Position Indication System counts the commands sent to the CEA gripper coils from the CEDM Control System that moves the CEAs. There is a 1 step counter for each group of CEAs. Individual CEAs in a group all receive the same signal to move and should, therefore, all be at the same position indicated by the group step counter for that group. Plant Computer CEA Position Indication System is considered highly precise (± 1 step or ± $\frac{3}{4}$ inch). If a CEA does not move 1 step for each command signal, the step counter will still count the command and incorrectly reflect the position of the CEA.

The Reed Switch Position Indication System provides a highly accurate indication of actual CEA position, but at a lower precision than the step counters. This system is based on inductive analog signals from a series of reed switches spaced along a tube with a center-to-center distance of 1.5 inches, which is 2 steps. To increase the reliability of the system, there are redundant reed switches at each position.

APPLICABLE SAFETY ANALYSES

CEA misalignment accidents are analyzed in the safety analysis (Ref. 4). The accident analysis defines CEA misoperation as any event, with the exception of sequential group withdraws, which could result from a single malfunction in the Reactivity Control System. For example, CEA misalignment may be caused by a malfunction of the CEDM or CEDM Control System, or by operator error. A stuck CEA may be caused by mechanical jamming of the CEA fingers or of the gripper. Inadvertent withdrawal of a single CEA may be caused by the opening of the electrical circuit of the CEDM holding coil for a full-length or part-length CEA. A

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

dropped CEA subgroup could be caused by an electrical failure in the CEA coil power programmers.

The acceptance criteria for addressing CEA inoperability/misalignment is that there be no violations of:

a. Specified acceptable fuel design limits;

b. Centerline fuel temperature;

c. Reactor Coolant System (RCS) pressure boundary damage; and

d. The core must remain subcritical after accident transients.

Three types of misalignment are distinguished in the safety analysis (Ref. 4). During movement of a group, one CEA may stop moving while the other CEAs in the group continue. This condition may cause excessive power peaking. The second type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition requires an evaluation to determine that sufficient reactivity worth is held in the remaining CEAs to meet the SDM requirement with the maximum worth CEA stuck fully withdrawn. If a CEA is stuck in the fully withdrawn position, its worth is added to the SDM, since the safety analysis does not take two stuck CEAs into account. The third type of misalignment occurs when one CEA drops partially or fully into the reactor core. This event causes an initial power reduction followed by a return towards the original power, due to positive reactivity feedback from the negative moderator temperature coefficient. Increased peaking during the power increase may result in excessive local linear heat rates (LHRs).

Two types of analysis are performed in regard to static CEA misalignment (Ref. 3). With CEA banks at their insertion limits, one type of analysis considers the case when any one CEA is inserted [ ] inches into the core. The second type of analysis considers the case of a single CEA withdrawn [ ] inches from a bank inserted into its insertion limit. Satisfying limits on departure from

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

nucleate boiling ratio in both of these cases bounds the situation when a CEA is misaligned from its group by [7] inches.

Another type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition is assumed in the evaluation to determine that the required SDM is met with the maximum worth CEA also fully withdrawn (Ref. 5).

Since the CEA drop incidents result in the most rapid approach to specified acceptable fuel design limits (SAFDL) caused by a CEA misoperation the accident analysis analyzed a single full-length CEA drop, a single part-length CEA drop, and a part-length CEA subgroup drop. The most rapid approach to the departure from nucleate boiling SAFDL may be caused by a single full length CEA drop or a CEA subgroup drop depending upon initial conditions.

All of the above CEA misoperations will result in an automatic reactor trip. In the case of the full-length CEA drop a prompt decrease in core average power and a distortion in radial power are initially produced, which when conservatively coupled, results in a local power and heat flux increase, and a decrease in DNB parameters.

The results of the CEA misoperation analysis show that during the most limiting misoperation events, no violations of the SAFDLs, centerline fuel temperature, or RCS pressure occur.

Shutdown and regulating CEA OPERABILITY and alignment are directly related to power distributions and SDMS, which are initial conditions assumed in safety analyses. Therefore they satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The limit on shutdown and regulating CEA alignments assure that the assumptions in the safety analysis will remain valid. The requirements on OPERABILITY assure that upon reactor trip, the assumed reactivity will be available and will be inserted. The OPERABILITY requirements also assure

(continued)

(continued)

BASES (continued)

LCO (continued)

that the CEA banks will move correctly upon command to maintain the correct power distribution and CEA alignment.

The requirement to maintain the CEA alignment to within 7 inches between the highest and lowest CEAs in a subgroup is conservative. The minimum misalignment assumed in safety analysis is [15 inches], and in some cases a total misalignment from fully withdrawn to fully inserted is assumed.

CEAs are OPERABLE when they meet the SRs of this LCO and can be inserted and withdrawn to meet the alignment limits, sequence and overlap withdrawal requirements, CEA drop times, and position indication requirements. Also, [for this facility, an OPERABLE CEA motion inhibit and CEA deviation circuit constitute the following:].

Furthermore, [for this facility, an OPERABLE Plant Computer CEA Position Indication System (if required) and Reed Switch Indication System constitute the following:]

[For this facility, the following support systems are required OPERABLE to ensure CEA OPERABILITY, including CEA motion inhibit and CEA deviation circuit:]

[For this facility, the required support systems which upon their failure do not declare the CEA inoperable (including CEA motion inhibit and CEA deviation circuit) and their justification are as follows:]

Failure to meet the requirements of this LCO may produce unacceptable power peaking factors and LHRs, or unacceptable SDMS, all of which may constitute initial conditions inconsistent with the safety analysis.

APPLICABILITY

The requirements on CEA OPERABILITY and alignment are applicable in MODES 1 and 2 because these are the only MODES in which neutron (or fission) power is generated, and the OPERABILITY and alignment of CEAs has the potential to affect the safety of the plant. In MODES 3, 4, 5, and 6, the alignment limits do not apply because the CEAs are bottomed and the reactor is shutdown and not producing fission power. In the shutdown MODES, the OPERABILITY of

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

the shutdown and regulating CEAs has the potential to affect the required SDM, but this effect can be compensated for by an increase in the boron concentration of the RCS. See LCO 3.1.1 for SDM in MODES 3, 4, and 5, and LCO 3.9.1 for boron concentration requirements during refueling.

A Note has been added to i[illegible]icate that for this LCO, Conditions A, B, an[illegible]ted as an entity with a single Completion [illegible]

ACTIONS

A.1, A.2.1, and A.2.2

A CEA is inoperable if it will not move in response to signals from the CEDM Control System. A CEA may become inoperable yet remain trippable. In this condition the CEA can still perform its required function of adding negative reactivity should a reactor trip be necessary. If a CEA is inoperable but trippable, continued operation in MODES 1 and 2 may continue provided the position of the inoperable CEA does not result in unacceptable peaking factors. This is accomplished by verifying that the CEA is either fully withdrawn (Shutdown CEA) (see LCO 3.1.6), and if in regulating group [5], the CEA is within the long-term steady-state insertion limits of LCO 3.1.7. Also, if it is a regulating CEA, it is verified that the CEA is positioned within [7] inches (indicated reed switch position) of all other CEAs in its group. The 1-hour Completion Time ensures an acceptable CEA alignment is established before xenon redistribution can generate unacceptable peaking factors.

B.1, B.2, B.3.1, and B.3.2

With one or more full-length regulating CEAs misaligned from other CEAs in its group by > [7] inches and ≤ [15] inches AND all full-length shutdown and regulating CEAs trippable, THERMAL POWER is reduced to ≤ 70% RTP within 1 hour. Power operation may continue as long as the misaligned regulating CEA can be aligned to all the other CEAs in the group within 1 hour, OR all the other CEAs within limits in the group are aligned to within [7] inches of the misaligned CEAs within 2 hours while maintaining the insertion and sequence limits of LCO 3.1.7.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER to ≤ 70% RATED THERMAL POWER (RTP) ensures acceptable power distributions are maintained (Ref. 6). For small misalignments (less than 15 inches) of the CEAs, there is:

a. A small effect on the time-dependent long-term power distributions relative to those used in generating LCOs and limiting safety system settings (LSSS) setpoints;

b. A small effect on the available SDM; and

c. A small effect on the ejected CEA worth used in the accident analysis.

Therefore, a 1-hour time period is sufficient to:

a. Identify causes of a misaligned CEA;

b. Take appropriate corrective action to realign the CEAs; and

c. Minimize the effects of xenon redistribution.

With a large CEA misalignment (≥ [15] inches), however, this misalignment would cause distortion of the core power distribution. This distribution may, in turn, have a significant effect on:

a. The available SDM;

b. The time-dependent long-term power distributions relative to those used in generating LCOs and LSSS setpoints; and

c. The ejected CEA worth used in the accident analysis.

Therefore, prompt reduction in power is required to eliminate a large misalignment.

Power operations may continue provided adequate SDM exists and the CEAs can be properly aligned. This may be accomplished by aligning the OPERABLE CEAs to the inoperable CEA (subgroup). Since the CEA may be misaligned by greater

(continued)

(continued)

ACTIONS (continued)

than [15 inches], a SDM verification is made. Subsequently, maintaining the insertion and sequence limits of LCO 3.1.6 and LCO 3.1.7 ensures that adequate SDM and proper power distribution are maintained. The 1-hour Completion Time to align the OPERABLE CEAs to provides the operator 1-hour to properly align the OPERABLE CEAs to the CEA (subgroup).

C.1

In most cases, when more than one CEA is found to trippable and aligned but immovable, the malfunction can be traced to the Reactor Regulating System. Since the majority of Reactor Regulating System malfunctions can be repaired without reactor shutdown, and since the unit conditions are not outside any accident analysis assumptions, the appropriate action is to locate the malfunction and restore the rods to an OPERABLE status. Maintaining the sequence, insertion, and power limits of LCO 3.1.6 and LCO 3.1.7 ensures that core design limits are not exceeded. Since a Completion Time of 72 hours provides adequate time to locate the malfunction as well to obtain parts and perform the repairs, if the malfunction is not corrected in 72 hours it would be indicative of additional problems and plant shutdown would be required.

D.1 and D.2

If more than one full-length regulating CEA is misaligned in more than one group, it may indicate serious problems with CEAs and their support systems and may place the plant outside the accident analysis. Therefore, LCO 3.0.3 must be immediately entered.

Continued operation is not allowed in the case of:

a. More than one regulating CEA inoperable or misaligned from any other CEA in its group by more than 15 inches in one or more CEA groups; or

b. One or more CEAs inoperable as the result of excessive friction or mechanical interferences or known to be untrippable.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

This is because either of these conditions may be indicative of a possible loss of mechanical functional capability of the CEAs and, in the event of a stuck or untrippable CEA, a loss of SDM.

If a CEA is inoperable as a result of excessive friction or mechanical interference or is untrippable, it is not available for reactivity insertion during a reactor trip. With an untrippable CEA, meeting the insertion limits of LCO 3.1.6 and LCO 3.1.7 does not ensure that adequate SDM exists. In this condition, an additional allowance must be made for the worth of the affected CEA when calculating the available SDM.

This is necessary since the OPERABLE CEAs must still meet the single failure criteria. If additional negative reactivity is required to provide the necessary SDM, it must be provided by increasing the RCS boron concentration. One hour allows sufficient time to perform the SDM calculation and make any required boron adjustment to the RCS. The 6-hour Completion Time to reach MODE 3 is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

<u>E.1, E.2.1, and E.2.2</u>

The CEA Motion Inhibit permits CEA motion within the requirements of LCO 3.1.7 and prevents Regulating CEAs from being misaligned from other CEAs in the group.

Performing SR 3.1.5.1, CEA position, within 1 hour and every 4 hours thereafter is considered acceptable in view of other information continuously available to the operator in the control room so that during actual CEA motion deviations can be detected and the protection afforded by the CEA deviation circuits.

With the CEA motion inhibit inoperable, 6 hours are allowed to restore the CEA Motion Inhibit to OPERABLE status <u>OR</u> place and maintain the CEA drive switch in either the "Off" or "Manual" position and fully withdraw all CEAs in groups [3] and [4] and withdraw all CEAs in group [5] to less than [5]% insertion.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Placing the CEA drive switch in the "Off" or "Manual" position ensures the CEAs will not move in response to Reactor Regulating System automatic motion commands. Withdrawal of the CEAs to the positions required in the Required Action E.2.2 ensures that core perturbations in local burnup, peaking factors, and SDM will not be more adverse than the Conditions assumed in the safety analyses and LCO setpoint determination (Ref. 7).

The 6-hours Completion Time takes into account Required Action D.1, the protection afforded by the CEA deviation circuits, and other information continuously available to the operator in the control room so that during actual CEA motion, deviations can be detected.

A Note has been added to Required Action E.2.2 to indicate that fully withdrawing all CEAs in Group(s) [3] and [4], and withdrawing all CEAs in Group [5] to less than [5]% insertion, is allowed if this Required Action is not in conflict with Required Actions B.3.1, B.3.2, and D.2 when these Required Actions are being executed.

F.1

When the CEA deviation circuit is inoperable, performing SR 3.1.5.1, CEA position, within 1 hour and every 4 hours thereafter ensures improper CEA alignments are identified before unacceptable flux distributions occur. The specified Completion Times take into account other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected, and protection can be provided by the CEA motion inhibit and deviation circuits.

G.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed time (6 hours) is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

Verification that individual CEA indicated reed switch positions are within 7 inches (indicated reed switch positions) of all other CEAs in the group at a 12-hour Frequency allows the operator to detect a CEA beginning to deviate from its expected position. The specified Frequency takes into account other CEA position information that is continuously available to the operator in the control room, so that during CEA movement, deviations can be detected and protection can be provided by the CEA motion inhibit and deviation circuits. [For this facility, each CEA Reed Switch Indication System is considered inoperable if it has [ ] individual reed switches inoperable.]

SR 3.1.5.2

OPERABILITY of at least two CEA position indicator channels is required to determine CEA positions and thereby ensure compliance with the CEA alignment and insertion limits. The CEA "full in" and "full out" limits provide an additional independent means for determining the CEA positions when the CEAs are at either their fully inserted or fully withdrawn positions. [For this facility, each CEA Reed Switch Indication System is considered inoperable if it has [ ] individual reed switches inoperable.]

The 12-hour Frequency takes into consideration other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected and protection can be provided by the CEA motion inhibit and deviation circuits.

SR 3.1.5.3

Demonstrating the CEA motion inhibit OPERABLE verifies that the CEA motion inhibit is functional even if it is not regularly operated. The 31-day Frequency takes into account other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected and protection can be provided by the CEA deviation circuits.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.5.4

Demonstrating the CEA deviation circuit is OPERABLE verifies the circuit is functional. The 31-day Frequency takes into account other information continuously available to the operator in the control room, so that during CEA movement, deviations can be detected and protection can be provided by the CEA motion inhibit.

SR 3.1.5.5

Exercising individual CEAs that are not fully inserted into the reactor core every 92 days verifies that all CEAs continue to be OPERABLE even if they are not regularly moved. A movement of [5] inches is adequate to demonstrate motion without exceeding the alignment limit when only one CEA is being moved. The 92-days Frequency takes into consideration other information available to the operator in the control room and other surveillances being performed more frequently which add to the determination of OPERABILITY of the CEAs.

SR 3.1.5.6

Verification of CEA drop times determines that the maximum CEA drop time permitted is consistent with the assumed drop time used in the safety analysis (Ref. 8). Measuring drop times prio [illegible] ctor criticality after reactor vessel head removal ass [illegible] e reactor internals and CEDM will not interfere with CEA motion or drop time. Also, every 18 months the CEA drop times are verified to ensure that no degradation in these systems has occurred that would adversely affect CEA motion or drop time. Individual CEAs whose drop times are greater than safety analysis assumptions are not OPERABLE. The 18-month Frequency was developed because it was considered prudent that this surveillance only be performed during a plant outage. This is due to the plant conditions needed to perform the SR and the potential for an unplanned plant transient if the surveillance is performed with the reactor at power. Operating experience has shown that these components usually pass this surveillance when performed on the 18-month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

The drop time is defined as the time the electrical power is interrupted to the CEA drive mechanism until the CEA reaches 90% insertion. The testing is performed with all reactor coolant pumps operating and average RCS temperature ≥ [ ]°F to simulate a trip under actual operating conditions.

SR 3.1.5.7

Performance of a CHANNEL FUNCTIONAL TEST of each reed switch position transmitter channel ensures the channel is OPERABLE and capable of indicating CEA position over the entire length of the CEAs travel. Since this test must be performed when the reactor is shut down, an 18-month Frequency to be coincident with refueling outage was selected. Operating experience has shown that these components usually pass this surveillance when performed with the 18-month Frequency. Furthermore, the Frequency takes into account other surveillances being performed at shorter Frequencies, which determine the OPERABILITY of the CEA Reed Switch Indication System.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," and General Design Criterion 26, "Reactivity Limits."
2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
3. [Unit Name] FSAR, Section [ ], "[Title]."
4. [Unit Name] FSAR, Section [ ], "[Title]."
5. [Unit Name] FSAR, Section [ ], "[Title]."
6. [Unit Name] FSAR, Section [ ], "[Title]."
7. [Unit Name] FSAR, Section [ ], "[Title]."
8. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.6 Shutdown Control Element Assembly (CEA) Insertion Limits (Analog)

BASES

BACKGROUND

The insertion limits of the shutdown and regulating CEAs are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions and assumptions of available SHUTDOWN MARGIN (SDM), ejected CEA worth, and initial reactivity insertion rate.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and GDC 26 "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2). Limits on shutdown CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the reactivity limits, ejected CEA worth, and SDM limits are preserved.

The CEAs are arranged into groups that are radially symmetric. Therefore, movement of the CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a reactor trip. The regulating CEAs also provide reactivity (power level) control during normal operation and transients. Their movement may be automatically controlled by the Reactor Regulating System.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are normally automatically controlled by the Reactor Regulating System, but they can also be manually controlled. They are capable of adding negative reactivity very quickly (compared to borating). The Regulating CEAs must be maintained above designed insertion limits and are typically near the fully withdrawn position during normal full power operations. Hence, they are not capable of adding a large amount of positive reactivity. Boration or dilution of the Reactor Coolant System (RCS) compensates for the reactivity changes associated with large changes in RCS temperature.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The shutdown CEAs are used primarily to help ensure that the required SDM is maintained. The shutdown CEAs are controlled manually or automatically by the control room operator. During normal unit operation, the shutdown CEAs are fully withdrawn. The shutdown CEAs must be completely withdrawn from the core prior to withdrawing any regulating CEAs during an approach to criticality. The shutdown CEAs are then left in this position until the reactor is shut down. They add negative reactivity to shut down the reactor upon receipt of a reactor trip signal.

APPLICABLE SAFETY ANALYSES

On a reactor trip, all CEAs (shutdown and regulating), except the most reactive CEA, are assumed to insert into the core. The shutdown CEAs shall be at their insertion limits and available to insert the maximum amount of negative reactivity on a reactor trip signal. The regulating CEAs may be partially inserted in the core as allowed by LCO 3.1.7, "Regulating Control Element Assembly (CEA) Insertion Limits." The shutdown CEA insertion limit is established to ensure that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM (see LCO 3.1.1) following a reactor trip from full power. The combination of regulating CEAs and shutdown CEAs (less the most reactive CEA, which is assumed to be fully withdrawn) is sufficient to take the reactor from full power conditions at rated temperature to zero power and to maintain the required SDM at rated no-load temperature (Ref. 3). The shutdown CEA insertion limit also limits the reactivity worth of an ejected shutdown CEA.

The acceptance criteria for addressing shutdown and regulating CEA insertion limits and inoperability or misalignment is that:

a. There be no violation of:

   1. specified acceptable fuel design limits,

   2. centerline fuel temperature, and

   3. RCS pressure boundary damage; and

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

b. The core must remain subcritical after accident transients.

As such, the shutdown CEA insertion limits affect safety analyses involving core reactivity, ejected CEA worth, and SDM (Ref. 3).

Shutdown CEA insertion limits preserve an initial condition assumed in the safety analyses and, as such, satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The shutdown CEAs must be within their insertion limits any time the reactor is critical or approaching criticality. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip.

[For this facility, an OPERABLE shutdown CEA is verified as follows:]

[For this facility, the following support systems are required OPERABLE to ensure shutdown CEA insertion limits are met and are OPERABLE: [LIST]]

[For this facility, the required support systems which, upon their failure, do not result in the shutdown CEAs not meeting their insertion limits or in CEA inoperability and their justification are as follows:] [List and Explain]

APPLICABILITY

The Shutdown CEAs must be within their insertion limits with the reactor in MODES 1 and 2. The Applicability in MODE 2 begins within 15 minutes prior to initial regulating CEA withdrawal during an approach to criticality and continues throughout MODE 2 until all regulating CEAs are again fully inserted by scram or during shutdown. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip. The reactor is not critical or approaching criticality in MODE 3, 4, 5, or 6 and, therefore, the shutdown CEAs must be fully inserted.

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

This LCO has been modified by a Note that suspends the LCO requirement during SR 3.1.5.5, which assures the freedom of the CEAs to move. This SR requires the shutdown CEAs to move below the LCO limits, which would normally violate the LCO.

ACTIONS

A.1

With the SDM reduced by the insertion of a shutdown CEA, the operator can no longer rely on the regulating CEAs being above the transient insertion limit to ensure adequate SDM exists. Initiation of boration within 15 minutes is required since the SDM in MODES 1 and 2 is no longer ensured by adhering to the regulating and safety CEA insertion limits (see LCO 3.1.1).

In the event that the shutdown CEA Position Indication System is found to be inoperable, the shutdown CEA is considered to be not within limits and Required Action A.2 applies.

A.2

Accident analysis assumes that the shutdown CEAs are fully withdrawn any time the reactor is critical. This ensures that:

a. The minimum SDM is maintained; and

b. The potential effects of a CEA ejection accident are limited to acceptable limits.

CEAs are considered fully withdrawn at 129 inches, since this position places them outside the active region of the core. The required Completion Time of 1 hour to fully withdraw the Shutdown CEA allows the operator adequate time to adjust the CEA in an orderly manner and is consistent with the required Completion Time for Action A.1 in LCO 3.1.5, "CEA Alignment."

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

B.1

When the Required Action of A.2 cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The 6-hour Completion Time is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

Verification that the shutdown CEAs are within their insertion limits within 15 minutes prior to an approach to criticality ensures that when the reactor is critical, or being taken critical, the shutdown CEAs will be available to shut down the reactor and the required SDM will be maintained following a reactor trip. This SR and Frequency ensure that the shutdown CEAs are withdrawn before the regulating CEAs are withdrawn during a unit startup.

Since the shutdown CEAs are positioned manually by the control room operator, a verification of shutdown CEA position at a frequency of 12 hours after the reactor is taken critical is adequate to ensure that they are within their insertion limits. Also, the 12-hour Frequency takes into account other information available to the operator in the control room that monitors the status of the shutdown CEAs.

SR 3.1.6.1 is modified by a Note that allows exemption to SR 3.0.4 for entering MODE 2. SR 3.0.4 is not applicable before entering the Applicability Condition of "within 15 minutes prior to initial regulating CEA withdrawal," because the surveillance is specifically selected to be concurrent with the Applicability.

[For this facility, an OPERABLE shutdown CEA within limits is verified as follows:]

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," and General Design Criterion 26, "Reactivity Limits."
2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
3. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Regulating Control Element Assembly (CEA) Insertion Limits (Analog)

BASES

BACKGROUND

The insertion limits of the shutdown and regulating CEAs are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions and assumptions of available SHUTDOWN MARGIN (SDM) and initial reactivity insertion rate. The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10 "Reactor Design," GDC 26 "Reactivity Limits" (Ref. 1), and 10 CFR Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors" (Ref. 2).

Limits on regulating CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking, ejected CEA worth, reactivity insertion rate, and SDM limits are preserved.

The regulating CEA groups operate with a predetermined amount of position overlap in order to approximate a linear relation between CEA worth and CEA position (integral CEA worth). The regulating CEA groups are withdrawn and operate in a predetermined sequence. The Reactor Regulating System controls reactivity by moving the regulating groups in sequence within analyzed ranges. The group sequence and overlap limits are specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3).

The Regulating CEA are used for precise reactivity control of the reactor. The positions of the regulating CEA are normally controlled automatically by the Reactor Regulating System but can also be manually controlled. They are capable of adding reactivity very quickly (compared to borating or diluting).

The power density at any point in the core must be limited to maintain specified acceptable fuel design limits, including limits that preserve the criteria specified in 10 CFR 50.46 (Ref. 2). Together, LCO 3.1.7, LCO 3.2.4, and

(continued)

(continued)

BACKGROUND (continued)

LCO 3.2.5 provide limits on control component operation and on monitored process variables to ensure the core operates within the linear heat rate (LHR) (LCO 3.2.1), total planar radial peaking factor (F_{xy}^T) (LCO 3.2.2), and total integrated radial peaking factor, F_r^T (LCO 3.2.3) limits in the COLR. Operation within the LHR limits given in the COLR prevents power peaks that would exceed the loss-of-coolant accident (LOCA) limits derived by the Emergency Core Cooling System analysis. Operation within the F_{xy}^T and F_r^T limits given in the COLR prevents departure from nucleate boiling (DNB) during a loss of forced reactor coolant flow accident. In addition to the LHR, F_{xy}^T and F_r^T limits, certain reactivity limits are preserved by regulating CEA insertion limits. The regulating CEA insertion limits also restrict the ejected CEA worth to the values assumed in the safety analysis and preserve the minimum required SDM in MODES 1 and 2.

The establishment of limiting safety system settings and LCOs require that the expected long- and-short-term behavior of the radial peaking factors be determined. The long term behavior relates to the variation of the steady-state radial peaking factors with core burnup and is affected by the amount of CEA insertion assumed, the portion of a burnup cycle over which such insertion is assumed, and the expected power level variation throughout the cycle. The short-term behavior relates to transient perturbations to the steady state radial peaks due to radial xenon redistribution. The magnitudes of such perturbations depend upon the expected use of the CEAs during anticipated power reductions and load maneuvering. Analyses are performed based on the expected mode of operation of the Nuclear Steam Supply System (base-loaded, maneuvering, etc.). From these analyses CEA insertions are determined and a consistent set of radial peaking factors defined. The long-term steady-state and short-term insertion limits are determined based upon the assumed mode of operation used in the analyses and provide a means of preserving the assumption on CEA insertions used. The long- and short-term insertion limits of LCO 3.1.7 are specified for the plant that has been designed primarily for base-loaded operation, but which has the ability to accommodate a limited amount of load maneuvering.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The shutdown and regulating CEA insertion and alignment limits are process variables that together characterize and control the three-dimensional power distribution of the reactor core. Additionally, the regulating bank insertion limits control the reactivity that could be added in the event of a CEA ejection accident, and the shutdown and regulating bank insertion limits assure the required SDM is maintained.

Operation within the subject LCO limits will prevent fuel cladding failures that would breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a LOCA, loss of flow, ejected CEA, or other accident requiring termination by a Reactor Trip System trip function.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition I) and anticipated operational occurrences (Condition II). The acceptance criteria for the regulating CEA insertion, AXIAL SHAPE INDEX (ASI), and AZIMUTHAL POWER TILT (T_q) LCOs are such as to preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a large-break LOCA, the peak cladding temperature must not exceed a limit of 2200°F (10 CFR 50.46, Ref. 2);

b. During a loss of forced reactor coolant flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition. This is referred to hereafter as the 95/95 DNB criterion;

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed [illegible] cal/g (Ref. 4); and

d. The CEA must be capable of shutting down the reactor with a minimum required SDM with the highest worth CEA stuck fully withdrawn (GDC 26, Ref. 1).

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSIS (continued)

Regulating CEA position, ASI, and T_q are process variables that together characterize and control the three-dimensional power distribution of the reactor core.

Fuel cladding damage does not occur when the core is operated outside these LCOs during normal operation. However, fuel cladding damage could result should an accident occur with simultaneous violation of one or more of these LCOs. Changes in the power distribution can cause increased power peaking and corresponding increased local LHR.

The SDM requirement is assured by limiting the regulating and shutdown CEA insertion limits so that the allowable inserted worth of the CEAs is such that sufficient reactivity is available to shut down the reactor to hot zero power. SDM assumes the maximum worth CEA remains fully withdrawn upon trip (Ref. 5).

Operation at the insertion limits or ASI limits may approach the maximum allowable linear heat generation rate or peaking factor with the allowed T_q present. Operation at the insertion limit may also indicate the maximum ejected CEA worth could be equal to the limiting value in fuel cycles which have sufficiently high ejected CEA worths.

The regulating and shutdown CEA insertion limits ensure that safety analyses assumptions for reactivity insertion rate, SDM, ejected CEA worth, and power distribution peaking factors are preserved (Ref. 6).

The insertion limits satisfy Criterion 2 of the NRC Interim Policy Statement, in that they are initial conditions assumed in the safety analysis.

LCO

The limits on shutdown and regulating CEAs sequence, overlap, and physical insertion as defined in the COLR (Ref. 3) must be maintained, because they serve the function of preserving power distribution, ensuring that the SDM is

(continued)

(continued)

BASES (continued)

LCO (continued)	maintained, ensuring that ejected CEA worth is maintained, and ensuring adequate negative reactivity insertion on trip. The overlap between regulating banks provides more uniform rates of reactivity insertion and withdrawal and is imposed to maintain acceptable power peaking during regulating CEA motion. [For this facility, an OPERABLE power-dependent insertion limit (PDIL) alarm circuit and regulating CEA group constitute the following:] [For this facility, the following support systems are required OPERABLE to ensure PDIL alarm circuit and regulating CEA group OPERABILITY:] [For this facility, the required support systems which upon their failure do not declare the PDIL alarm circuit and regulating CEA group inoperable and their justification are as follows:]
APPLICABILITY	The shutdown and regulating CEA sequence, overlap, and physical insertion limits shall be maintained with the reactor in MODE 1 and MODE 2. These limits must be maintained since they preserve the assumed power distribution, ejected CEA worth, SDM, and reactivity rate insertion assumptions. Applicability in MODES 3, 4, and 5 is not required, since neither the power distribution nor ejected CEA worth assumptions would be exceeded in these MODES. SDM is preserved in MODES 3, 4, and 5 by adjustments to the soluble boron concentration. This LCO has been modified by a Note that permits the requirements of this LCO to be not applicable during the performance of SR 3.1.5.5. This SR requires that the CEA be moved at least every 92 days to verify their OPERABILITY. The individual CEAs are moved at least 5 inches and then returned to their original position. A Note has been added to indicate that the Completion Time is on a Condition basis.

(continued)

BASES (continued)

ACTIONS

A.1, A.2.1 and A.2.2

Operation beyond the transient insertion limits results in a loss of SDM and excessive peaking factors. Restoration of the required SDM requires increasing the Reactor Coolant System (RCS) boron concentration, because the regulating CEAs may be inserted too far to provide sufficient negative reactivity. RCS boration must occur as described in Section B 3.1.1. The required Completion Time of 15 minutes to initiate boration is reasonable, based on limiting the potential xenon redistribution, the low probability of an accident occurring, and the steps required to complete the action. This allows the operator sufficient time to align the required valves and to start the boric acid pumps. Boration will continue until the regulating CEA group positions are restored to at least within the restricted operation region, which restores the minimum SDM capability. While boron addition to the RCS should be initiated within 15 minutes to ensure adequate SDM, the CEAs must be returned to above the transient insertion limits to eliminate the peaking problem. This can be accomplished by either restoring the CEAs to within the insertion limits or reducing THERMAL POWER to less than or equal to that fraction of RATED THERMAL POWER (RTP) that is allowed by CEA group position using the limits specified in the COLR. The Completion Time of 2 hours is reasonable based on the low probability of an event occurring simultaneously with the limit out of specification, and on limiting the potential xenon redistribution.

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action A.2.1 or A.2.2 applies.

B.1

If the CEAs are inserted between the long-term steady-state insertion limits and the Transient Insertion Limits for intervals greater than 4 hours per 24-hour period, peaking factors can develop which are of immediate concern (Ref.7).

Verifying that the short-term steady-state insertion limits are not exceeded ensures that the peaking factors that do develop are within those allowed for continued operation.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

B.2

Experience has shown that rapid power increases in areas of the core in which the flux has been depressed can result in fuel damage, as the linear heat rate in those areas rapidly increases. Restricting the rate of THERMAL POWER increases to ≤ 5% RTP per hour following CEA insertion beyond the long-term steady-state insertion limits ensures the power transients experienced by the fuel will not result in fuel failure (Ref. 8).

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action B.2 applies.

C.1

With the Regulating CEAs inserted between the long-term steady-state insertion limit and the transient limit, and approaching the 5 effective full power days (EFPDs) per 30 EFPDs or 14 EFPDs per 365 EFPDs limits, the core is approaching the acceptable limits placed on operation with flux patterns outside those assumed in the long-term burnup assumptions (Ref. 9). In this case the CEAs must be returned to within the long-term steady-state insertion limits as soon as possible or the core must be placed in a Condition in which the abnormal fuel burnup can not continue. Two hours is allotted to return the CEAs to within the long-term steady-state insertion limits.

The required Completion Time of 2 hours from initial discovery of a regulating CEA group outside the limits until its restoration within the long-term steady-state limits shown on the figures in the COLR allows sufficient time for borated water to enter the RCS from the chemical addition and makeup systems, and to cause the regulating CEAs to withdraw to the acceptable region. Operation for another 2 hours outside the limits is reasonable, based on limiting the potential xenon redistribution, the low probability of an accident occurring, and the steps required to complete the action.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

D.1

When the PDIL alarm circuit is inoperable, SR 3.1.7.1 is performed, Regulating CEA group position, within 1 hour and once per 4 hours thereafter to ensure improper CEA alignments are identified before unacceptable flux distributions occur.

E.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed time (6 hours) is reasonable, based on operating experience, to reach MODE 3 from full power conditions in an orderly manner and without challenging plant systems. In MODE 3 the reactor is not critical and excessive power peaking cannot occur.

SURVEILLANCE REQUIREMENTS

SR 3.1.7.1

With the PDIL alarm circuit OPERABLE, verification of each regulating CEA group position every 12 hours is sufficient to detect CEA positions that may approach the limits, and to provide the operator with time to undertake the Required Action(s) should the sequence or insertion limits be found to be exceeded. The 12-hour Frequency also takes into account the indication provided by the PDIL Alarm Circuit and other information about CEA group positions available to the operator in the control room.

SR 3.1.7.1 is modified by a Note which allows exemption to SR 3.0.4. SR 3.0.4 is not applicable since the unit must be in the applicable MODES in order to perform surveillances which demonstrate the LCO limits are met.

SR 3.1.7.2

Verification of the accumulated time of CEA group insertion between the long-term steady-state insertion limits and the transient insertion limits assures the cumulative time limits are not exceeded. The 24-hour Frequency ensures the operator identifies a time limit that is being approached before it is reached.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

[For this facility, acceptable accumulated time of each CEA group insertion between the long-term steady-state insertion limits and the transient insertion limits is as follows:]

SR 3.1.7.3

Demonstrating the PDIL alarm circuit OPERABLE verifies that the PDIL alarm circuit is functional. The 31-day Frequency takes into account other surveillances being performed at shorter frequencies which identify improper CEA alignments.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criteria 10, "Reactor Design," and General Design Criterion 26, "Reactivity Limits."

2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Plants."

3. [Unit Name] Core Operating Limits Report, "[Title]."

4. [Unit Name] FSAR:

   a. Section [ ], "CEA Ejection Accident, Accident Bases."

   b. Section [ ], "CEA Ejection Accident, Fuel CEA Damage."

   c. Section [ ], "Thermal and Hydraulic Limits."

5. [Unit Name] FSAR, Section [ ], "[Title]."

6. [Unit Name] FSAR, Section [ ], "[Title]."

7. [Unit Name] FSAR, Section [ ], "[Title]."

8. [Unit Name] FSAR, Section [ ], "[Title]."

9. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1. REACTIVITY CONTROL SYSTEMS

B 3.1.8 Special Test Exception (STE)—SHUTDOWN MARGIN (SDM) (Analog)

BASES

BACKGROUND

The primary purpose of the MODES 2 and 3 STE is to permit relaxations of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are constructed to determine the control element assembly (CEA) worth and SDM.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC for the purpose of conducting tests and experiments are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Provide assurance that the facility has been adequately designed;

b. Validate the analytical models used in design and analysis;

c. Verify assumptions used for predicting plant response;

d. Provide assurance that installation of equipment in the facility has been accomplished in accordance with the design; and

e. Verify that operating and emergency procedures are adequate.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

To accomplish these objectives, testing prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at-power operation is required. The requirements for PHYSICS TESTS for reload fuel cycles assure that the operating characteristics of the core are consistent with the design predictions, and that the core can be operated as designed (Ref. 4).

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure design intent is met. PHYSICS TESTS are performed in accordance with these procedures, and test results are approved prior to continued power escalation and long-term power operation. Examples of PHYSICS TESTS include determination of critical boron concentration, CEA group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

The acceptance criteria to allow suspension of certain LCOs for PHYSICS TESTS are that fuel damage criteria are not exceeded. Even if an accident occurs during PHYSICS TESTS with one or more LCOs suspended, fuel damage criteria are preserved because adequate limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines the requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1985 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved.

In this test the following LCOs are suspended:

a. LCO 3.1.1, "Shutdown Margin—T_{avg} > 200°F";

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

b. LCO 3.1.5, "CEA Position Alignment"; and

c. LCO 3.1.7, "Regulating CEA Insertion Limits."

Therefore, this LCO places limits on the minimum amount of CEA worth required to be available for reactivity control when CEA worth measurements are performed.

The individual LCOs cited above govern CEA group height, insertion, and alignment. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature T_c, and pressurizer pressure contribute to maintaining departure from nucleate boiling (DNB) parameter limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss-of-coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 6). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

SRs are conducted as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these SRs allows PHYSICS TESTS to be conducted without decreasing the margin of safety. Requiring that shutdown reactivity equivalent to at least the highest estimated CEA worth be available for trip insertion from the OPERABLE CEA provides a high degree of assurance that shutdown capability is maintained for the most challenging postulated accident, a stuck CEA. Since LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," is suspended, however, there is not the same degree of assurance during this test that the reactor would always be shutdown if the highest worth CEA was stuck out and calculational uncertainties or the estimated highest CEA worth was not as expected (the single failure criteria is not met). This situation is judged acceptable, however, because specified acceptable fuel damage limits are still met. The risk of experiencing a stuck CEA and subsequent criticality is reduced during this PHYSICS TEST exception by the requirements to determine CEA positions every 2 hours; by the trip of each CEA to be withdrawn 24 hours prior to suspending the SHUTDOWN MARGIN;

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

and by ensuring that shutdown reactivity is available equivalent to the reactivity worth of the estimated highest worth CEA, Ref. 5.

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, azimuthal power tilt, and AXIAL SHAPE INDEX, which represent initial condition input (power peaking) to the accident analysis. Also involved are the movable control components (shutdown and regulating CEAs), which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the CORE OPERATING LIMITS REPORT (Ref. 6).

PHYSICS TESTS meet the criteria for inclusion in Technical Specifications, since the components and process variable LCOs suspended during PHYSICS TESTS meet Criteria 1, 2, and 3 of the NRC Interim Policy Statement.

LCO

This LCO provides that a minimum amount of CEA worth is immediately available for reactivity control when CEA worth measurement tests are performed. The STE is required to permit the periodic verification of the actual versus predicted core reactivity condition occurring as a result of fuel burnup or fuel cycling operations. The SDM requirements of LCO 3.1.1 and the regulating CEA insertion limits of LCO 3.1.7 may be suspended.

[For this facility, an OPERABLE CEA constitutes the following:]

[For this facility, the following support systems are required OPERABLE to ensure that the LCO and SR conditions are met: [List]]

[For this facility, the required support systems which upon their failure to do not result in CEA inoperability of the condition of this LCO to not be met and their justification are as follows: [List]]

(continued)

BASES (continued)

APPLICABILITY

This LCO is applicable in MODES 2 and 3. Although CEA worth testing is conducted in MODE 2, sufficient negative reactivity is inserted during the performance of these tests to result in temporary entry into MODE 3. Because the intent is to immediately return to MODE 2 to continue CEA worth measurements, the STE allows limited operation to 6 consecutive hours in MODE 3 without having to borate to meet the SDM requirements of LCO 3.1.1.

ACTIONS

A.1

With any CEA not fully inserted and less than the minimum required reactivity equivalent available for insertion, or with all CEAs inserted and the reactor subcritical by less than the reactivity equivalent of the highest worth CEA, restoration of the minimum SDM requirements must be accomplished by increasing the RCS boron concentration. The required Completion Time to initiate boration allows the operator sufficient time to align the valves and start the boric acid pumps and is consistent with the Completion Time of LCO 3.1.1.

In the event that any withdrawn CEA is found to be inoperable, the Required Action A.1 applies.

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

Verification of the position of each partially or fully withdrawn full-length or part-length CEA is necessary to ensure that the minimum negative reactivity requirements for insertion on a trip are preserved. A 2-hour Frequency is sufficient for the operation to verify that each CEA position is within the acceptance criteria.

SR 3.1.8.2

Prior demonstration that each CEA to be withdrawn from the core during PHYSICS TESTS is capable of full insertion when tripped from an at least 50% withdrawn position provides assurance that the CEA will insert on a trip signal. The

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

7-day requirement ensures that the CEAs are OPERABLE prior to reducing SDM to less than the limits of LCO 3.1.1.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix B, Section XI (Test Control), "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants."

2. Title 10, Code of Federal Regulations, Part 50.59, "Changes, Tests, and Experiments."

3. Regulatory Guide 1.68, Revision 2, "Initial Test Programs for Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission, August 1978.

4. ANSI/ANS-19.6.1-1985, "Reload Startup PHYSICS TESTS for Pressurized Water Reactors," American National Standards Institute, December 13, 1985.

5. [Unit Name] FSAR, Section [14], "[Testing Requirements]."

6. [Unit Name] Core Operating Limits Report, "[Title.]"

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.9 PHYSICS TEST Exceptions—MODES 1 & 2 (Analog)

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 special test exceptions is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine specific reactor core characteristics.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfacturily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC for the purpose of conducting tests and experiments are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Provide assurance that the facility has been adequately designed;

b. Validate the analytical models used in design and analysis;

c. Verify assumptions used for predicting plant response;

d. Provide assurance that installation of equipment in the facility has been accomplished in accordance with design; and

e. Verify that operating and emergency procedures are adequate.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

To accomplish these objectives, testing prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at-power operation is required. The requirements for PHYSICS TESTS for reload fuel cycles assure that the operating characteristics of the core are consistent with the design predictions, and that the core can be operated as designed (Ref. 4).

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long-term power operation. Examples of PHYSICS TESTS include determination of critical boron concentration, control element assembly (CEA) group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

It is acceptable to suspend certain LCOs for PHYSICS TESTS because fuel damage criteria are not exceeded. Even if an accident occurs during a PHYSICS TEST with one or more LCOs suspended, fuel damage criteria are preserved because the limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines the requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS-19.6.1-1985 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved even when the limits specified in the following LCOs are suspended:

a. LCO 3.1.4, "Moderator Temperature Coefficient (MTC)";

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

b. LCO 3.1.5, "CEA Alignment;"

c. LCO 3.1.6, "Shutdown CEA Insertion Limits;"

d. LCO 3.1.7, "Regulating CEA Insertion Limits;"

e. LCO 3.2.2, "Total Planar Radial Peaking Factor;"

f. LCO 3.2.3, "Total Integrated Radial Peaking Factor;" and

g. LCO 3.2.4, "AZIMUTHAL POWER TILT (T_q)."

The safety analysis (Ref. 7) places limits on allowable THERMAL POWER during PHYSICS TESTS and requires the LHR and the departure from nucleate boiling (DNB) parameter to be maintained within limits. The power plateau of < 85% RATED THERMAL POWER (RTP) and the associated trip setpoints are required to ensure [explain].

The individual LCOs governing CEA group height, insertion and alignment, AXIAL SHAPE INDEX (ASI), total planar radial peaking factor, total integrated radial peaking factor, and T_q preserve the LHR limits. Additionally, the LCOs governing Reactor Coolant System flow, reactor inlet temperature T_c, and pressurizer pressure contribute to maintaining DNB parameter limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss-of-coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 6). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

During PHYSICS TESTS, one or more of the LCOs that normally preserve the LHR and DNB parameters limits may be suspended. The results of the accident analysis are not impacted, however, if LHR and DNB parameters are verified to be within their limits while the LCOs are suspended. Therefore, SRs are placed as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Performance of these Surveillances allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, T_q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the movable control components (shutdown and regulating CEAs), which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 8).

PHYSICS TESTS meet the criteria for inclusion in the Technical Specifications, since the components and process variable LCOs suspended during PHYSICS TESTS meet Criteria 1, 2, and 3 of the NRC Interim Policy Statement.

LCO

This LCO permits individual CEAs to be positioned outside of their normal group heights and insertion limits during the performance of PHYSICS TESTS such as those required to:

a. Measure CEA worth;

b. Determine the reactor stability index and damping factor under xenon oscillation conditions;

c. Determine power distributions for non-normal CEA configurations;

d. Measure rod shadowing factors; and

e. Measure temperature and power coefficients.

Additionally, it permits the center CEA to be misaligned during PHYSICS TESTS required to determine the isothermal temperature coefficient, MTC, and power coefficient.

(continued)

(continued)

BASES (continued)

LCO (continued)

The requirement of LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, LCO 3.1.7, LCO 3.2.2, LCO 3.2.3, LCO 3.2.4 may be suspended during the performance of PHYSICS TESTS provided:

a. THERMAL POWER is restricted to test power plateau which shall not exceed 85% RTP, and

b. In MODE 1 > 20% RTP, the limits of LCO 3.2.1, "Linear Heat Rate (LHR)," are maintained and determined as specified in SR 3.1.9.1.

APPLICABILITY

This LCO is applicable in MODES 1 and 2 because the reactor must be critical at various THERMAL POWER levels to perform the PHYSICS TESTS described in the LCO section. Limiting the test power plateau to less than 85% of RTP ensures that LHRs are maintained within acceptable limits.

ACTIONS

A.1 and B.1

If THERMAL POWER exceeds the test power plateau, or the LHR requirements of LCO 3.2.1 are exceeded, THERMAL POWER must be reduced to restore the additional thermal margin provided by the reduced THERMAL POWER. The 15-minute Completion Time ensures that prompt action is taken to reduce THERMAL POWER to within acceptable limits.

C.1 and C.2

If Required Actions A.1 and B.1 cannot be completed within the required Completion Time, PHYSICS TESTS must be suspended within 1 hour and the reactor must be placed in MODE 3. Allowing 1 hour to suspend PHYSICS TESTS allows the operator sufficient time to change any abnormal CEA configuration back to within the limits of LCO 3.1.5, LCO 3.1.6, and LCO 3.1.7. Placing the reactor in MODE 3 within 6 hours increases thermal margin and is consistent with the Required Actions of the power distribution LCOs. The required Completion Time of 6 hours is adequate to perform a controlled shutdown in an orderly manner and without challenging plant systems, and is consistent with power distribution LCO Completion Times.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.1.9.1

Monitoring LHR continuously ensures that the limits are not exceeded. Refer to B 3.1.4, "Power Distribution Limits," for a discussion of the bases for these parameters. This surveillance is not applicable at < 20% RTP because adequate LHR margin exists below this power level and because the Incore Detector Monitoring System is not available below 20% RTP.

SR 3.1.9.2

Verifying that THERMAL POWER is equal to or less than that allowed by the test power plateau, as specified in the PHYSICS TEST procedure and required by the safety analysis, ensures that adequate LHR and DNB parameter margins are maintained while LCOs are suspended. The 1-hour Frequency is sufficient based on the slow rate of power change and increased operational controls in place during PHYSICS TESTS.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix B, Section XI (Test Control), "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants."

2. Title 10, Code of Federal Regulations, Part 50.59, "Changes, Tests, and Experiments."

3. Regulatory Guide 1.68, Revision 2, "Initial Test Programs for Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission, August 1978.

4. ANSI/ANS-19.6.1-1985, "Reload Startup Physics Tests for Pressurized Water Reactors," American National Standards Institute, December 13, 1985.

5. [Unit Name] FSAR, Section 14, "[Testing Requirements]."

6. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Plants."

(continued)

(continued)

BASES (continued)

REFERENCES (continued)	7. [Unit Name] FSAR, Section [15.3.2.1], "[Title]."
	8. [Unit Name] Core Operating Limits Report, "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM)—T_{avg} > 200°F (Digital)

BASES

BACKGROUND

The reactivity control system must be redundant and capable of holding the reactor core subcritical when shutdown under cold conditions (GDC 26, Ref. 1). Maintenance of the SDM ensures that postulated reactivity events will not damage the fuel. SDM requirements provide sufficient reactivity margin to ensure that acceptable fuel design limits will not be exceeded for normal shutdown and anticipated operational occurrences (AOO). As such, in MODES 1 and 2 the SDM defines the degree of subcriticality which would be obtained immediately following the insertion or scram of all control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn. In MODES 3, 4, and 5, the SDM specified continues to provide for adequate shutdown capability and acceptable fuel design limits for potential accidents initiated from shutdown conditions.

The system design requires that two independent Reactivity Control Systems be provided, and that one of these systems be capable of maintaining the core subcritical under cold conditions. These requirements are provided by the use of movable CEAs and soluble boric acid in the Reactor Coolant System (RCS). The CEA System can compensate for the reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full-load to no-load. In addition, the CEAs, together with the Boration System, provide the SDM during power operation and are capable of making the core subcritical rapidly enough to prevent exceeding acceptable fuel damage limits, assuming that the CEA of highest reactivity worth remains fully withdrawn.

The soluble Boron System can compensate for fuel depletion during operation and all xenon burnout reactivity changes, and maintain the reactor subcritical under cold conditions.

During power operation, SDM control is ensured by operating with the shutdown CEAs fully withdrawn and the regulating CEAs within the limits of LCO 3.1.7. When in the shutdown and refueling MODES, the SDM requirements are met by adjustments to the RCS boron concentration.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Ref. 2) establishes a SDM that ensures that specified acceptable fuel design limits are not exceeded for normal operation and AOOs with the assumption of the highest worth CEA stuck out on SCRAM.

The acceptance criteria for the SDM are that specified acceptable fuel design limits are maintained by ensuring that:

a. The reactor can be made subcritical from all operating conditions and transients and Design Basis Events;

b. The reactivity transients associated with postulated accident conditions are controllable within acceptable limits (departure from nucleate boiling ratio (DNBR), fuel centerline temperature limit AOOs, and ≤ 280 cal/gm energy deposition for the CEA ejection accident).

c. The reactor will be maintained sufficiently subcritical to preclude inadvertent criticality in the shutdown condition.

The most limiting accident for the SDM requirements are based on a main steam line break (MSLB) as described in the accident analysis (Ref. 2). The increased steam flow resulting from a pipe break in the main steam system causes an increased energy removal from the affected steam generator (SG), and consequently the RCS. This results in a reduction of the reactor coolant temperature. The resultant coolant shrinkage causes a reduction in pressure. In the presence of a negative moderator temperature coefficient, this cooldown causes an increase in core reactivity. As RCS temperature decreases, the severity of an MSLB decreases until the MODE 5 value is reached. The most limiting MSLB, with respect to potential fuel damage before a reactor trip occurs, is a guillotine break of a main steam line inside containment initiated at the end of core life. The positive reactivity addition from the moderator temperature decrease will terminate when the affected SG boils dry, thus terminating RCS heat removal and cooldown. Following the MSLB, a post-trip return to power may occur; however, no

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

fuel damage occurs as a result of the post-trip return to power and the THERMAL POWER does not violate the Safety Limit (SL) requirement of SL 2.1.1.

In addition to the limiting MSLB transient, the SDM requirement must also protect against:

a. inadvertent boron dilution;

b. An uncontrolled CEA withdrawal from a subcritical or low power condition;

c. Startup of an inactive Reactor Coolant Pump (RCP); and

d. CEA ejection.

Each of these is discussed below.

In the boron dilution analysis, the required SDM defines the reactivity difference between an initial subcritical boron concentration and the corresponding critical boron concentration. These values, in conjunction with the configuration of the RCS and the assumed dilution flow rate, directly affect the results of the analysis. This event is most limiting at the beginning of core life when critical boron concentrations are highest.

Depending on the system initial conditions and reactivity insertion rate, the uncontrolled CEA withdrawal transient is terminated by either a high power level trip, or a high pressurizer pressure trip. In all cases, power level, RCS pressure, linear heat rate, and the DNBR do not exceed allowable limits.

The startup of an inactive RCP will not result in a "cold water" criticality, even if the maximum difference in temperature exists between the SG and the core. The maximum positive reactivity addition which can occur due to an inadvertent RCP start is less than half the minimum required SDM. An idle RCP cannot, therefore, produce a return to power from the hot standby condition.

The withdrawal of CEAs from subcritical or low power Conditions adds reactivity to the reactor core, causing both the core power level and heat flux to increase with

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

corresponding increases in reactor coolant temperatures and pressure. The withdrawal of CEAs also produces a time-dependent redistribution of core power.

SDM satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed from the control room, SDM is considered an initial condition process variable because it is periodically monitored to provide assurance that the unit is operating within the bounds of accident analysis assumptions.

LCO

The accident analysis has shown that the required SDM is sufficient to avoid unacceptable consequences to the fuel or RCS as a result of the events addressed above. Shutdown boron concentration requirements assume the highest worth CEA is stuck in the fully withdrawn position to account for a postulated inoperable or untrippable CEA prior to reactor shutdown.

The MSLB (Ref. 2) and the boron dilution (Ref. 3) accidents are the most limiting analyses that establish the SDM value of the LCO. For MSLB accidents, if the LCO is violated, there is a potential to exceed the DNBR limit and to exceed 10 CFR 100 limits. SDM is a core physics design condition that can be ensured during operation through CEA positioning (regulating and shutdown CEAs) and through the soluble boron concentration. To ensure that SDM is behaving as anticipated so that the acceptance criteria are met, the SDM is evaluated during SR 3.1.1.1 and appropriate actions are taken as necessary when the SDM is not within the required limit. For the boron dilution accident, if the LCO is violated, then the minimum required time assumed for operator action to terminate dilution may no longer be applicable.

APPLICABILITY

In MODES 1, 2, 3, and 4, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analyses discussed above. In MODE 5, SDM is addressed by LCO 3.1.2. In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1, "Boron Concentration."

(continued)

BASES (continued)

ACTIONS

A.1

If the SDM requirements are not met, boration must be initiated immediately. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. Boration will be continued until SDM is within limit.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique design basis event that must be satisfied. It is imperative to raise the boron concentration of the RCS as soon as possible.

Therefore, the operator should begin boration with the best source available for the plant conditions. Some of the possible sources of boron originate from either the boric acid storage tank (BAST), whose minimum concentration of boron is [11600] ppm or the borated water storage tank (BWST), whose minimum concentration of boron is [2270] ppm. These sources include:

a. Makeup flow through makeup pumps from makeup tank: Makeup pumps are rated at [300] gpm at [2400] psig Boron concentration of the makeup tank varies with the time in life and the concentration in the RCS;

b. Makeup flow through makeup pumps from BWST: Makeup pumps are rated at [300] gpm at [2400] psig;

c. Makeup flow through makeup pumps from BAST: Makeup pumps are rated at [300] gpm at [2400] psig;

d. High pressure injection through makeup pumps from BWST: Makeup pumps are rated at [500] gpm at [600] psig;

e. Decay heat flow through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig;

f. Low Pressure Injection (LPI) through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig; and,

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

g. Boric acid through boric acid pumps from BAST: Boric acid pumps are rated at [25] gpm at [100] psig.

In determining the boration flow rate, it should be remembered that the most difficult time in core life to increase the RCS boron concentration is at beginning of cycle when the boron concentration may approach or exceed [2000] ppm.

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

In MODES 1 and 2, SDM is verified by observing that the requirements of LCO 3.1.6, "Shutdown CEA Insertion Limit," and LCO 3.1.7, "Regulating CEA Insertion Limit," are met. However, in the event that a CEA is known to be untrippable, SDM verification must account for the worth of the untrippable CEA as well as another CEA of maximum worth.

In MODES 3, 4, and 5, the SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration;

b. CEA positions;

c. RCS average temperature;

d. Fuel burnup based on gross thermal energy generation;

e. Xenon concentration;

f. Samarium concentration; and,

g. Isothermal Temperature Coefficient (ITC).

Using the ITC accounts for Doppler reactivity in this calculation because the reactor is subcritical and the fuel temperature will be changing at the same rate as the RCS. The Frequency of 24 hours is based on the generally slow change in required boron concentration, and also allows sufficient time for the operator to collect the required data, including boron concentration analysis, and complete the calculation.

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 26, "Reactivity Control System Redundancy and Capability."
2. [Unit Name] FSAR, Section [15.4.2.], "[Title]."
3. [Unit Name] FSAR, Section [15.4.2.], '[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 SHUTDOWN MARGIN (SDM)—$T_{avg} \leq 200°F$ (Digital)

BASES

BACKGROUND

The reactivity control system must be redundant and capable of holding the reactor core subcritical when shut down under cold conditions (Ref. 1). Maintenance of the SDM ensures that postulated reactivity events will not damage the fuel. SDM requirements provide sufficient reactivity margin to assure that acceptable fuel design limits will not be exceeded for normal shutdown and anticipated operational occurrences (AOOs). As such, in MODES 1 and 2 the SDM defines the degree of subcriticality which would be obtained immediately following the insertion or scram of all control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn. In MODES 3, 4, and 5, the SDM specified continues to provide for adequate shutdown capability and acceptable fuel design limits for potential accidents initiated from shutdown conditions.

The system design requires that two independent reactivity control systems be provided, and that one of these systems be capable of maintaining the core subcritical under cold conditions. These requirements are provided by the use of movable CEAs and soluble boric acid in the Reactor Coolant System (RCS). The CEA system can compensate for the reactivity effects of the fuel and water temperature changes accompanying power level changes over the range from full-load to no-load. In addition, the CEAs, together with the Boration System, provide the SDM during power operation and are capable of making the core subcritical rapidly enough to prevent exceeding the acceptable fuel damage limits, assuming that the CEA of highest reactivity worth remains fully withdrawn.

The soluble Boron System can compensate for fuel depletion during operation and all xenon burnout reactivity changes, and maintain the reactor subcritical under cold conditions.

During power operation, SDM control is ensured by operating with the shutdown CEAs fully withdrawn and the regulating

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

CEAs within the limits of LCO 3.1.7. When in the shutdown and refueling MODES, the SDM requirements are met by adjustments to the RCS boron concentration.

APPLICABLE SAFETY ANALYSES

The minimum required SDM is assumed as an initial condition in safety analysis. The safety analysis (Ref. 2) establishes a SDM that ensures that specified acceptable fuel design limits are not exceeded for normal operation and AOOs with the assumption of the highest worth CEA stuck out on scram. Specifically, for MODE 5, the primary safety analysis which relies on the SDM limits is the boron dilution analysis.

The acceptance criteria for the SDM are that the specified acceptable fuel design limits are maintained by ensuring that:

a. The reactor can be made subcritical from all operating conditions and transients and Design Basis Events;

b. The reactivity transients associated with postulated accident conditions are controllable within acceptable limits (departure from nucleate boiling ratio (DNBR), fuel centerline temperature limits for AOOs, and $\leq$ 280 cal/gm energy deposition for the CEA ejection accident); and

c. The reactor will be maintained sufficiently subcritical to preclude inadvertent criticality in the shutdown condition.

An inadvertent boron dilution is a moderate Frequency incident as defined in Reference 2. The core is initially subcritical with all CEAs inserted. A Chemical and Volume Control System malfunction occurs which causes unborated water to be pumped to the RCS via three charging pumps.

During the event, a minimum flow of [3000] gal/min will be circulated through the RCS by the Shutdown Cooling System (SDC): complete mixing of boron within the RCS is assumed. A cold (200°F) RCS volume, excluding the pressurizer, surge line, and the SDC, of [10,060] ft^3 is assumed. Excluding

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

the pressurizer, surge line, and SDC increases the severity of the dilution. At the SDC flow rate, an equivalent RCS volume will be circulated in approximately 30 minutes. The reactivity change rate associated with boron concentration changes is within the capabilities of operator recognition and control.

The high neutron flux alarm on the startup channel instrumentation will alert the operator of the boron dilution with a minimum of 15 minutes remaining before the core becomes critical. The event can then be terminated by either:

a. Turning off the charging pumps;

b. Turning off the primary makeup pump;

c. Isolating the reactor makeup water supply;

d. Isolating the volume control tank; or

e. Actuating safety injection.

SDM satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed from the control room, SDM is considered an initial condition process variable because it is periodically monitored to provide assurance that the unit is operating within the bounds of accident analysis assumptions.

LCO

The accident analysis has shown that the required SDM is sufficient to avoid unacceptable consequences to the fuel or RCS as a result of the events addressed above.

The boron dilution (Ref. 2) accident initiated in MODE 5 is the most limiting analysis which establishes the SDM value of the LCO. For the boron dilution accident, if the LCO is violated, then the minimum required time assumed for operator action to terminate dilution may no longer be applicable.

(continued)

(continued)

BASES (continued)

LCO (continued)

SDM is a core physics design condition that is evaluated during SR 3.1.2.1, and appropriate actions are taken as necessary when the SDM is not within the required limit.

APPLICABILITY

In MODE 5, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analysis discussed above. In MODES 1, 2, 3, and 4, the SDM requirements are given in LCO 3.1.1, "SHUTDOWN MARGIN (SDM)—T_{avg} >200°F." In MODE 6, the shutdown reactivity requirements are given in LCO 3.9.1 "Boron Concentration."

ACTIONS

A.1

If the SDM requirements are not met, boration must be initiated immediately. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. Boration will be continued until the SDM is within the limit.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique design basis event which must be satisfied. It is imperative to raise the boron concentration of the RCS as soon as possible.

Therefore, the operator should begin boration with the best source available for the plant conditions. Some of the possible sources of boron originate from either the boric acid storage tank (BAST), whose minimum concentration of boron is [11600] ppm, or the borated water storage tank (BWST), whose minimum concentration of boron is [2270] ppm. These sources include:

a. Makeup flow through makeup pumps from makeup tank: Makeup pumps are rated at [300] gpm at [2400] psig. (boron concentration of the makeup tank varies with the time in life and the concentration in the RCS);

b. Makeup flow through makeup pumps from BWST: Makeup pumps are rated at [300] gpm at [2400] psig;

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

c. Makeup flow through makeup pumps from BAST: Makeup pumps are rated at [300] gpm at [2400] psig;

d. High pressure injection through makeup pumps from BWST: Makeup pumps are rated at [500] gpm at [600] psig;

e. Decay heat flow through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig;

f. Low pressure injection through decay heat pumps from BWST: Decay heat pumps are rated at [3000] gpm at [100] psig; and

g. Boric acid through boric acid pumps from BAST: Boric acid pumps are rated at [25] gpm at [100] psig.

In determining the boration flow rate, it should be remembered that the most difficult time in core life to increase the RCS boron concentration is at beginning of cycle when the boron concentration may approach or exceed [2000] ppm.

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1

In MODE 5 the SDM is verified by performing a reactivity balance calculation, considering the listed reactivity effects:

a. RCS boron concentration;

b. CEA positions;

c. RCS average temperature;

d. Fuel burnup based on gross thermal energy generation;

e. Xenon concentration;

f. Samarium concentration; and

g. Isothermal Temperature Coefficient (ITC).

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

Using the ITC accounts for Doppler reactivity in this calculation because the reactor is subcritical and the fuel temperature will be changing at the same rate as that of the RCS.

The Frequency of 24 hours is based on the generally slow change in required boron concentration, and it allows sufficient time for the operator to collect the required data, including a boron concentration analysis, and complete the calculation.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 26, "Reactivity Control System Redundancy and Capability."
2. [Unit Name] FSAR, Section [15.2.4], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Reactivity Balance (Digital)

BASES

BACKGROUND

Per GDCs 26, 28, and 29 (Ref. 1), reactivity shall be controllable such that subcriticality is maintained under cold conditions and acceptable fuel design limits are not exceeded during normal operation and anticipated operational occurrences. Therefore, reactivity balance is used as a measure of the predicted versus measured core reactivity during power operation. The periodic confirmation of core reactivity is necessary to ensure that safety analyses of design basis transients and accidents remain valid. A large reactivity difference could be the result of unanticipated changes in fuel, control element assembly (CEA) worth, or operation at conditions not consistent with those assumed in the predictions of core reactivity and could potentially result in a loss of SHUTDOWN MARGIN (SDM) or violation of acceptable fuel design limits. Comparing predicted versus measured core reactivity validates the nuclear methods used in the safety analysis and supports the SDM demonstrations (LCO 3.1.1) in assuring the reactor can be brought safely to cold, subcritical conditions.

When the reactor core is critical or in normal power operation, a reactivity balance exists and the net reactivity is zero. A comparison of predicted and measured reactivity is convenient under such a balance since parameters are being maintained relatively stable under steady-state power conditions. The positive reactivity inherent in the core design is balanced by the negative reactivity of the control components, thermal feedback, neutron leakage, and materials in the core that absorb neutrons, such as burnable absorbers producing zero net reactivity. Excess reactivity can be inferred from the boron letdown curve (or critical boron curve), which provides an indication of the soluble boron concentration in the Reactor Coolant System (RCS) versus cycle burnup. Periodic measurement of the RCS boron concentration for comparison with the predicted value with other variables fixed such as CEA height, temperature, pressure, and power, provides a convenient method of ensuring that core reactivity is within design expectations, and that the calculation models used to generate the safety analysis are adequate.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

In order to achieve the required fuel cycle energy output, the uranium enrichment, in the new fuel loading and in the fuel remaining from the previous cycle, provides excess positive reactivity beyond that required to sustain steady-state operation throughout the cycle. When the reactor is critical at RATED THERMAL POWER (RTP) and moderator temperature, the excess positive reactivity is compensated by burnable absorbers (if any), CEAs, whatever neutron poisons (mainly xenon and samarium) are present in the fuel, and the RCS boron concentration.

When the core is producing THERMAL POWER, the fuel is being depleted and excess reactivity is decreasing. As the fuel depletes, the RCS boron concentration is reduced to decrease negative reactivity and maintain constant THERMAL POWER. The boron letdown curve is based on steady-state operation a RTP. Therefore, deviations from the predicted boron letdown curve may indicate deficiencies in the design analysis, deficiencies in the calculational models, or abnormal core conditions, and must be evaluated

APPLICABLE SAFETY ANALYSES

Accurate prediction of core reactivity is either an explicit or implicit assumption in the accident analysis evaluations. Every accident evaluation (Ref. 2) is, therefore, dependent upon accurate evaluation of core reactivity. In particular, SDM, and reactivity transients, such as CEA withdrawal accidents or CEA ejection accidents, are very sensitive to accurate prediction of core reactivity. These accident analysis evaluations rely on computer codes that have been qualified against available test data, operating plant data, and analytical benchmarks. Monitoring reactivity balance provides additional assurance that the nuclear methods provide an accurate representation of the core reactivity.

Design calculations and safety analyses are performed for each fuel cycle for the purpose of predetermining reactivity behavior and the RCS boron concentration requirements for reactivity control during fuel depletion.

The comparison between measured and predicted initial core reactivity provides a normalization for calculational models used to predict core reactivity. If the measured and

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

predicted RCS boron concentrations for identical core conditions at beginning of cycle (BOC) do not agree, then the assumptions used in the reload cycle design analysis or the calculation models used to predict soluble boron requirements may not be accurate. If reasonable agreement between measured and predicted core reactivity exists at BOC, then the prediction may be normalized to the measured boron concentration. Thereafter, any significant deviations in the measured boron concentration from the predicted boron letdown curve that develop during fuel depletion may be an indication that the calculation model is not adequate for core burnups beyond BOC, or that an unexpected change in core conditions has occurred.

The normalization of predicted RCS boron concentration to the measured value is typically performed after reaching RTP following startup from a refueling outage, with the CEAs in their normal positions for power operation. The normalization is performed at BOC conditions so that core reactivity relative to predicted values can be continually monitored and evaluated as core conditions change during the cycle.

Reactivity balance provides an additional assurance that SDM is maintained within the limits. Thus, reactivity balance satisfies Criterion 2 of the NRC Interim Policy Statement.

LCO

This Specification is provided to ensure that core reactivity behaves as expected in the long term, and to ensure that significant reactivity anomalies will be investigated.

The reactivity balance limit is established to ensure plant operation is maintained within the assumptions of the safety analyses. Large differences between actual and predicted core reactivity may indicate that the assumptions of the design basis transient and accident analyses are no longer valid, or that the uncertainties in the nuclear method are larger than expected. A limit on the reactivity balance of $\pm$ 1% $\Delta k/k$ has been established based on engineering

(continued)

(continued)

BASES (continued)

LCO (continued)

judgment. A 1% deviation in reactivity from that predicted is larger than expected for normal operation, and should therefore be evaluated

When measured core reactivity is within 1% $\Delta k/k$ of the predicted value at steady-state thermal conditions, the core is considered to be operating within acceptable design limits. Since deviations from the limit are normally detected by comparing predicted and measured steady-state RCS critical boron concentrations, the difference between measured and predicted values would be approximately 100 ppm (depending on the boron worth) before the limit is reached. These values are well within the uncertainty limits for analysis of boron concentration samples, so that spurious violations of the limit due to uncertainty in measuring the RCS boron concentration are unlikely.

APPLICABILITY

In MODE 1, most of the CEAs are withdrawn and steady-state operation is typically achieved. Under these conditions, the comparison between predictions and measurements provides an effective measure of the reactivity balance. In MODE 2, control rods are typically being withdrawn during a startup. In MODES 3, 4, and 5, all CEAs are fully inserted, and therefore the reactor is in the least reactive state where monitoring core reactivity is not necessary. In MODE 6, fuel loading results in a continually changing core reactivity. Boron concentration requirements (LCO 3.9.1) ensure that fuel movements are performed within the bounds of the safety analysis and an SDM demonstration is required during the first startup following operations which could have altered core reactivity (e.g., fuel movement or CEA replacement or shuffling).

ACTIONS

A.1 and A.2

Should an anomaly develop between measured and predicted core reactivity, an evaluation of the core design and safety analysis is performed. In practice, smaller deviations in core reactivity (greater than 0.5% $\Delta k/k$) are generally cause

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

for concern, and evaluations of both core conditions and the core design are performed to determine the cause of the deviation.

When a reactivity deviation is noted, the evaluation of core conditions typically includes the following steps:

a. Core conditions and the input to calculational models are verified to be consistent;

b. Shutdown capability from both the CEAs and the Boron Injection System is determined to be adequate;

c. A core power distribution map is obtained to evaluate peaking factors;

d. OPERABILITY of all CEAs is verified; and

e. Physical changes in the fuel or boron content of the RCS are considered.

An evaluation of the core design and safety analysis typically includes the following steps:

a. Reactivity worth calculations of boron, the CEAs, xenon, and samarium are reviewed;

b. The moderator and fuel temperature coefficient calculations are reviewed and verified to be within the bounds of the safety analysis;

c. The fuel depletion calculations are reviewed to determine that the calculated core burnup is appropriate; and

d. The calculation models are reviewed to verify that they are adequate for representation of the core conditions.

Reactivity anomalies are generally investigated when they are small, so that the evaluations are in progress before the 1% $\Delta k/k$ reactivity limit for a deviation is reached, and corrective measures may be defined. The required Completion

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Time of 72 hours is based on operating experience and the low probability of a Design Basis Accident (DBA) occurring during this period. Also, it allows sufficient time to assess the physical condition of the reactor and complete an evaluation of the core design and safety analysis.

Following evaluations of the core design and safety analysis, the cause of the reactivity anomaly may be resolved. If the cause of the reactivity anomaly is a mismatch in core conditions at the time of RCS boron concentration sampling, then a recalculation of the RCS boron concentration requirements may be performed to demonstrate that core reactivity is behaving as expected. If an unexpected physical change in the condition of the core has occurred, it must be evaluated and corrected, if possible. If the cause of the reactivity anomaly is in the calculation technique, then the calculational models must be revised to provide more accurate predictions. If any of these results are demonstrated and it is concluded that the reactor core is acceptable for continued operation, then the boron letdown curve may be renormalized, and power operation may continue. If operational restrictions or additional SRs are necessary to ensure the reactor core is acceptable for continued operation, then they must be defined.

B.1

The unit must be placed in a MODE in which the LCO does not apply if the core reactivity cannot be restored to within the 1% $\Delta k/k$ limit by the methods discussed in Required Action A.1 and the associated Completion Time. This is done by placing the unit in at least MODE 3 within 6 hours. If the SDM for MODE 3 is not met, then boration required by SR 3.1.1.1 would occur. The allowed Completion Time is reasonable, based on operating experience related to the time required, to reach the required plant conditions from full power in an orderly manner without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1

Core reactivity is verified by periodic comparisons of measured and predicted RCS boron concentrations. The

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

comparison is made considering that other core conditions are fixed or stable including CEA position, moderator temperature, fuel temperature, fuel depletion, xenon concentration, and samarium concentration. The surveillance is performed prior to entering MODE 1 as an initial check on core conditions and design calculations at BOC. A Note is included in the SR to indicate that the normalization of predicted core reactivity to the measured value must take place within the first 60 effective full power days (EFPDs) after each fuel loading. This allows sufficient time for core conditions to reach steady state, but prevents operation for a large fraction of the fuel cycle without establishing a benchmark for the design calculations. The required subsequent Frequency of 31 EFPDs, after the initial 60 EFPDs, after entering MODE 1, is acceptable based on the slow rate of core changes due to fuel depletion and the presence of other indicators, e.g., Quadrant Power Tilt Ratio, for prompt indication of an anomaly. Another Note is included in SR to indicate that the provisions of SR 3.0.4 are not applicable for this SR for entering MODE 2.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 26, "Reactivity Control System Redundancy and Capability"; General Design Criterion 28, "Reactivity Limits"; General Design Criterion 29, "Protection against Anticipated Operational Occurrences."

2. [Unit Name] FSAR, Section [ ], "[Accident Analysis]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Moderator Temperature Coefficient (MTC) (Digital)

BASES

BACKGROUND

Per GDC 11 (Ref. 1), the reactor core and its interaction with the reactor system coolant must be designed for inherently stable power operation, even in the possible event of an accident. In particular, the net reactivity feedback in the system must compensate for any unintended reactivity increases.

The MTC relates a change in core activity to a change in reactor coolant temperature (a positive MTC means that reactivity increases with increasing moderator temperature; conversely, a negative MTC means that reactivity decreases with increasing moderator temperature). The reactor is designed to operate with a negative MTC over the largest possible range of fuel cycle operation. Therefore, a coolant temperature increase will cause a reactivity decrease, so that the coolant temperature tends to return toward its initial value. Reactivity increases that cause a coolant temperature increase will thus be self-limiting, and stable power operation will result. The same characteristic is true when the MTC is positive and coolant temperature decreases occur.

MTC values are predicted at selected burnups during the safety evaluation analysis and are confirmed to be acceptable by measurements. Both initial and reload cores are designed so that the beginning of cycle (BOC) MTC is less than zero when THERMAL POWER is [95%] of RATED THERMAL POWER (RTP) or greater. The actual value of the MTC is dependent on core characteristics such as fuel loading and reactor coolant soluble boron concentration. The core design may require additional fixed distributed poisons (lumped burnable poison assemblies) to yield a MTC at the BOC within the range analyzed in the plant accident analysis. The end of cycle (EOC) MTC is also limited by the requirements of the accident analysis. Fuel cycles designed to achieve high burnups or with changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The acceptance criteria for the specified MTC are:

a. The MTC values must remain within the bounds of those used in the accident analysis (Ref. 2); and

b. The MTC must be such that inherently stable power operations result during normal operation and during accidents such as overheating and overcooling events.

Reference 2 contains analyses of accidents that result in both overheating and overcooling of the reactor core. MTC is one of the controlling parameters for core reactivity in these accidents. Both the most positive value and most negative value of the MTC are important to safety, and both values must be bounded. Values used in the analyses consider worst-case conditions, such as very large soluble boron concentrations, to ensure the accident results are bounding (Ref. 3).

Accidents that cause core overheating (either decreased heat removal or increased power production) must be evaluated for results when the MTC is positive. Reactivity accidents that cause increased power production include the control element assembly (CEA) withdrawal transient from either zero or full THERMAL POWER. The limiting overheating event relative to plant response is based on the maximum difference between core power and steam generator heat removal during a transient. The most limiting event with respect to a positive MTC is a [CEA withdrawal accident from zero power, also referred to as a startup accident (Ref. 4).]

Accidents that cause core overcooling must be evaluated for results when the MTC is most negative. The event which produces the most rapid cooldown of the Reactor Coolant System (RCS), and is therefore the most limiting event with respect to the negative MTC, is a steam line break (SLB) event. Following the reactor trip for the postulated EOC SLB event, the large moderator temperature reduction combined with the large negative MTC may produce reactivity increases that are as much as the shutdown reactivity. When this occurs, a substantial fraction of core power is produced with all CEAs inserted except the most reactive one. Even if the reactivity increase produces slightly subcritical conditions, a large fraction of core power may be produced through the effects of subcritical neutron multiplication.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

MTC values are bounded in reload safety evaluations assuming steady-state conditions at BOC and EOC. A middle of cycle (MOC) EOC measurement is conducted at conditions when the RCS boron concentration reaches approximately 300 ppm. The measured value may be extrapolated to project the EOC value, in order to confirm reload design predictions.

MTC satisfies Criterion 2 of the NRC Interim Policy Statement. Even though it is not directly observed and controlled from the control room, MTC is considered an initial condition process variable because of its dependence on boron concentration.

LCO

LCO 3.1.4 requires the MTC to be within the specified limits of the CORE OPERATING LIMITS REPORT (COLR) (Ref. 5) to ensure the core operates within the assumptions of the accident analysis. During the reload core safety evaluation, the MTC is analyzed to determine that its values remain within the bounds of the original accident analysis during operation. The limit of [+0.9E-4] (%Δk/k)/F on a positive MTC when THERMAL POWER is less than [95%] of RTP assures that core overheating accidents will not violate the accident analysis assumptions. The requirement for a negative MTC when THERMAL POWER is [95%] of RTP or greater ensures that core operation will be stable. The negative MTC limit for EOC specified in the COLR ensures that core overcooling accidents will not violate the accident analysis assumptions.

MTC is a core physics parameter determined by the fuel and fuel cycle design and cannot be easily controlled once the core design is fixed. During operation, therefore, the conditions of the LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on a MTC provide confirmation that the MTC is behaving as anticipated so that the acceptance criteria are met.

APPLICABILITY

In MODE 1, the limits on the MTC must be maintained to assure that any accident initiated from THERMAL POWER operation will not violate the design assumptions of the accident initiated from THERMAL POWER operation will not

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

violate the design assumptions of the accident analysis. In MODE 2, the limits must also be maintained to ensure startup and subcritical accidents (such as the uncontrolled CEA assembly or group withdrawal) will not violate the assumptions of the accident analysis. In MODES 3, 4, 5, and 6, this LCO is not applicable, since no Design Basis Accidents (DBAs) using the MTC as an analysis assumption are initiated from these MODES. However, the variation of the MTC with temperature in MODES 3, 4, and 5, for DBAs initiated in MODES 1 and 2, is accounted for in the subject accident analysis. The variation of the MTC with temperature assumed in the safety analysis is accepted as valid once the BOC and MOC measurements are used for normalization.

ACTIONS

A.1

MTC is a function of the fuel and fuel cycle design and cannot be controlled directly once their designs have been implemented in the core. If the MTC exceeds its limits, the reactor must be placed in MODE 3 with a minimum SHUTDOWN MARGIN. This eliminates the potential for violation of the accident analysis bounds. The associated Completion Time of 6 hours is reasonable considering the probability of an accident occurring during the time period which would require a MTC value within the LCO limits, and the length of time required to reach MODE 3 Conditions from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

The SRs for measurement of the MTC at the beginning and middle of each fuel cycle provide for confirmation of the limiting MTC values. The MTC changes smoothly from most positive (least negative) to most negative value during fuel cycle operation as the RCS boron concentration is reduced to compensate for fuel depletion. The requirement for measurement prior to operation above 5% of RTP satisfies the confirmatory check on the most positive (least negative) MTC value. The requirement for measurement within 7 days after

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

reaching 40 effective full power days (EFPD) and a $\frac{2}{3}$ core burnup satisfies the confirmatory check of the most negative MTC value. The measurement is performed at any THERMAL POWER so that the projected EOC MTC may be evaluated before the reactor actually reaches the EOC condition. MTC values may be extrapolated and compensated to permit direct comparison to the specified MTC limits.

The SR is modified by a Note that states that SR 3.0.4 is not applicable for entering MODE 2. Although this surveillance is applicable in MODE 2, the reactor must be critical before the surveillance can be completed. Therefore, entry into the applicable MODE prior to accomplishing the surveillance is necessary.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 11, "Reactor Inherent Protection."
2. [Unit Name] FSAR, Section [ ], "[Safety Analysis]."
3. [Unit Name] FSAR, Section [ ], "[Title]."
4. [Unit Name] FSAR, Section [ ], "[Title]."
5. [Unit Name] Core Operating Limits Report, "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Control Element Assembly (CEA) Alignment (Digital)

BASES

BACKGROUND

The OPERABILITY of the shutdown and regulating CEAs are initial assumptions in all safety analyses which assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analyses which directly affects core power distributions and assumptions of available SHUTDOWN MARGIN (SDM).

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled Nuclear Power Plants" (Ref. 2).

Mechanical or electrical failures may cause a CEA to become inoperable or to become misaligned from its group. CEA inoperability or misalignment may cause increased power peaking due to the asymmetric reactivity distribution and a reduction in the total available CEA worth for reactor shutdown. Therefore CEA alignment and operability are related to core operation in design power peaking limits and the core design requirement of a minimum SDM.

Limits on CEA alignment and operability have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking and SDM limits are preserved.

CEAs are moved by their CEA drive mechanisms. Each CEA drive mechanism moves its CEA one step (approximately [$\frac{3}{4}$ inches]) at a time but at varying rates (steps per minute) depending on the signal output from the Rod Control System.

The CEAs are arranged into groups that are radially symmetric. Therefore, movement of the CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

reactor trip. The regulating CEAs also provide reactivity (power level) control during normal operation and transients. Their movement may be automatically controlled by the Reactor Regulating System.

The axial position of shutdown and regulating CEAs is indicated by two separate and independent systems, which are the Plant Computer CEA Position Indication System and the Reed Switch Position Indication System.

The Plant Computer CEA Position Indication System counts the commands sent to the CEA gripper coils from the Control Element Drive Mechanism (CEDM) Control System that moves the CEAs. There is one step counter for each group of CEAs. Individual CEAs in a group all receive the same signal to move and should, therefore, all be at the same position indicated by the group step counter for that group. The Plant Computer CEA Position Indication System is considered highly precise (± one step or ± $\frac{3}{4}$ inch). If CEA does not move 1 step for each command signal, the step counter will still count the command and incorrectly reflect the position of the CEA.

The Reed Switch Position Indication System provides a highly accurate indication of actual CEA position, but at a lower precision than the step counters. This system is based on inductive analog signals from a series of reed switches spaced along a tube with a center-to-center distance of 1.5 inches, which is 2 steps. To increase the reliability of the system, there are redundant reed switches at each position.

APPLICABLE SAFETY ANALYSES

CEA misalignment accidents are analyzed in the safety analysis (Ref. 4). The accident analysis defines CEA misoperation as any event, with the exception of sequential group withdrawals, which could result from a single malfunction in the Reactivity Control System. For example, CEA misalignment may be caused by a malfunction of the CEA drive mechanism, CEDM Control System, or by operator error. A stuck CEA may be caused by mechanical jamming of the CEA fingers or of the gripper. Inadvertent withdrawal of a single CEA may be caused by opening of the electrical circuit of the CEDM holding coil for a full-length

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

or part-length CEA. A dropped CEA subgroup could be caused by an electrical failure in the CEA coil power programmers.

The acceptance criteria for addressing CEA inoperability or misalignment is that there be no violations of:

a. Specified acceptable fuel design limits;

b. Centerline fuel temperature;

c. Reactor Coolant System (RCS) pressure boundary damage; and

d. The core must remain subcritical after accident transients.

Three types of misalignment are distinguished. During movement of a group, one CEA may stop moving while the other CEAs in the group continue. This condition may cause excessive power peaking. The second type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition requires an evaluation to determine that sufficient reactivity worth is held in the remaining CEAs to meet the SDM requirement with the maximum worth CEA stuck fully withdrawn. If a CEA is stuck in the fully withdrawn position, its worth is added to the SDM, since the safety analysis does not take two stuck CEAs into account. The third type of misalignment occurs when one CEA drops partially or fully into the reactor core. This event causes an initial power reduction followed by a return towards the original power due to positive reactivity feedback from the negative moderator temperature coefficient. Increased peaking during the power increase may result in excessive local linear heat rates (LHRs).

Two types of analysis are performed in regard to static CEA misalignment (Ref. 3). With CEA banks at their insertion limits, one type of analysis considers the case when any one CEA is inserted [ ] inches into the core. The second type of analysis considers the case of a single CEA withdrawn [ ] inches from a bank inserted to its insertion limit. Satisfying limits on departure from nucleate boiling ratio (DNBR) in both of these cases bounds the situation when a CEA is misaligned from its group by [7 inches].

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Another type of misalignment occurs if one CEA fails to insert upon a reactor trip and remains stuck fully withdrawn. This condition is assumed in the evaluation to determine that the required SDM is met with the maximum worth CEA also fully withdrawn (Ref. 5).

The effect of any misoperated CEA on the core power distribution will be assessed by the CEA calculators, and an appropriately augmented power distribution penalty factor will be supplied as input to the core protection calculators (CPCs). As the reactor core responds to the reactivity changes caused by the misoperated CEA and the ensuing reactor coolant and Doppler feedback effects, the CPCs will initiate a low DNBR or high local power density trip signal if specified acceptable fuel design limits (SAFDLs) are approached.

Since the CEA drop incidents result in the most rapid approach to SAFDLs caused by a CEA misoperation, the accident analysis analyzed a single full-length CEA drop, a single part-length CEA drop, and a part-length CEA subgroup drop. The most rapid approach to the DNBR SAFDL may be caused by either a single full-length drop or a part-length CEA subgroup drop depending upon initial conditions. The most rapid approach to the fuel center-line melt SAFDL is caused by a single part-length CEA drop.

In the case of the full-length CEA drop, a prompt decrease in core average power and a distortion in radial power are initially produced, which when conservatively coupled result in local power and heat flux increases, and a decrease in DNBR. For plant operation within the DNBR and local power density (LPD) LCOs, DNBR and LPD trips can normally be avoided on a dropped CEA.

For a part-length CEA subgroup drop, a distortion in power distribution, primarily axial, and either a rapid increase or decrease in core power are initially produced. The initial change in core power depends on the reactivity insertion, which may be positive or negative depending on the relative position of the axial peak and the position of the part-length CEA subgroup. As the dropped part-length CEA subgroup is detected, an appropriate power distribution penalty factor is supplied to the CPCs, and a reactor trip signal on low DNBR is generated.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

For the part-length CEA drop, both core average power and three-dimensional peak-to-average power density increase promptly. As the dropped part-length CEA is detected, core power and an appropriately augmented power distribution penalty factor are supplied to the CPCs.

Shutdown and regulating CEA operability and alignment are directly related to power distribution and SDM, which are initial conditions assumed in safety analyses. Therefore, they satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The limit on shutdown and regulating CEA alignments assure that the assumptions in the safety analysis will remain valid. The requirements on operability assure that upon reactor trip, the assumed reactivity will be available and will be inserted. The operability requirements also assure that the CEA banks will move correctly upon command, to maintain the correct power distribution and CEA alignment.

The requirement to maintain the CEA alignment to within 7 inches between the highest and lowest CEAs in a subgroup is conservative. The minimum misalignment assumed in safety analysis is [19 inches], and in some cases a total misalignment from fully withdrawn to fully inserted is assumed.

CEAs are operable when they meet the SRs of this LCO, i.e., can be inserted and withdrawn to meet the alignment limits, sequence and overlap withdrawal requirements, CEA drop times, and position indication requirements.

[For this facility, an OPERABLE Plant Computer CEA Position Indication System (if required) and Reed Switch Indication System constitute the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure CEA OPERABILITY:]

[For this facility, the required support systems which upon their failure do not declare the CEA inoperable and their justification are as follows:]

(continued)

(continued)

BASES (continued)

LCO (continued)

Failure to meet the requirements of this LCO may produce unacceptable power peaking factors and LHRs, or unacceptable SDM, all of which may constitute initial conditions inconsistent with the safety analysis.

APPLICABILITY

The requirements on CEA OPERABILITY and alignment are applicable in MODES 1 and 2 because these are the only modes in which neutron (or fission) power is generated, and the operability and alignment of CEAs has the potential to affect the safety of the plant. In MODES 3, 4, 5, and 6, the alignment limits do not apply because the CEAs are bottomed and the reactor is shut down and not producing fission power. In the shutdown modes, the OPERABILITY of the shutdown and regulating CEAs has the potential to affect the required SDM, but this effect can be compensated for by an increase in the boron concentration of the RCS. See LCO 3.1.1 for SDM in MODES 3, 4, and 5, and LCO 3.9.1 for boron concentration requirements during refueling.

ACTIONS

A.1, A.2.1, and A.2.2

A CEA is inoperable if it will not move in response to signals from the CEDM Control System. A CEA may become inoperable yet remain trippable. In this condition the CEA can still perform its required function of adding negative reactivity should a reactor trip be necessary. If a CEA is inoperable but trippable, continued operation in MODES 1 and 2 may continue provided the position of the inoperable CEA does not result in unacceptable peaking factors. This is accomplished by verifying that the CEA is either fully withdrawn (shutdown CEA) (see LCO 3.1.6), and if in regulating group [5], the CEA is within the long-term steady-state insertion limits of LCO 3.1.7. Also, if it is a regulating CEA, it is verified that the CEA is positioned within [7] inches (indicated reed switch position) of all other CEAs in its group. The 1-hour Completion Time ensures an acceptable CEA alignment is established before xenon redistribution can generate unacceptable peaking factors.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

B.1, B.2, B.3.1, and B.3.2

With one or more full-length regulating CEAs misaligned from other CEAs in its group by > [7] inches and ≤ [19] inches AND all full-length shutdown and regulating CEAs trippable, THERMAL POWER is reduced per Figure 3.1.5-1. Power operation may continue as long as the misaligned regulating CEA can be aligned to all the other CEAs in the group within 1 hour, OR all the other CEAs within limits in the group are aligned to within [7] inches of the misaligned CEAs within two hours while maintaining the insertion and sequence limits of LCO 3.1.7.

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER in accordance with Figure 3.1.5-1 ensures acceptable power distributions are maintained (Ref. 6). For small misalignments (< 19 inches) of the CEAs, there is:

a. A small effect on the time-dependent long-term power distributions relative to those used in generating LCOs and limiting safety system settings (LSSS) setpoints;

b. A small effect on the available SDM; and

c. A small effect on the ejected CEA worth used in the accident analysis.

Therefore, a 1-hour time period is sufficient to:

a. Identify causes of a misaligned CEA;

b. Take appropriate corrective action to realign the CEAs; and

c. Minimize the effects of xenon redistribution.

With a large CEA misalignment (≥ [19] inches), however, this misalignment would cause distortion of the core power distribution. This distortion may, in turn, have a significant effect on:

a. The available SDM;

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

b. The time-dependent, long-term power distributions relative to those used in generating LCOs and LSSS setpoints; and

c. The ejected CEA worth used in the accident analysis.

Therefore, prompt reduction in power is required to eliminate a large misalignment.

Power operations may continue provided adequate SDM exists and the CEAs can be properly aligned. This may be accomplished by aligning the OPERABLE CEAs to the inoperable CEA (subgroup). Since, the CEA may be misaligned by > [19] inches, an SDM verification is made. Subsequently, maintaining the insertion and sequence limits of LCO 3.1.6 and LCO 3.1.7 ensures adequate SDM and proper power distribution are maintained. The 1-hour Completion Time to align the OPERABLE CEAs provides the operator 1 hour to properly align the OPERABLE CEAs to the CEA (subgroup).

Although a part-length CEA has less of an effect on core flux than a full-length CEA, a misaligned part-length CEA will still result in xenon redistribution and effect core power distribution. Requiring realignment within 1 hour minimizes these effects and ensures acceptable power distribution is maintained.

C.1

In most cases, when more than one CEA is found to be trippable and aligned but immovable, the malfunction can be traced to the Reactor Regulating System. Since the majority of Reactor Regulating System malfunctions can be repaired without reactor shutdown, and since the unit conditions are not outside any accident analysis assumptions, the appropriate action is to locate the malfunction and restore the rods to an OPERABLE status. Maintaining the sequence, insertion, and power limits of LCO 3.1.6 and LCO 3.1.7 ensures that core design limits are not exceeded. Since a Completion Time of 72 hours provides adequate time to locate the malfunction as well to obtain parts and perform the repairs, if the malfunction is not corrected in 72 hours it would be indicative of additional problems and plant shutdown would be required.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

D.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown is commenced. The allowed time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

E.1 and E.2

If more than one full-length regulating CEA is misaligned in more than one group, it may indicate a serious problem with the CEAs and their support systems, and may place the plant outside the accident analysis. Therefore, LCO 3.0.3 must be immediately entered.

In the case of:

a. More than one CEA misaligned from any other CEA in their group by more than 19 inches, or

b. One or more CEAs inoperable as the result of excessive friction or mechanical interferences or known to be untrippable,

continued operation is not allowed. This is because any one of these conditions may be indicative of a possible loss of mechanical functional capability of the CEAs and in the event of a stuck or untrippable CEA, a loss of SDM.

If a CEA is inoperable as a result of excessive friction or mechanical interference or is untrippable, it is not available for reactivity insertion during a reactor trip. With an untrippable CEA, meeting the insertion limits of LCO 3.1.6 and LCO 3.1.7 does not ensure that adequate SDM exists. In this condition, an additional allowance must be made for the worth of the affected CEA when calculating the available SDM.

This is necessary since the OPERABLE CEAs must still meet the single failure criteria. If additional negative reactivity is required to provide the necessary SDM, it must

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

be provided by increasing the RCS boron concentration. One hour allows sufficient time to perform the SDM calculation and make any required boron adjustment to the RCS. The
6-hour Completion Time to reach MODE 3 is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

Verification that individual CEA indicated reed switch positions are within 7 inches (indicated reed switch positions) of all other CEAs in the group at a 12-hour Frequency allows the operator to detect a CEA beginning to deviate from its expected position. The specified frequency takes into account other CEA position information that is continuously available to the operator in the control room so that during actual CEA motion, deviations can immediately be detected.

[For this facility, each CEA Reed Switch Indication System is considered inoperable if it has [ ] individual reed switches inoperable.]

SR 3.1.5.2

Operability of at least two CEA position indicator channels is required to determine CEA positions and thereby ensure compliance with the CEA alignment and insertion limits. The CEA "full in" and "full out" limits provide an additional independent means for determining the CEA positions when the CEAs are at either their fully inserted or fully withdrawn positions. [For this facility, each CEA Reed Switch Indication System is considered inoperable if it has [ ] individual reed switches inoperable.]

SR 3.1.5.3 and SR 3.1.5.4

Exercising individual CEAs that are not fully inserted into the reactor core every 92 days verifies that all CEAs continue to be OPERABLE even if they are not regularly moved. A movement of [5] inches is adequate to demonstrate

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

motion without exceeding the alignment limit when only one CEA is being moved. The 92-day Frequency takes into consideration other information available to the operator in the control room and other surveillances being performed more frequently which add to the determination of OPERABILITY of the CEAs.

SR 3.1.5.5

Performance of a CHANNEL FUNCTIONAL TEST of each reed switch position transmitter channel ensures the channel is OPERABLE and capable of indicating CEA position over the entire length of the CEAs travel. Since this test must be performed when the reactor is shut down, an 18-month Frequency to be coincident with refueling outage was selected. Operating experience has shown that these components usually pass this surveillance when performed with the 18-month Frequency. Furthermore, the Frequency takes into account other surveillances being performed at shorter Frequencies which determine the OPERABILITY of the CEA Reed Switch Indication System.

SR 3.1.5.6

Verification of CEA drop times determines that the maximum CEA drop time permitted is consistent with the assumed drop time used in the safety analysis (Ref. 7). Measuring drop times prior to reactor criticality after reactor vessel head removal assures the reactor internals and CEDM will not interfere with CEA motion or drop time. Also, every 18 months the CEA drop times are verified to ensure that no degradation in these systems has occurred that would adversely affect CEA motion or drop time. Individual CEAs whose drop times are greater than safety analysis assumptions are not OPERABLE. The 18-month Frequency was developed because it was considered prudent that this surveillance only be performed during a plant outage. This is due to the plant conditions needed to perform the SR and the potential for an unplanned plant transient if the surveillance is performed with the reactor at power. Operating experience has shown that these components usually pass this surveillance when performed on the 18-month Frequency. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," and General Design Criterion 26, "Reactivity Limits."
2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
3. [Unit Name] FSAR, Section [ ], "[Title]."
4. [Unit Name] FSAR, Section [ ], "[Title]."
5. [Unit Name] FSAR, Section [ ], "[Title]."
6. [Unit Name] FSAR, Section [ ], "[Title]."
7. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.6 Shutdown Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the shutdown and regulating CEAs are initial assumptions in all safety and analyses which assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions and assumptions of available SHUTDOWN MARGIN (SDM), ejected CEA worth, and initial reactivity insertion rate.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design," and 26, "Reactivity Limits" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2). Limits on shutdown CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the reactivity limits, ejected CEA worth, and SDM limits are preserved.

The CEAs are arranged into groups that are radially symmetric. Therefore, movement of the CEAs does not introduce radial asymmetries in the core power distribution. The shutdown and regulating CEAs provide the required reactivity worth for immediate reactor shutdown upon a reactor trip. The regulating CEAs also provide reactivity (power level) control during normal operation and transients. Their movement may be automatically controlled by the Reactor Regulating System.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are normally automatically controlled by the Reactor Regulating System, but they can also be manually controlled. They are capable of adding negative reactivity very quickly (compared to borating). The regulating CEAs must be maintained above designed insertion limits and are typically near the fully withdrawn position during normal full power operations. Hence, they are not capable of adding a large amount of positive reactivity. Boration or dilution of the Reactor

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)	Coolant System (RCS) Compensates for the reactivity changes associated with large changes in RCS temperature.
	The shutdown CEAs are used primarily to help ensure that the required SDM is maintained. The shutdown CEAs are controlled manually or automatically by the control room operator. During normal unit operation, the shutdown CEAs are fully withdrawn. The shutdown CEAs must be completely withdrawn from the core prior to withdrawing regulating CEAs during an approach to criticality. The shutdown CEAs are then left in this position until the reactor is shut down. They add negative reactivity to shut down the reactor upon receipt of a reactor trip signal.
APPLICABLE SAFETY ANALYSES	On a reactor trip, all CEAs (shutdown CEAs and regulating CEAs), except the most reactive CEA, are assumed to insert into the core. The shutdown CEAs shall be at their insertion limits and available to insert the maximum amount of negative reactivity on a reactor trip signal. The regulating CEAs may be partially inserted in the core as allowed by LCO 3.1.7, "Regulating Control Element Assembly (CEA) Insertion Limits." The shutdown CEA insertion limit is established to ensure that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM (See LCOs 3.1.1) following a reactor trip from full power. The combination of regulating CEAs and shutdown CEAs (less the most reactive CEA which is assumed to be fully withdrawn) is sufficient to take the reactor from full power conditions at rated temperature to zero power and to maintain the required SDM at rated no-load temperature (Ref. 3). The shutdown CEA insertion limit also limits the reactivity worth of an ejected shutdown CEA.
	The acceptance criteria for addressing shutdown and regulating CEA insertion limits and inoperability or misalignment is that:

a. There be no violations of:

1. Specified acceptable fuel design limits,

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

2. Centerline fuel temperature, or

3. RCS pressure boundary damage; and

b. The core must remain subcritical after accident transients.

As such, the shutdown CEA insertion limits affect safety analyses involving core reactivity, ejected CEA worth, and SDM (Ref. 3). Shutdown CEA insertion limits preserve an initial condition assumed in the safety analyses and, as such, satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The shutdown CEAs must be within their insertion limits any time the reactor is critical or approaching criticality. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required SDM following a reactor trip.

[For this facility, an OPERABLE shutdown CEA is verified as follows:]

[For this facility, the following support systems are required OPERABLE to ensure shutdown CEA insertion limits are met and are OPERABLE: [List].]

[For this facility, the required support systems which, upon their failure, do not result in the shutdown CEAs not meeting their insertion limits or in CEA inoperability and their justification are as follows:]

APPLICABILITY

The shutdown CEAs must be within their insertion limits with the reactor in MODE 1 and MODE 2. The applicability in MODE 2 begins within 15 minutes prior to initial regulating CEA withdrawal during an approach to criticality and continues throughout MODE 2 until all regulating CEAs are again fully inserted by scram or during shutdown. This ensures that a sufficient amount of negative reactivity is available to shut down the reactor and maintain the required

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

SDM following a reactor trip. The reactor is not critical or approaching criticality in MODE 3, 4, 5, or 6, and, therefore, the shutdown CEAs must be fully inserted.

This LCO has been modified by a Note that suspends the LCO requirement during SR 3.1.5.5, which assures the freedom of the CEAs to move. This SR requires the shutdown CEAs to move below the LCO limits, which would normally violate the LCO.

ACTIONS

A.1

With the SDM reduced by the insertion of a shutdown CEA, the operator can no longer rely on the regulating CEAs being above the transient insertion limit to ensure adequate SDM exists. Initiation of boration within 15 minutes is required since the SDM in MODES 1 and 2 is no longer ensured by adhering to the regulating and safety CEA insertion limits (See LCO 3.1.1).

In the event that the shutdown CEA Position Indication System is found to be inoperable, the shutdown CEA is considered to be not within limits and Required Action A.2 applies.

A.2

Accident analysis assumes that the s tdown CEAs are fully withdrawn any time the reactor is cr cal. This ensures that:

a. The minimum SDM is maintained; and

b. The potential effects of a CEA ejection accident are limited to acceptable limits.

CEAs are considered fully withdrawn at 145 inches since this position places them outside the active region of the core. The required Completion Time of 1 hour to fully withdraw the shutdown CEA all s the operator adequate time to adjust the CEA in an orderly manner and is consistent with the required Completion Time for Action A.1 in LCO 3.1.5, "CEA Alignment."

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

B.1

When the Required Action of A.2 cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The 6-hour Completion Time is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

Verification that the shutdown CEAs are within their insertion limits within 15 minutes prior to an approach to criticality ensures that when the reactor is critical, or being taken critical, the shutdown CEAs will be available to shut down the reactor and the required SDM will be maintained following a reactor trip. This SR and Frequency ensure that the shutdown CEAs are withdrawn before the regulating CEAs are withdrawn during a unit startup.

Since the shutdown CEAs are positioned manually by the control room operator, a verification of shutdown CEA position at a Frequency of 12 hours after the reactor is taken critical is adequate to ensure that they are within their insertion limits. Also, the Frequency takes into account other information available to the operator in the control room that monitors the status of the shutdown CEAs.

SR 3.1.6.1 is modified by a Note that allows exemption to SR 3.0.4 for entering MODE 2. SR 3.0.4 is not applicable before entering the applicability condition of "within 15 minutes prior to initial regulating CEA withdrawal," because the surveillance is specifically selected to be concurrent with the applicability.

[For this facility an OPERABLE shutdown CEA within limits is verified as follows:]

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," and General Design Criterion 26, "Reactivity Limits."
2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
3. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Regulating Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the shutdown and regulating CEAs are initial assumptions in all safety analyses which assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions and assumptions of available SHUTDOWN MARGIN (SDM) and initial reactivity insertion rate. The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10 "Reactor Design," GDC 26, "Reactivity Limits" (Ref. 1), and 10 CFR Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 2).

Limits on regulating CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution and reactivity limits defined by the design power peaking, ejected CEA worth, reactivity insertion rate, and SDM limits are preserved.

The regulating CEA groups operate with a predetermined amount of position overlap in order to approximate a linear relation between CEA worth and position (integral CEA worth). The regulating CEA groups are withdrawn and operate in a predetermined sequence. The Reactor Regulating System controls reactivity by moving the regulating CEA groups in sequence within analyzed ranges. The group sequence and overlap limits are specified in the CORE OPERATING LIMITS REPORT (COLR).

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are normally controlled automatically by the Reactor Regulating System, but can also be manually controlled. They are capable of adding reactivity very quickly (compared to borating or diluting).

The power density at any point in the core must be limited to maintain specified acceptable fuel design limits, including limits that preserve the criteria specified in 10 CFR 50.46 (Ref. 2). Together, LCO 3.1.7, LCO 3.2.4,

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

and LCO 3.2.5 provide limits on control component operation and on monitored process variables to ensure the core operates within the linear heat rate (LHR) (LCO 3.2.1), planar radial peaking factor (F_{xy}) (LCO 3.2.2), and departure from nuclear boiling ratio (DNBR) (LCO 3.2.4) limits in the COLR (Ref. 3). Operation within the LHR limits given in the COLR prevents power peaks that would exceed the loss-of-coolant accident (LOCA) limits derived by the Emergency Core Cooling System analysis. Operation within the F_{xy} and departure from nucleate boiling (DNB) limits given in the COLR prevents DNB during a loss of forced reactor coolant flow accident. In addition to the LHR and F_{xy} and DNBR limits, certain reactivity limits are preserved by regulating CEA insertion limits. The regulating rod insertion limits also restrict the ejected CEA worth to the values assumed in the safety analysis and preserve the minimum required SDM in MODES 1 and 2.

The establishment of limiting safety system settings and LCOs require that the expected long- and short-term behavior of the radial peaking factors be determined. The long-term behavior relates to the variation of the steady-state radial peaking factors with core burnup and is affected by the amount of CEA insertion assumed, the portion of a burnup cycle over which such insertion is assumed,and the expected power level variation throughout the cycle. The short-term behavior relates to transient perturbations to the steady-state radial peaks due to radial xenon redistribution. The magnitudes of such perturbations depend upon the expected use of the CEAs during anticipated power reductions and load maneuvering. Analyses are performed based on the expected mode of operation of the Nuclear Steam Supply System (base-loaded, maneuvering, etc.). From these analyses CEA insertions are determined and a consistent set of radial peaking factors defined. The long-term steady-state and short-term insertion limits are determined based upon the assumed mode of operation used in the analyses,and provide a means of preserving the assumptions on CEA insertions used. The long- and short-term insertion limits of LCO 3.1.7 are specified for the plant that has been designed for primarily base loaded operation, but which has the ability to accommodate a limited amount of load maneuvering.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The shutdown and regulating CEA insertion and alignment limits, AXIAL SHAPE INDEX (ASI), and AZIMUTHAL POWER TILT (T_q), are process variables that together characterize and control the three-dimensional power distribution of the reactor core. Additionally, the regulating bank insertion limits control the reactivity that could be added in the event of a CEA ejection accident, and the shutdown and regulating bank insertion limits ensure the required SDM is maintained.

Operation within the subject LCO limits will prevent fuel cladding failures that would breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a LOCA, loss of flow, ejected CEA, or [illegible] accident requiring termination by a Reactor Trip System trip function.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition I) and anticipated operational occurrences (Condition II). The acceptance criteria for the regulating CEA insertion, ASI, and T_q LCOs are such as to preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a large-break LOCA, the peak cladding temperature must not exceed a limit of 2200°F (10 CFR 50.46, Ref. 2);

b. During a loss of forced reactor coolant flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition. This is referred to hereafter as the 95/95 DNB criterion;

c. During an ejected CEA accident, the fission-energy input to the fuel must not exceed 280 cal/gm (Ref. 4); and

d. The CEAs must be capable of shutting down the reactor with a minimum required SDM with the highest worth CEA stuck fully withdrawn (GDC 26, Ref. 1).

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)	Regulating CEA position, ASI, and T_q are process variables that together characterize and control the three-dimensional power distribution of the reactor core. Fuel cladding damage does not occur when the core is operated outside these LCOs during normal operation. However, fuel cladding damage could result should an accident occur with simultaneous violation of one or more of these LCOs. Changes in the power distribution can cause increased power peaking and corresponding increased local linear heat rates (LHRs). The SDM requirement is ensured by limiting the regulating and shutdown CEA insertion limits so that the allowable inserted worth of the CEAs is such that sufficient reactivity is available in the CEAs to shut down the reactor to hot zero power with a reactivity margin that assumes the maximum worth CEA remains fully withdrawn upon trip (Ref. 5). Operation at the insertion limits or ASI may approach the maximum allowable linear heat generation rate or peaking factor with the allowed T_q present. Operation at the insertion limit may also indicate the maximum ejected CEA worth could be equal to the limiting value in fuel cycles which have sufficiently high ejected CEA worths. The regulating and shutdown CEA insertion limits ensure that safety analyses assumptions for reactivity insertion rate, SDM, ejected rod worth, and power distribution peaking factors are preserved (Ref. 6). The insertion limits satisfy Criterion 2 of the NRC Interim Policy Statement in that they are initial conditions assumed in the safety analysis.
LCO	The limits on shutdown and regulating CEA sequence, overlap, and physical insertion as defined in the COLR (Ref. 3) must be maintained because they serve the function of preserving power distribution, ensuring that the SDM is maintained, ensuring that ejected CEA worth is maintained, and ensuring adequate negative reactivity insertion on trip.

(continued)

(continued)

BASES (continued)

LCO (continued)

The overlap between regulating banks provides more uniform rates of reactivity insertion and withdrawal, and is imposed to maintain acceptable power peaking during regulating CEA motion.

[For this facility, an OPERABLE power dependent insertion limit (PDIL) alarm circuit and regulating CEA group constitute the following:]

[For this facility, the following support systems are required OPERABLE to ensure PDIL alarm circuit and regulating CEA group OPERABILITY:]

[For this facility, the required support systems which upon their failure do not declare the PDIL alarm circuit and Regulating CEA group inoperable and their justification are as follows:]

APPLICABILITY

The shutdown and regulating CEA sequence, overlap, and physical insertion limits shall be maintained with the reactor in MODES 1 and 2. These limits must be maintained since they preserve the assumed power distribution, ejected CEA worth, SDM, and reactivity rate insertion assumptions. Applicability in MODES 3, 4, and 5 is not required, since neither the power distribution nor ejected CEA worth assumptions would be exceeded in these MODES. SDM is preserved in MODES 3, 4, and 5 by adjustments to the soluble boron concentration.

This LCO has been modified by a Note which permits the requirements of this LCO to be not applicable during the performance of SR 3.1.5.5. This SR requires that the CEA be moved at least every 92 days to verify their OPERABILITY. The individual CEAs are moved at least 5 inches and then returned to their original position.

A Note has been added to indicate that the Completion Time is on a Condition basis.

(continued)

BASES (continued)

ACTIONS

A.1 and A.2

If the CEAs are inserted between the long-term steady-state insertion limits and the transient insertion limits for intervals greater than 4 hours per 24-hour period and the short-term steady-state insertion limits are exceeded, peaking factors can develop that are of immediate concern (Ref. 7).

Additionally, since the CEAs can be in this condition without misalignment, penalty factors are not inserted in the core protection calculators (CPCs) to compensate for the developing peaking factors. Verifying the short-term steady-state insertion limits are not exceeded ensures that the peaking factors which do develop are within those allowed for continued operation. Fifteen minutes provides adequate time for the operator to verify if the short-term steady-state insertion limits are exceeded.

Experience has shown that rapid power increases in areas of the core in which the flux has been depressed may result in fuel damage as the LHR in those areas rapidly increases. Restricting the rate of THERMAL POWER increases to ≤ 5% RATED THERMAL POWER (RTP) per hour following CEA insertion beyond the long-term steady-state insertion limits ensures the power transients experienced by the fuel will not result in fuel failure (Ref. 8).

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action A.2 and LCO 3.1.5 apply.

B.1

With the regulating CEAs inserted between the long-term steady-state insertion limit and the transient insertion limit and approaching the 5 effective full power days (EFPDs) or 14 EFPDs limits, the core is approaching the acceptable limits placed on operation with flux patterns outside those assumed in the long-term burnup assumptions. In this case the CEAs must be returned to within the long-term steady-state insertion limits or the core must be placed in a condition in which the abnormal fuel burnup can not continue. Two hours is a reasonable time to return the CEAs to within the long-term steady-state insertion limits.

(continued)

BASES (continued)

ACTIONS (continued)

The required Completion Time of 2 hours from initial discovery of a regulating CEA group outside the limits until its restoration to within the long-term steady-state limits shown on the figures in the COLR allows sufficient time for borated water to enter the Reactor Coolant System (RCS) from the chemical addition and makeup systems, and to cause the regulating CEAs to withdraw to the acceptable region. Operation for another 2 hours outside the limits is reasonable based on limiting the potential xenon redistribution, the low probability of an accident occurring, and the steps required to complete the action.

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action B.1 and LCO 3.1.5 apply.

C.1 and C.2

With the Core Operating Units Supervisory System out-of-service, operation beyond the short-term steady-state insertion limits can result in peaking factors that could approach the DNB or local power density trip setpoints. Eliminating this condition within 2 hours limits the magnitude of the peaking factors to acceptable levels (Ref. 9). Restoring the CEAs to within the limit or reducing THERMAL POWER to that fraction of RTP that is allowed by CEA group position using the limits specified in the COLR, ensures acceptable peaking factors are maintained.

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action C.2 and LCO 3.1.5 apply.

D.1

During power operations SDM requirements are met by maintaining the shutdown CEAs fully withdrawn and maintaining the regulating CEAs above the transient insertion limit (also called the PDIL).

Satisfying these conditions ensures that initial operating conditions are no more severe than the initial conditions assumed in the accident analysis and that the minimum required SDM exists. This includes an allowance for the most reactive CEA which is assumed to be withdrawn from the

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

core. With the regulating CEAs inserted beyond the transient insertion limit, adequate SDM may not exist.

Restoration of the required SDM requires increasing the RCS boron concentration, because the regulating RODS may be inserted too far to provide sufficient negative reactivity. RCS boration must occur as described in Section B 3.1.1. The required Completion Time of 15 minutes to initiate boration is reasonable based on limiting the potential xenon redistribution, the low probability of an accident occurring, and the steps required to complete the action. This allows the operator sufficient time to align the required valves and to start the boric acid pumps. Boration will continue until the regulating rod group positions are restored to at least within the restricted operation region, which restores the minimum SDM capability.

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action D.1, Required Action D.2.1, Required Action D.2.2, and LCO 3.1.5 apply.

D.2.1 and D.2.2

Operation beyond the transient insertion limits results in a loss of SDM and excessive peaking factors. While boron addition to the RCS can ensure adequate SDM, the CEAs must be returned to above the transient insertion limits to eliminate the peaking problem. This can be accomplished by either restoring the CEAs to within the insertion limits (Required Action D.2.1) or reducing THERMAL POWER to less than or equal to that fraction of RTP that is allowed by CEA group position using the limits specified in the COLR (Required Action D.2.2). Two hours provides a reasonable time to accomplish this while limiting the peaking factors to acceptable levels. The Completion Time of 2 hours is reasonable, based on the low probability of an event occurring simultaneously with the limit out of specification, and on limiting the potential xenon redistribution.

E.1

With the PDIL circuit inoperable, performing SR 3.1.7.1, CEA position, within 1 hour and every 4 hours thereafter

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

ensures improper CEA alignments are identified before unacceptable flux distributions occur.

F.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should be commenced. The allowed time of 6 hours is reasonable, based on operating experience, to reach MODE 3 from full power in an orderly manner and without challenging plant systems. In MODE 3 the reactor is not critical and excessive power peaking cannot occur.

SURVEILLANCE REQUIREMENTS

SR 3.1.7.1

With the PDIL alarm circuit OPERABLE, verification of each regulating CEA group position every 12 hours is sufficient to detect CEA positions that may approach the limits, and provide the operator with time to undertake the required Action(s) should the sequence or insertion limits be found to be exceeded. The 12-hour frequency also takes into account the indication provided by the PDIL alarm circuit and other information about CEA group positions available to the operator in the control room.

SR 3.1.7.1 is modified by a Note that allows exception to SR 3.0.4. SR 3.0.4 is not applicable since the unit must be in the applicable MODES in order to perform Surveillances that demonstrate the LCO limits are met.

SR 3.1.7.2

Verification of the accumulated time of CEA group insertion between the long-term steady-state insertion limits and the transient insertion limits assures the cumulative time limits are not exceeded. The 24-hour Frequency ensures the operator identifies a time limit that is being approached before it is reached.

[For this facility, acceptable accumulated time of each CEA group insertion between the long-term steady-state insertion limits and the transient insertion limits is as follows;]

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.7.3

Demonstrating the PDIL alarm circuit OPERABLE verifies that the PDIL alarm circuit is functional. The 31-day Frequency takes into account other Surveillances being performed at shorter Frequencies which identify improper CEA alignments.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design," General Design Criterion 26, "Reactivity Limits."
2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
3. [Unit Name] Core Operating Limits Report, "[Title]."
4. [Unit Name] FSAR, Section [ ], "[Rod Ejection Accident, Accident Bases]"; Section [ ], "[Ejection Accident, Fuel Rod Damage]"; Section [ ], "[Thermal and Hydraulic Limits]."
5. [Unit Name] FSAR, Section [ ], "[Title]."
6. [Unit Name] FSAR, Section [ ], "[Title]."
7. [Unit Name] FSAR, Section [ ], "[Title]."
8. [Unit Name] FSAR, Section [ ], "[Title]."
9. [Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.8 Part-Length Control Element Assembly (CEA) Insertion Limits (Optional) (Digital)

BASES

BACKGROUND

The insertion limits of the part-length CEAs are initial assumptions in all safety analyses. The insertion limits directly affect core power distributions. The applicable criteria for these power distribution design requirements are 10 CFR 50, Appendix A, GDC 10, "Reactor Design" (Ref. 1), and 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Plants" (Ref. 2). Limits on part-length CEA insertion have been established, and all CEA positions are monitored and controlled during power operation to ensure that the power distribution defined by the design power peaking limits is preserved.

The regulating rods are used for precise reactivity control of the reactor. The positions of the regulating rods are normally controlled automatically by the Reactor Regulating System, but can also be manually controlled. They are capable of adding reactivity very quickly (compared to borating or diluting).

The power density at any point in the core must be limited to maintain specified acceptable fuel design limits, including limits that preserve the criteria specified in 10 CFR 50.46 (Ref. 2). Together, LCO 3.1.7, LCO 3.1.8, LCO 3.2.4, and LCO 3.2.5 provide limits on control component operation and on monitored process variables to ensure the core operates within the linear heat rate (LHR) (LCO 3.2.1), planar peaking factor (F_{xy}) (LCO 3.2.2), and departure from nucleate boiling ratio (LCO 3.2.4) limits in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3). Operation within the limits given in the COLR prevents power peaks that would exceed the loss-of-coolant accident (LOCA) limits derived by the Emergency Core Cooling System analysis. Operation within the F_{xy} and departure from nucleate boiling (DNB) limits given in the COLR prevents DNB during a loss of forced reactor coolant flow accident.

The establishment of limiting safety system settings and LCOs requires that the expected long- and short-term

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

behavior of the radial peaking factors be determined. The long-term behavior relates to the variation of the steady-state radial peaking factors with core burnup; it is affected by the amount of CEA insertion assumed, the portion of a burnup cycle over which such insertion is assumed, and the expected power-level variation throughout the cycle. The short-term behavior relates to transient perturbations to the steady-state radial peaks due to radial xenon redistribution. The magnitudes of such perturbations depend upon the expected use of the CEAs during anticipated power reductions and load maneuvering. Analyses are performed based on the expected mode of operation of the Nuclear Steam Supply System (base-loaded, maneuvering, etc.). From these analyses CEA insertions are determined, and a consistent set of radial peaking factors are defined. The long-term (steady-state) and short-term insertion limits are determined based upon the assumed mode of operation used in the analyses; they provide a means of preserving the assumptions on CEA insertions used. The long- and short-term insertion limits of LCO 3.1.8 are specified for the plant that has been designed primarily for base-loaded operation, but which has the ability to accommodate a limited amount of load maneuvering.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition I) and anticipated operational occurrences (Condition II). The regulating CEA insertion, part-length CEA insertion, AXIAL SHAPE INDEX (ASI), and AZIMUTHAL POWER TILT (T_q) LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a large-break LOCA, the peak cladding temperature must not exceed 2200°F (Ref. 2);

b. During a loss of forced reactor coolant flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition. This is referred to hereafter as the 95/95 DNB criterion;

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

c. During an ejected CEA accident, the fission-energy input to the fuel must not exceed 280 cal/gm (Ref. 4); and

d. The CEAs must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth CEA stuck fully withdrawn (GDC 26, Ref. 1).

Regulating CEA position, part-length CEA position, ASI, and T_q are process variables that together characterize and control the three-dimensional power distribution of the reactor core.

Fuel cladding damage does not occur when the core is operated outside these LCOs during normal operation. Fuel cladding damage could result, however, should an accident occur with simultaneous violation of one or more of these LCOs. Changes in the power distribution can cause increased power peaking and corresponding increased local linear heat rates.

The insertion limits satisfy of Criterion 2 of the NRC Interim Policy Statement in that they are initial conditions assumed in the safety analysis.

LCO

The limits on part-length CEA insertion as defined in the COLR (Ref. 3) must be maintained because they serve the function of preserving power distribution.

[For this facility an OPERABLE Part-Length CEA group and power dependent insertion limit (PDIL) alarm circuit constitute the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure Part-Length CEA group and PDIL Alarm circuitry OPERABILITY:]

[For this facility, the required support systems which upon their failure do not declare the Part-Length CEA-group or PDIL Alarm Circuitry inoperable, and their justification are as follows:]

(continued)

BASES (continued)

APPLICABILITY

The part-length insertion limits shall be maintained with the reactor in MODES 1 and 2. These limits must be maintained since they preserve the assumed power distribution. Applicability in MODES 3, 4, and 5 is not required, since the power distribution assumptions would not be exceeded in these MODES.

This LCO has been modified by a Note that permits the requirements of this LCO to be waived during the performance of SR 3.1.5.5. This SR requires that the CEAs be moved at least every 92 days to verify their OPERABILITY. The individual CEAs are moved at least 5 inches and then returned to their original position.

ACTIONS

A.1, A.2, and B.1

If the part-length CEA groups are inserted beyond the transient insertion limit or between the long-term (steady-state) insertion limit and the transient limit for 7 or more effective full power days (EFPDs) out of any 30-EFPD period or for 14 EFPDs or more out of any 365-EFPD period, flux patterns begin to develop, that are outside the range assumed for long-term fuel burnup. If allowed to continue beyond this limit, the peaking factors assumed as initial conditions in the accident analysis may be invalidated (Ref. 5). Restoring the CEAs to within limits or reducing THERMAL POWER to that fraction of RATED THERMAL POWER (RTP) that is allowed by CEA group position using the limits specified in the COLR, ensures that acceptable peaking factors are maintained.

Since these effects are cumulative, actions are provided to limit the total time the part-length CEAs can be out of limits in any 30-EFPD or 365-EFPD period. Since the cumulative out-of-limit times are in days, an additional 2 hours is a reasonable time to restore the part-length CEAs to within the allowed limits.

In the event that a CEA group is found inoperable, the CEA group is considered to be not within limits and Required Action A.2 and LCO 3.1.5 apply.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

C.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should commence. Four hours is a reasonable time, based on operating experience, to reduce power to ≤ 20 RTP from full power in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

Verification of each part-length CEA group position every 12 hours is sufficient to detect CEA positions that may approach the limits, and provide the operator with time to undertake the Required Action(s) should insertion limits be found to be exceeded. The 12-hour Frequency also takes into account the indication provided by the PDIL alarm circuit and other information about CEA group positions available to the operator in the control room.

SR 3.1.8.1 is modified by a Note that allows exception to SR 3.0.4. SR 3.0.4 is not applicable since the unit must be in the applicable MODES in order to perform surveillances that demonstrate the LCO limits are met.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 10, "Reactor Design"; General Design Criterion 26, "Reactivity Limits."

2. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Cooled Nuclear Power Reactors."

3. [Unit Name] Core Operating Limits Report, Section [ ], "[CEA Ejection Accident, Accident Bases]"; Section [ ], "[CEA Ejection Accident, Fuel Rod Damage"; Section [ ], "[Thermal and Hydraulic Limits]."

(continued)

(continued)

BASES (continued)

REFERENCES (continued)	4.	[Unit Name] FSAR, Section [ ], "[Title]."
	5	[Unit Name] FSAR, Section [ ], "[Title]."

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.9 Special Test Exceptions (STE)—SHUTDOWN MARGIN (SDM) (Digital)

BASES

BACKGROUND

The primary purpose of MODES 2 and 3 STE is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine the control element assembly (CEA) worth and SDM.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC for the purpose of conducting tests and experiments are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Provide assurance that the facility has been adequately designed;

b. Validate the analytical models used in design and analysis;

c. Verify assumptions used for predicting plant response;

d. Provide assurance that installation of equipment in the facility has been accomplished in accordance with the design; and

e. Verify that operating and emergency procedures are adequate.

To accomplish these objectives, testing prior to initial criticality, after each refueling shutdown, and during

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

startup, low power operation, power ascension, and at-power operation is required. The requirements for PHYSICS TESTS for reload fuel cycles assure that the operating characteristics of the core are consistent with the design predictions and that the core can be operated as designed (Ref. 5).

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that the design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long-term power operation. Examples of PHYSICS TESTS include determination of critical boron concentration, CEA group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

The acceptance criteria to allow suspension of certain LCOs for PHYSICS TESTS are that fuel damage criteria are not exceeded. Even if an accident occurs during PHYSICS TESTS with one or more LCOs suspended, fuel damage criteria are preserved because adequate limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines the requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS 19.6.1-1985 (Ref. 4). PHYSICS TESTS for reload fuel cycles are given in Table 1 of ANSI/ANS 19-6.1-1985. Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TESTS possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved. In this test, the following LCOs are suspended:

a. LCO 3.1.1, "SHUTDOWN MARGIN—T_{avg} > 200°F";

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

b. LCO 3.1.5, "CEA Alignment";

c. LCO 3.1.7, "Regulating CEA Insertion Limits"; and

d. LCO 3.1.8, "Part-Length CEA Insertion Limits.

Therefore, this LCO places limits on the minimum amount of CEA worth required to be available for reactivity control when CEA worth measurements are performed.

The individual LCOs cited above govern CEA group height, insertion, and alignment. Additionally, the LCOs governing Reactor Coolant System flow, reactor inlet temperature T_c, and pressurizer pressure contribute to maintaining departure from nucleate boiling (DNB) parameter limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss-of-coolant accident (LOCA) are specified in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref. 6). The criteria for the loss of forced reactor coolant flow accident are specified in the Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

SRs are placed as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these SRs allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

Requiring that shutdown reactivity equivalent to at least the highest estimated CEA worth be available for trip insertion from the OPERABLE CEAs, provides a high degree of assurance that shutdown capability is maintained for the most challenging postulated accident, a stuck CEA. Since LCO 3.1.1, "SHUTDOWN MARGIN," is suspended, however, there is not the same degree of assurance during this test that the reactor would always be shut down if the highest worth CEA was stuck out and calculational uncertainties or the estimated highest CEA worth was not as expected (the single failure criteria is not met). This situation is judged acceptable, however, because specified acceptable fuel

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

damage limits are still met. The risk of experiencing a stuck CEA and subsequent criticality is reduced during this PHYSICS TEST exception by the requirements to determine CEA positions every 2 hours; by the trip of each CEA to be withdrawn within 24 hours prior to suspending the SDM; and by ensuring that shutdown reactivity is available equivalent to the reactivity worth of the estimated highest worth CEA, Ref. 5.

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, AZIMUTHAL POWER TILT, and AXIAL SHAPE INDEX, which represent initial condition input (power peaking) to the accident analysis. Also involved are the movable control components (shutdown and regulating CEAs), which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the CORE OPERATING LIMITS REPORT (Ref. 6).

PHYSICS TESTS meet the criteria for inclusion in Technical Specifications since the components and process variable LCOs suspended during PHYSICS TESTS meet Criteria 1, 2, and 3 of the NRC Interim Policy Statement.

LCO

This LCO provides that a minimum amount of CEA worth is immediately available for reactivity control when CEA worth measurement tests are performed. This Special Test Exception is required to permit the periodic verification of the actual-versus-predicted core reactivity condition occurring as a result of fuel burnup or fuel cycling operations. The SDM requirements of LCO 3.1.1 and the regulating CEA insertion limits of LCO 3.1.7 may be suspended.

[For this facility, an OPERABLE CEA constitutes the following:]

[For this facility, the following support systems are required OPERABLE to ensure that the LCO and SR conditions are met: [List]]

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, the required support systems which upon their failure do not result in CEA inoperability or the condition of this LCO to not be met and their justification are as follows: [List]]

APPLICABILITY

This LCO is applicable in MODES 2 and 3. Although CEA worth testing is conducted in MODE 2, sufficient negative reactivity is inserted during the performance of these tests to result in temporary entry into MODE 3. Because the intent is to immediately return to MODE 2 to continue CEA worth measurements, the Special Test Exception allows limited operation to 6 consecutive hours in MODE 3 without having to borate to meet the SDM requirements of LCO 3.1.1.

ACTIONS

A.1

With any CEA not fully inserted and less than the minimum required reactivity equivalent available for insertion, or with all CEAs inserted and the reactor subcritical by less than the reactivity equivalent of the highest worth CEA, restoration of the minimum SDM requirements must be accomplished by increasing the RCS boron concentration. The required Completion Time of 15 minutes to initiate boration allows the operator sufficient time to align the valves and start the boric acid pumps and is consistent with the Completion Time of LCO 3.1.1.

In the event that any withdrawn CEA is found to be inoperable, the Required Action A.1 applies.

SURVEILLANCE REQUIREMENTS

SR 3.1.9.1

Verification of the position of each partially or fully withdrawn full-length or part-length CEA is necessary to ensure that the minimum negative reactivity requirements for insertion on a trip are preserved. A two-hour Frequency is sufficient for the operator to verify that each CEA position is within the acceptance criteria.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.9.2

Prior demonstration that each CEA to be withdrawn from the core during PHYSICS TESTS is capable of full insertion when tripped from at least a 50% withdrawn position provides assurance that the CEA will insert on a trip signal. The 7-day requirement ensures that the CEAs are OPERABLE prior to reducing SHUTDOWN MARGIN to less than the limits of LCO 3.1.1.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix B, Section XI (Test Control), "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants."

2. Title 10, Code of Federal Regulations, Part 50.59, "Changes, Tests, and Experiments."

3. Regulatory Guide 1.68, Revision 2, "Initial Test Programs for Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission, August 1978.

4. ANSI/ASME-19.6.1-1985, "Reload Startup PHYSICS TESTS for Pressurized Water Reactors," American National Standards Institute, December 13, 1985.

5. [Unit Name] FSAR, Section [14], "[Testing Requirements]."

6. [Unit Name] Core Operating Limits Report, "[Title]".

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.10 PHYSICS TEST Exceptions—MODES 1 & 2 (Digital)

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 Special Test Exceptions is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are conducted to determine specific reactor core characteristics.

Section XI of 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants" (Ref. 1), requires that a test program be established to ensure that structures, systems, and components will perform satisfactorily in service. All functions necessary to ensure that specified design conditions are not exceeded during normal operation and anticipated operational occurrences (AOOs) must be tested. Testing is required as an integral part of the design, fabrication, construction, and operation of the power plant. Requirements for notification of the NRC for the purpose of conducting tests and experiments are specified in 10 CFR 50.59, "Changes, Tests, and Experiments" (Ref. 2).

The key objectives of a test program are to (Ref. 3):

a. Provide assurance that the facility has been adequately designed;

b. Validate the analytical models used in design and analysis;

c. Verify assumptions used for predicting plant response;

d. Provide assurance that installation of equipment in the facility has been accomplished in accordance with design; and

e. Verify that operating and emergency procedures are adequate.

To accomplish these objectives, testing prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at-power

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

operation is required. The requirements for PHYSICS TESTS for reload fuel cycles assure that the operating characteristics of the core are consistent with the design predictions and that the core can be operated as designed (Ref. 4).

PHYSICS TESTS procedures are written and approved in accordance with established formats. The procedures include all information necessary to permit a detailed execution of testing required to ensure that design intent is met. PHYSICS TESTS are performed in accordance with these procedures and test results are approved prior to continued power escalation and long-term power operation. Examples of PHYSICS TESTS include determination of critical boron concentration, CEA group worths, reactivity coefficients, flux symmetry, and core power distribution.

APPLICABLE SAFETY ANALYSES

It is acceptable to suspend certain LCOs for PHYSICS TESTS because fuel damage criteria are not exceeded. Even if an accident occurs during PHYSICS TESTS with one or more LCOs suspended, fuel damage criteria are preserved because the limits on power distribution and shutdown capability are maintained during PHYSICS TESTS.

Reference 5 defines requirements for initial testing of the facility, including PHYSICS TESTS. Requirements for reload fuel cycle PHYSICS TESTS are defined in ANSI/ANS 19.6.1-1985 (Ref. 4). Although these PHYSICS TESTS are generally accomplished within the limits of all LCOs, conditions may occur when one or more LCOs must be suspended to make completion of PHYSICS TEST possible or practical. This is acceptable as long as the fuel design criteria are not violated. As long as the linear heat rate (LHR) remains within its limit, fuel design criteria are preserved even when one or more of the limits specified in the following LCOs are suspended:

a. LCO 3.1.4, "Moderator Temperature Coefficient (MTC)";

b. LCO 3.1.5, "CEA Alignment";

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

c. LCO 3.1.6, "Shutdown CEA Insertion Limits;"

d. LCO 3.1.7, "Regulating CEA Insertion Limits;"

e. LCO 3.1.8, "Part-Length CEA Insertion Limits;"

f. LCO 3.2.2, "Planar Radial Peaking Factors;" and,

g. LCO 3.2.3, "AZIMUTHAL POWER TILT (T_q)."

The safety analysis (Ref. 7) places limits on allowable THERMAL POWER during PHYSICS TESTS and requires that the LHR and the departure from nucleate boiling (DNB) parameter be maintained within limits. The power plateau of < 85% Rated Thermal Power (RTP) and the associated trip setpoints are required to ensure [explain].

The individual LCOs governing CEA group height, insertion and alignment, AXIAL SHAPE INDEX (ASI), total planar radial Peaking Factor, total integrated radial peaking factor, and T_q preserve the LHR limits. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature (T_c), and pressurizer pressure contribute to maintaining DNB parameter limits. The initial condition criteria for accidents sensitive to core power distribution are preserved by the LHR and DNB parameter limits. The criteria for the loss-of-coolant accident (LOCA) are specified in 10 CFR 50.46 "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors" (Ref.6). The criteria for the loss of forced reactor coolant flow accident are specified in Reference 7. Operation within the LHR limit preserves the LOCA criteria; operation within the DNB parameter limits preserves the loss of flow criteria.

During PHYSICS TESTS, one or more of the LCOs that normally preserve the LHR and DNB parameter limits may be suspended. The results of the accident analysis are not adversely impacted, however, if LHR and DNB parameters are verified to be within their limits while the LCOs are suspended. Therefore, SRs are placed as necessary to ensure that LHR and DNB parameters remain within limits during PHYSICS TESTS. Performance of these SRs allows PHYSICS TESTS to be conducted without decreasing the margin of safety.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

PHYSICS TESTS include measurement of core parameters or exercise of control components that affect process variables. Among the process variables involved are total planar radial peaking factor, total integrated radial peaking factor, T_q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the movable control components (shutdown and regulating CEAs), which affect power peaking and are required for shutdown of the reactor. The limits for these variables are specified for each fuel cycle in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 8).

PHYSICS TESTS meet the criteria for inclusion in Technical Specifications, since the component and process variable LCOs suspended during PHYSICS TESTS meet Criteria 1, 2, and 3 of the NRC Interim Policy Statement.

LCO

This LCO permits individual CEAs to be positioned outside of their normal group heights and insertion limits during the performance of PHYSICS TESTS, such as those required to:

a. Measure CEA worth;

b. Determine the reactor stability index and damping factor under xenon oscillation conditions;

c. Determine power distributions for non-normal CEA configurations;

d. Measure rod shadowing factors; and

e. Measure temperature and power coefficients.

Additionally, it permits the center CEA to be misaligned during PHYSICS TESTS required to determine the isothermal temperature coefficient (ITC), MTC, and power coefficient.

The requirements of LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, LCO 3.1.7, LCO 3.1.8, LCO 3.2.2, LCO 3.2.3, may be suspended during the performance of PHYSICS TESTS provided:

a. THERMAL POWER is restricted to test power plateau which shall not exceed 85% RTP, and

(continued)

(continued)

BASES (continued)

LCO (continued)	b. In MODE 1 > 20% RTP, the limits of LCO 3.2.1, "Linear Heat Rate (LHR)," are maintained and determined as specified in SR 3.1.10.1
APPLICABILITY	This LCO is applicable in MODES 1 and 2 because the reactor must be critical at various THERMAL POWER levels to perform the PHYSICS TESTS described in the LCO section. Limiting the test power plateau to less than 85% RTP ensures that LHRs are maintained within acceptable limits.

ACTIONS

A.1 and B.1

If THERMAL POWER exceeds the test power plateau, or the LHR requirements of LCO 3.2.1 are exceeded in MODE 1, THERMAL POWER must be reduced to restore the additional thermal margin provided by the reduced THERMAL POWER. The 15-minute Completion Time ensures that prompt action is taken to reduce THERMAL POWER to within acceptable limits.

C.1 and C.2

If Required Actions A.1 or B.1 cannot be completed within the required Completion Time, PHYSICS TESTS must be suspended within 1 hour and the reactor must be placed in MODE 3. Allowing 1 hour to suspend PHYSICS TESTS allows the operator sufficient time to change any abnormal CEA configuration back to within the limits of LCO 3.1.5, LCO 3.1.6 and LCO 3.1.7, prior to placing the reactor in MODE 3 within 6 hours. This increases thermal margin and is consistent with the Required Actions of the power distribution LCOs.

The required Completion Time of 6 hours is adequate to perform a controlled shutdown and is consistent with the power distribution LCO Completion Times.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.1.10.1

Monitoring LHR and the departure from nucleate boiling ratio (DNBR) ensures that the LHR and DNBR limits are not exceeded. Refer to LCO B 3.1.4, "Power Distribution Limits," for a discussion of the Bases for these parameters. Continuous monitoring is accomplished by the Core Operating Limits Supervisory System (COLSS), which generates margin limits based on the LHR and the DNBR and will generate a COLSS margin alarm should a limit be exceeded. This Surveillance is not applicable at < 20% RTP because adequate LHR and DNBR margins exist up to this power level.

SR 3.1.10.2

Verifying that THERMAL POWER is equal to or less than that allowed by the test power plateau, as specified in the PHYSICS TEST procedure and required by the safety analysis, ensures that adequate LHR and DNBR margins are maintained while LCOs are suspended. The 1-hour Frequency is sufficient, based upon the slow rate of power change and increased operational controls in place during PHYSICS TESTS. Monitoring LHR ensures that the limits are not exceeded. Refer to LCO B 3.1.4, "Power Distribution Limits," for a discussion of the Bases for these parameters.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix B, Section XI (Test Control), "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants."

2. Title 10, Code of Federal Regulations, Part 50.59, "Changes, Tests, and Experiments."

3. Regulatory Guide 1.68, Revision 2, "Initial Test Programs for Water-Cooled Nuclear Power Plants," U.S. Nuclear Regulatory Commission, August 1978.

4. ANSI/ANS-19.6.1-1985, "Reload Startup PHYSICS TESTS for Pressurized Water Reactors," American National Standards Institute, December 13, 1985.

(continued)

(continued)

BASES (continued)

REFERENCES (continued)

5. [Unit Name] FSAR, Section [14], "[Testing Requirements]."

6. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

7. [Unit Name] FSAR, Section [15.3.2.i], "[Title]."

8. [Unit Name] Core Operating Limits Report, "[Title]."

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR) (Analog)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss of flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., a CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in control of the axial power distribution.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the LHR and Departure from Nucleate Boiling (DNB).

The limits on the LHR, the Total Planar Radial Peaking Factor (F^T_{xy}), the Total Integrated Radial Peaking Factor (F^T_r), the AZIMUTHAL POWER TILT (T_q), and the AXIAL SHAPE INDEX (ASI) represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System and the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3).

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.6 and LCO 3.1.7 are satisfied;

b. The (T_q) restrictions of LCO 3.2.4 are satisfied; and

c. The F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a direct measure of the peaking factors and the alarms which have been established for the individual incore detector segments ensure that the peak LHRs will be maintained within

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062;

b. An engineering uncertainty factor of 1.03;

c. An allowance of 1.002 for axial fuel densification and thermal expansion; and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 4, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (Ref. 4, GDC 10). This is referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn (Ref. 4, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F^T_{xy}, F^T_r, and T_q limits specified in the COLR (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses.

Fuel-cladding damage does not occur while operating at conditions outside the limits of these LCOs during normal operation. Fuel-cladding damage could result, however, should an accident occur from initial conditions outside the limits of these LCOs. The potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increase local LHRs.

LHR, ASI, F^T_{xy}, F^T_r, and T_q satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and Departure from Nucleate Boiling Ratio (DNBR) operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on the LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F.

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, an OPERABLE Incore Detector Monitoring System and Excore Detector Monitoring System constitute the following:]

[For this facility, the following support systems are required OPERABLE to ensure Incore Detector Monitoring System and Excore Detector Monitoring System OPERABILITY:]

[For this facility, those required support systems which upon their failure do not declare the Incore Detector Monitoring System and Excore Detector Monitoring System inoperable and their justification are as follows:]

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1 and A.2

With the LHR exceeding its limit, excessive fuel damage could occur following an accident. In this condition, prompt action must be taken to reduce the LHR to within the specified limits. [For this facility, LHR is restored to within its limits by the following actions:] Fifteen minutes to initiate corrective actions to reduce the LHR allows the operator sufficient time to evaluate core conditions and to initiate proper corrective actions. One hour to restore the LHR to within its specified limits is reasonable and ensures that the core does not continue to operate in this condition.

B.1

If the LHR cannot be returned to within its specified limit or LHR can not be determined because of Incore Detector and Excore Detector Monitoring Systems inoperability, THERMAL POWER must be reduced. The change to MODE 2 ensures that the core is operating within its thermal limits and places

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

the core in a conservative condition. Six hours is a reasonable amount of time to allow, based on operating experience, to reach MODE 2 in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.1.1

Continuous monitoring of the LHR is provided by the Incore Detector Monitoring System and the Excore Detector Monitoring System. Either of these two core power distribution monitoring systems provides adequate monitoring of the core power distribution and is capable of verifying that the LHR does not exceed its specified limits. A Note has been added to indicate that the provisions of SR 3.0.4 do not apply for this SR.

SR 3.2.1.2 and SR 3.2.1.3

Performance of these SRs is necessary to ensure that the Excore Detector Monitoring System can accurately monitor the LHR. Therefore, these SRs are only applicable when the Excore Detector Monitoring System is being used to determine the LHR. [For this facility the purpose of the SRs is as follows:] [For this facility the justification for performing SR 3.2.1.2 every 12 hours and SR 3.2.1.3 and SR 3.3.1.4 every 31 days is as follows:]

SR 3.2.1.4 and SR 3.2.1.5

Performance of these two SRs is necessary to ensure that the Incore Detector Monitoring System can accurately monitor LHR. Therefore, they are only applicable when the Incore Detector Monitoring System is being used to determine the LHR. [For this facility, the purpose of SRs is as follows:] [For this facility, the justification for performing these surveillances every 31 days is as follows:]

A Note has been added to each of the SRs to indicate that the provisions of SR 3.0.4 do not apply.

(continued)

BASES (continued)

REFERENCES

1. [Unit Name] FSAR, Chapter [15], "[Accident Analysis]."
2. [Unit Name] FSAR, Chapter [6], "[Emergency Core Cooling System]."
3. [Unit Name] Core Operating Limits Report.
4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."
5. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 Total Planar Radial Peaking Factor (F^T_{xy}) (Analog)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings (LSSSs) and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in control of the axial power distribution.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) Departure from Nucleate Boiling (DNB).

The limits on the LHR, the F^T_{xy}, the Total Integrated Radial Peaking Factor (F^T_r), AZIMUTHAL POWER TILT (T_q), and the AXIAL SHAPE INDEX (ASI) represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System and the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3).

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.6 and 3.1.7 are satisfied;

b. The T_q restrictions of LCO 3.2.4 are satisfied; and

c. The F^T_{xy} does not exceed the limits of this LCO.

The Incore Detector Monitoring System continuously provides a direct measure of the peaking factors, and the alarms which have been established for the individual incore detector segments ensure that the peak LHRs will be maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in the conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062;

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

b. An engineering uncertainty factor of 1.03;

c. An allowance of 1.002 for axial fuel densification and thermal expansion; and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 4, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (Ref. 4, GDC 10), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. []); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck, fully withdrawn (Ref. 4, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions such that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F^T_{xy}, F^T_r, and T_q limits specified in the COLR (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses.

Fuel-cladding damage does not occur while at conditions outside the limits of these LCOs during normal operation. Fuel-cladding damage could result, however, should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.

LHR, ASI, F^T_{xy}, F^T_r, and T_q satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and Departure from Nucleate Boiling Ratio (DNBR) operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on the LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F.

[For this facility, an OPERABLE Incore Detector Monitoring System constitutes the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure Incore Detector Monitoring System OPERABILITY:]

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, those required support systems which, upon their failure, do not require declaring the Incore Detector Monitoring System inoperable and their justification are as follows:]

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analyses to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1 and A.2

The limitations on F^T_{xy} provided in the COLR ensure that the assumptions used in the analysis for establishing the LHR, LCO, and LSSS remain valid during operation at the various allowable CEA group insertion limits. If F^T_{xy} exceeds its basic limitation, operation may continue under the additional restrictions imposed by these Required Actions (reducing THERMAL POWER and withdrawing CEAs to or beyond the long-term steady-state insertion limits of LCO 3.1.7) since these additional restrictions provide adequate provisions to assure that the assumptions used in establishing the LHR, LCO, and LSSS remain valid (Ref. 3). Six hours to return F^T_{xy} to within its limit is reasonable and ensures that all CEAs meet the long-term steady-state insertion limits of LCO 3.1.7, "Regulating CEAs." [For this facility, the justification for the Completion Time is as follows:]

B.1

If F^T_{xy} cannot be returned to within its limit, or F^T_{xy} cannot be determined because of Incore Detector Monitoring System inoperability, THERMAL POWER must be reduced. A change to MODE 3 ensures that the core is operating within its thermal limits and places the core in a conservative condition. Six hours is a reasonable amount of time to allow, based on operating experience, to reach MODE 3 in an orderly manner and without challenging plant systems.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.2.2.1

The periodic surveillance requirements for determining the calculated F^T_{xy} provides assurance that the F^T_{xy} remains within the range assumed in the analysis throughout the fuel cycle. Determining the measured F^T_{xy} after each fuel loading prior to exceeding 70% of RATED THERMAL POWER (RTP) provides additional assurance that the core was properly loaded.

Performance of the surveillance every 31 days of accumulated operation in MODE 1 ensures that unacceptable changes in the F^T_{xy} are promptly detected. [For this facility, the justification for the 31-day Frequency is as follows:].

This surveillance can only be accomplished after THERMAL POWER exceeds 20% RTP because the incore detectors are not available below 20% RTP. Therefore, entry into the applicable MODE will occur prior to the completion of this surveillance.

SR 3.2.2.1 is modified by two Notes. The first Note permits entry into MODE 1 to perform this SR. [For this facility, the reasons for the second Note in the SR are as follows:].

SR 3.2.2.2 and SR 3.2.2.3

Measuring the value of F_{xy} and T_q each time a calculated value of F^T_{xy} is required provides assurance that the calculated value of F^T_{xy} accurately reflects the condition of the core. [For this facility the reasons for the above are as follows:].

The Frequency for these surveillances is in accordance with the Frequency requirements of SR 3.2.2.1.

REFERENCES

1. [Unit Name] FSAR, Chapter [15], "[Accident Analysis]."
2. [Unit Name] FSAR, Chapter [6], "[Emergency Core Cooling System]."
3. [Unit Name] Core Operating Limits Report.

(continued)

(continued)

BASES (continued)

REFERENCES (continued)

4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

5. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 Total Integrated Radial Peaking Factor (F_r^T) (Analog)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings (LSSSs) and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in control of the axial power distribution.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and Departure from Nucleate Boiling (DNB).

The limits on the LHR, the Total Planar Radial Peaking Factor (F^T_{xy}), the F^T_r, the AZIMUTHAL POWER TILT (T_q), and the AXIAL SHAPE INDEX (ASI) represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System and the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3).

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.6 and LCO 3.1.7 are satisfied;

b. The T_q restrictions of LCO 3.2.4 are satisfied; and

c. The F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a direct measure of the peaking factors, and the alarms which have been established for the individual incore detector segments ensure that the peak LHRs will be maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062;

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

b. An engineering uncertainty factor of 1.03;

c. An allowance of 1.002 for axial fuel densification and thermal expansion; and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 4, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (Ref. 4, GDC 10), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck full withdrawn (Ref. 4, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F_{xy}^T, F_r^T, and T_q limits specified in the COLR (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analysis.

Fuel-cladding damage does not occur while at conditions outside the limits of these LCOs during normal operation. Fuel-cladding damage could result, however, should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution cause increased power peaking and correspondingly increased local LHRs.

LHR, ASI, F_{xy}^T, F_r^T, and T_q satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and the measured variables used as inputs to the LHR and Departure from Nucleate Boiling Ratio (DNBR) operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on the LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F.

[For this facility, an OPERABLE Incore Detector Monitoring System constitutes the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure Incore Detector Monitoring System OPERABILITY:]

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, those required support systems which, upon their failure, do not require declaring the Incore Detector Monitoring System inoperable and their justification are as follows:]

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1, A.2, and A.3

The limitations on F_r^T provided in the COLR ensure that the assumptions used in the analysis for establishing the ASI, LCO, and LSSS remain valid during operation at the various allowable CEA group insertion limits. If F_r^T exceeds its basic limitation, operation may continue under the additional restrictions imposed by the Required Actions (reducing THERMAL POWER; withdrawing CEAs to or beyond the long-term steady-state insertion limits of LCO 3.1.7; and establishing a revised upper THERMAL POWER limit) since these additional restrictions provide adequate provisions to assure that the assumptions used in establishing the LHR, LCO, and LSSS remain valid (Ref. 3). Six hours to return F_r^T to within its limits is reasonable and ensures that all CEAs meet the long-term steady-state insertion limits of LCO 3.1.7, "Regulating CEAs." [For this facility, the justification for the Completion Time is as follows:]

B.1

If F_r^T cannot be returned to within its limit or F_r^T cannot be determined because of Incore Detector Monitoring System inoperability, THERMAL POWER must be reduced. A change to MODE 3 ensures that the core is operating within its thermal limits and places the core in a conservative condition. Six

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

hours is a reasonable amount of time to allow, based on operating experience, to reach MODE 3 in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.3.1

The periodic surveillance requirements for determining the calculated F_r^T provides assurances that the F_r^T remains within the range assumed in the analysis throughout the fuel cycle. Determining the measured F_r^T once after each fuel loading prior to exceeding 70% of RATED THERMAL POWER (RTP) provides additional assurance that the core was properly loaded.

Performance of the surveillance every 31 days of accumulated operation in MODE 1 ensures that unacceptable changes in the F_r^T are promptly detected. [For this facility, the 31-day Frequency is justified as follows:]

This surveillance must be accomplished after THERMAL POWER exceeds 20% of RTP because the incore detectors are not available below 20% RTP. Therefore, entry in the applicable MODE will occur prior to the completion of this surveillance.

SR [3.2.3.1] is modified by two Notes. The first Note permits entry into MODE 1 to perform this SR. [For this facility, the reasons for the second Note in the SR are as follows:]

SR 3.2.3.2 and SR 3.2.3.3

Measuring the value of F_r^T and T_q each time a calculated value of F_r^T is required provides assurance that the calculated value of F_r^T accurately reflects the condition of the core. [For this facility this is because:]

The Frequency for these surveillances is in accordance with the requirements of SR 3.2.3.1.

(continued)

BASES (continued)

REFERENCES

1. [Unit Name] FSAR, Chapter [15], "Accident Analysis."

2. [Unit Name] FSAR, Chapter [6], "Emergency Core Cooling System."

3. [Unit Name] Core Operating Limits Report.

4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

5. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 AZIMUTHAL POWER TILT (T_q) (Analog)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in control of the axial power distribution.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and Departure from Nucleate Boiling (DNB).

The limits on the LHR, the Total Planar Radial Peaking Factor (F^T_{xy}), the Total Integrated Radial Peaking Factor (F^T_r), the T_q, and the AXIAL SHAPE INDEX (ASI) represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System and the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LCR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron detectors and verifying that the ASI is maintained within the allowable limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3).

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.6 and LCO 3.1.7 are satisfied;

b. The T_q restrictions of LCO 3.2.4 are satisfied; and

c. The F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a direct measure of the peaking factors, and the alarms which have been established for the individual incore detector segments ensure that the peak LHRs will be maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062;

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

b. An engineering uncertainty factor of 1.03;

c. An allowance of 1.002 for axial fuel densification and thermal expansion; and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation (Condition 1) and AOOs (Condition 2) (Ref. 4, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (Ref. 4, GDC 10), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission-energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn (Ref. 4, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analysis (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the Reactor Control System ensure that these criteria are met as long as the core is operated within the ASI, F^T_{xy}, F^T_r, and T_q limits specified in the COLR (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses.

Fuel-cladding damage does not occur while at conditions outside these LCOs during normal operation. Fuel-cladding damage could result, however, should an accident occur from initial conditions outside the limits of these LCOs. Changes in the power distribution cause increased power peaking and correspondingly increased local LHRs.

LHR, ASI, F^T_{xy}, F^T_r, and T_q satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and the measured variables used as inputs to the LHR and Departure from Nucleate Boiling Ratio (DNBR) operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on the LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F.

[For this facility, an OPERABLE Incore Detector Monitoring System constitutes the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure Incore Detector Monitoring System OPERABILITY]

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, those required support systems which, upon their failure, do not require declaring the Incore Detector Monitoring System inoperable and their justification are as follows:]

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on core power distribution.

ACTIONS

A.1 and A.2

If the measured T_q is greater than [0.03] and less than 0.10, the calculation of T_q may be non-conservative. T_q must be restored within 2 hours or F_{xy}^T and F_r^T must be determined to be within the limits of LCO 3.2.2 and LCO 3.2.3 within 2 hours and determined to be within these limits every 8 hours thereafter as long as T_q is out of limits. Two hours is sufficient time to allow the operator to reposition CEAs, and significant radial xenon redistribution will not occur within this time. [For this facility, the justification for the 8-hour Completion Time is as follows:]

[For this facility, T_q is restored to within its limits by the following actions:]

B.1, B.2.1, B.2.2, and B.2.3

With $T_q > 0.10$, F_{xy}^T and F_r^T must be within their specified limits within 2 hours to ensure that acceptable flux peaking factors are maintained. Based on operating experience, 1 hour is sufficient time for the operator to evaluate these factors. If F_{xy}^T and F_r^T are within limits, operation may proceed for up to 2 hours while attempts are made to restore T_q to within its limit. [For this facility , T_q is restored to within its limits by the following actions:] [For this facility, the justification of 2 hours to restore T_q within its limit is as follows:]

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

If $T_q \leq 0.03$ cannot be achieved, it may still be desirable to retain the ability to operate the reactor. In the case of a tilt generated to be a CEA misalignment, it allows recovery of the CEA while continuing to operate. Except as a result of CEA misalignment, a T_q of greater than 0.10 is not expected; if it should occur, continued operation of the reactor may be necessary to discover the cause of the tilt. If this occurs, operation is restricted to only those conditions required to identify the cause of the tilt. It is necessary to explicitly account for power asymmetries because the radial power peaking factors used in the core power distribution calculations are based on an untilted power distribution.

If the T_q is not restored to within its limits, the reactor will continue to operate with an axial power distribution mismatch. Continued operation in this configuration may induce an axial xenon oscillation which will result in increased linear heat generation rates when the xenon redistributes. If T_q cannot be restored to within its limits within 2 hours, reactor power must be reduced. Reducing THERMAL POWER to < 20% RATED THERMAL POWER (RTP) within 2 hours provides conservative protection from increased peaking due to potential xenon redistribution. Required Action B.2.1 is modified by two Notes which require all subsequent actions be performed once Required Action B.2.1 is entered. This ensures corrective action is taken before unrestricted power operation resumes. Following THERMAL POWER reduction < 20% RTP, T_q must be restored $\leq$ [0.03] before THERMAL POWER is increased (Required Action B.2.2.1). This Required Action prevents the operator from increasing THERMAL POWER above the conservative limit when the condition, T_q outside its limits, has existed but allows the unit to continue operation for diagnostic purposes. The Completion Time of Required Action B.2.2.1 is modified with a note to indicate that the cause of the out-of-limit condition must be corrected prior to increasing THERMAL POWER. Also, this note indicates that subsequent power operation above 20% RTP may proceed provided that the measured T_q is verified $\leq$ [0.03] at least once per hour for 12 hours, or until verified at 95% of RTP. [For this facility, the 12-hour verification of $T_q \leq$ [0.03] is justified as follows:]

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

C.1

If Required Actions and associated Completion Times are not met, or F^T_{xy}, F^T_r or T_q cannot be determined because of Incore Detector Monitoring System inoperability, THERMAL POWER must be reduced. A change to MODE 3 ensures that the core is operating within its thermal limits and places the core in a conservative condition. Six hours is a reasonable amount of time to allow, based on operating experience, to reach MODE 3 in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.4.1

T_q must be calculated at 12-hour intervals. Some tilt events are detectable in their own right, however. Therefore, [for this facility, the purpose of this statement as related to the 12-hour Frequency is as follows:]. Also, the 12-hour Frequency prevents significant xenon redistribution.

[For this facility, the Frequency is justified as follows:]

REFERENCES

1. [Unit Name] FSAR, Chapter [15], "Accident Analysis."

2. [Unit Name] FSAR, Chapter [6], "Emergency Core Cooling System.

3. [Unit Name] Core Operating Limits Report.

4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

5. Title 10, Code of Federal Regulations, Part 50, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.5 AXIAL SHAPE INDEX (ASI) (Analog)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analysis. Specifically, operation within the limits imposed by this LCO limits potential fuel cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss of flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., a CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings (LSSSs) and this LCO are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in control of the axial power distribution.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and Departure from Nucleate Boiling (DNB).

The limits on the LHR, the Total Planar Radial Peaking Factor (F^T_{xy}), the Total Integrated Radial Peaking Factor (F^T_r), the Azimuthal Power Tilt (T_q), and the ASI represent limits within which the LHR algorithms are valid. These limits are obtained directly from the core reload analysis.

Either of the two core power distribution monitoring systems, the Excore Detector Monitoring System and the Incore Detector Monitoring System, provide adequate monitoring of the core power distribution and are capable of verifying that the LHR does not exceed its limits. The Excore Detector Monitoring System performs this function by continuously monitoring the ASI with the OPERABLE quadrant symmetric excore neutron flux detectors and verifying that the ASI is maintained within the allowable limits specified in the COLR (Ref. 3).

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.6 and LCO 3.1.7 are satisfied;

b. The T_q restrictions of LCO 3.2.4 are satisfied; and

c. The F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a direct measure of the peaking factors and the alarms which have been established for the individual incore detector segments ensure that the peak LHRs will be maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, for:

a. A measurement calculational uncertainty factor of 1.062;

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

b. An engineering uncertainty factor of 1.03;

c. An allowance of 1.002 for axial fuel densification and thermal expansion; and

d. A THERMAL POWER measurement uncertainty factor of 1.02.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation (Condition 1) and AOOs (Condition 2) (Ref. 4, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from reaching levels that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability of 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (Ref. 4, GDC 10), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stick fully withdrawn (Ref. 4, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the Reactor Coolant System ensure that these criteria are met as long as the core is operated within the ASI, F^T_{xy}, F^T_r, and T_q limits specified in the COLR (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses.

Fuel-cladding damage does not occur while at conditions outside these LCO during normal operation. Fuel-cladding damage could result, however, should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.

LHR, ASI, F^T_{xy}, F^T_r, and T_q satisfy Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and Departure from Nucleate Boiling Ratio (DNBR) operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on the LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F.

The limitation on ASI, along with the limitations of LCO 3.3.1, represents a conservative envelope of operating conditions consistent with the assumptions which have been analytically demonstrated adequate to maintain an acceptable minimum DNBR throughout all AOOs. Of these, the loss-of-flow transient is the most limiting. Operation of the core with conditions within the specified limits

(continued)

(continued)

BASES (continued)

LCO (continued)

provides assurance that an acceptable minimum margin from DNB conditions will be maintained in the event of any AOO, including a loss-of-flow transient.

[For this facility, an OPERABLE Excore Detector Monitoring System constitutes the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure Excore Detector Monitoring System OPERABILITY:]

[For this facility, those required support systems which, upon their failure, do not require declaring the Excore Detector Monitoring System inoperable and their justification are as follows:]

APPLICABILITY

In MODE 1, power distribution must be maintained within the limits assumed in the accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because there is not sufficient THERMAL POWER to require a limit on the core power distribution.

ACTIONS

A.1

Operating the core within the limits of the ASI specified in the COLR and within the limits of LCO 3.3.1, "Reactor Protection System Instrumentation," provides assurance that an acceptable margin for DNB will be maintained in the event of a loss-of-flow accident. If the core power exceeds the core power limit based on DNB, fuel design limits may not be maintained following a loss-of-flow accident and prompt action must be taken to restore the DNB parameters. The Required Actions, which are to restore the ASI, should be completed within 2 hours to limit the time the plant is operated outside the initial conditions assumed in the accident analyses. Additionally, this Completion Time is sufficiently short so that the xenon distribution in the core will not change significantly.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

[For this facility, ASI is restored to within its limits by the following actions:]

B.1

If the ASI cannot be restored to within its specified limits, or ASI cannot be determined because of Excore Detector Monitoring System inoperability, core power must be reduced. A change to MODE 2 ensures that the core is operating further from thermal limits and places the core in a conservative condition. Six hours is a reasonable amount of time to allow, based on operating experience, to reach MODE 2 in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.5.1

Verification that the ASI is within the specified limits ensures that the core is not approaching DNB conditions. A 12-hour Frequency is adequate to allow the operator to identify trends in conditions that would result in an approach to the ASI limits, because the mechanisms that affect the ASI, such as xenon redistribution or CEA drive mechanism malfunctions, cause the ASI to change slowly and should be discovered before the limits are exceeded.

[For this facility, ASI is verified using the following instrumentation:]

A Note is added to this SR to indicate that the provisions of SR 3.0.4 do not apply.

REFERENCES

1. [Unit Name] FSAR, Chapter [15], "Accident Analysis."

2. [Unit Name] FSAR, Chapter [6], "Emergency Core Cooling System."

3. [Unit Name] Core Operating Limits Report.

(continued)

(continued)

BASES (continued)

REFERENCES (continued)

4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

5. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR) (Digital)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA) or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full-length (or part-length) CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 4 and 5), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in axial power distribution control.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the LHR and the Departure from Nucleate Boiling (DNB).

Proximity to the DNB condition is expressed by the Departure from Nucleate Boiling Ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 6) and corrected for such factors as rod bows and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two core power distribution monitoring systems, the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs), which monitor the core power distribution and are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by [ ].

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculation to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup will experience a greater magnitude of rod bow. Conversely, fuel assemblies which receive lower than the average burnup will experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty which is applied to the batch's maximum integrated planar-radial power peak. This penalty is correlated with the amount of rod bow that is determined from a batch's maximum average assembly burnup. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The COLSS and CPC will indicate continuously to the operator how far the core is from the operating limits and provide an audible alarm should an operating limit be exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

The COLSS continually generates an assessment of the calculated margin for specified LHR and specified DNBR limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies which indicate CEA position. In this case, the CPCs assume a minimum core power of 20% RATED THERMAL POWER (RTP). This threshold is set at 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS will initiate a reactor trip prior to exceeding fuel design limits.

The limits on the AXIAL SHAPE INDEX (ASI), the Planar Radial Peaking Factor (F_{xy}), and the AZIMUTHAL POWER TILT (T_q) represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation (Condition 1) and AOOs (Condition 2) (Ref. 2).

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from reaching levels that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F, 10 CFR 50.46 (Ref. 1);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (Ref. 2), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn (GDC 26, Ref. [ ]).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 1 and 2). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 4) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 1). High peak cladding temperatures exceeding 2200°F will cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the RCS ensure that these criteria are met as long as the core is operated within the ASI limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses (Ref. [ ]).

Fuel-cladding damage does not occur from conditions outside the limits of these LCOs during normal operation. However, fuel-cladding damage could result should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs.

The LHR satisfies Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

The limitation on the LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F.

[For this facility, an OPERABLE COLSS and an OPERABLE CPC consists of the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure the COLSS and the CPCs are OPERABLE:]

[For this facility, those required support systems, which upon their failure do not result in the inoperability of the COLSS and CPCs, and their justifications are as follows:]

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 above 20% RTP. The reasons these LCOs are not applicable below 20% RTP are:

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

a. The incore neutron detectors which provide input to the COLSS which then calculates the operating limits are inaccurate due to the poor signal-to-noise ratio which they experience at relatively low core power levels; and

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the local power density (LPD) and DNBR trip signals. When the core power is below this level, the core is operating well below its thermal limits and the resultant CPC-calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1 and A.2

Operation at or below the COLSS calculated power limit based on the LHR in units of kW/ft assures that the LHR limit is not exceeded. If the COLSS calculated core power limit based on the LHR exceeds the operating limit, initiating corrective action within 15 minutes ensures that prompt action is taken to reduce LHR to below the specified limit. [For this facility, LHR is restored to within its limits by the following actions:] One hour is a reasonable time to accomplish this because [ ].

B.1 and B.2

If the COLSS is not available, the OPERABLE local power density channels are monitored to ensure that the LHR limit is not exceeded. Operation within this limit ensures that in the event of a LOCA, the peak temperature of the fuel cladding will not exceed 2200°F. If the LHR limit is exceeded, initiating corrective action within 15 minutes ensures that the allowance of 2 hours to complete this ACTION is a reasonable time, based on [ ], to restore LHR to within limits when the COLSS is not in use. If, during this time, conditions develop that would approach core safety limits, a reactor trip will be generated by the CPCs.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

C.1

If the LHR cannot be returned to within its limit or LHR cannot be determined because of COLSS and CPC inoperability, core power must be reduced. Reduction to less than 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on the trip setpoints generated by the CPCs which assume a minimum core power of 20% RTP. Six hours is a reasonable time to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.1.1

This surveillance to verify LHR is only applicable when the COLSS is in service (as indicated by Note 2). In this case, continuous monitoring of the LHR is provided by the COLSS which calculates core power and core power operating limits based on the LHR and continuously displays these limits to the operator. A COLSS margin alarm is annunciated in the event that the THERMAL POWER exceeds the core power operating limit based on the LHR.

The SR is also modified by a Note that states that SR 3.0.4 does not apply because surveillance cannot be accomplished prior to increasing THERMAL POWER above 20% RTP because the COLSS assumes a minimum THERMAL POWER of 20% RTP.

SR 3.2.1.2

With the COLSS out of service (Note 2), the operator must monitor the LHR with each OPERABLE local power density channel. For this facility a 2-hour Frequency is sufficient to allow the operator to identify trends that would result in an approach to the LHR limits, and is justified as follows: [ ].

The surveillance is also modified by a Note that states that SR 3.0.4 does not apply because the surveillance cannot be accomplished prior to increasing THERMAL POWER above 20% RTP because [ ].

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.2.1.3

Verification that the COLSS margin alarm actuates at a THERMAL POWER level equal to or less than the core power operating limit based on the LHR in units of kW/ft ensures that the operator will be alerted should operating conditions approach the LHR operating limit. [For this facility, the justification for performing this SR every 31 days is as follows:]

The surveillance is modified by a Note that states that SR 3.0.4 does not apply because surveillance cannot be accomplished prior to increasing THERMAL POWER above 20% RTP because COLSS assumes a minimum THERMAL POWER of 20% RTP.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
2. Title 10, Code of Federal Regulations, Part 50.46, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 10, "Reactor Design."
3. [Unit Name] Core Operating Limits Report [Title].
4. [Unit Name] FSAR, Section [15], "[Accident Analysis]."
5. [Unit Name] FSAR, Section [6], "[Emergency Core Cooling System]."
6. CE-1 Correlation for DNBR.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 Planar Radial Peaking Factors (F_{xy}) (Digital)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of full-length (or part-length) CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., a CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. Limiting safety system settings and this LCO are based on the accident analyses (Refs. 4 and 5), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in axial power distribution control. Power distribution is

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the Departure from Nucleate Boiling (DNB).

Proximity to the DNB condition is expressed by the Departure from Nucleate Boiling Ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 6) and corrected for such factors as rod bows and grid spacers and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two core power distribution monitoring systems, the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs) which monitor the core power distribution and are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by [ ].

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculation to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup will experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup will experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty which is applied to the batch's maximum integrated planar-radial power peak. This penalty is correlated with the amount of rod bow that is determined from a batch's maximum average assembly burnup. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The COLSS will indicate continuously to the operator how far the core is from the operating limits and provide an audible alarm should an operating limit be exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies which indicate CEA position. In this case, the CPCs assume a minimum core power of 20% RATED THERMAL POWER (RTP). This threshold is set at 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS will initiate a reactor trip prior to exceeding fuel design limits.

The limits on the AXIAL SHAPE INDEX (ASI), the Planar Radial Peaking Factor (F_{xy}), and the AZIMUTHAL POWER TILT (T_q) represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation (Condition 1) and AOOs (Condition 2) (Ref. 2). The Power Distribution and CEA Insertion and Alignment LCOs

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

preclude core power distributions from reaching levels that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (10 CFR 50.46) (Ref. 1);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (GDC 10) (Ref. 2), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn (GDC 26, Ref. [ ]).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 1 and 2). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 4) with due regard for the correlations between measured quantities, the power distribution, and the uncertainties in the determination of power distribution.

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F, (Ref. 1). High peak cladding temperatures exceeding 2200°F will cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the RCS ensure that these criteria are met as long as the core is operated within the ASI, F_{xy}, and T_q limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of reactor core. Operation within the

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

limits for these variables ensures that their actual values are within the range used in the accident analyses (Ref. [ ]).

Fuel-cladding damage does not occur from conditions outside the limits of these LCOs for the ASI, F_{xy}, and T_q during normal operation. However, fuel-cladding damage could result should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased LHRs.

The F_{xy} satisfies Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

Limiting the values of the calculated Planar Radial Peaking Factors, (F^c_{xy}) used in the COLSS and CPCs to values equal to or greater than the measured Planar Radial Peaking Factors (F^m_{xy}) provides assurance that the limits calculated by the COLSS and CPSs remain valid.

[For this facility, an OPERABLE COLSS and an OPERABLE CPC consist of the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure the COLSS and the CPCs are OPERABLE:]

[For this facility, those required support systems, which upon their failure do not result in the inoperability of the COLSS and CPCs, and their justifications are as follows:]

(continued)

BASES (continued)

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 > 20% RTP. The reasons these LCOs are not applicable < 20% RTP are:

a. The incore neutron detectors which provide input to the COLSS which then calculates the operating limits are inaccurate due to the poor signal-to-noise ratio that they experience at relatively low core power levels; and

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the local power density (LPD) and DNBR trip signals. When the core power is below this level, the core is operating well below its thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1.1 and A.1.2

If the F^m_{xy} exceeds the F^c_{xy} values used in the COLSS and CPCs, non-conservative operating limits and trip setpoints may be calculated. In this case, action must be taken to ensure that the COLSS operating limits and CPC trip setpoints remain valid with respect to the accident analysis. The operator can do this by performing the Required Actions (A.1.1 and A.1.2). Analyses in Ref. [ ] show that by taking these Required Actions, the safety requirements established in the accident analyses are met. [For this facility, the justification for the 6-hour Completion Time is as follows:] This is supported by Reference [ ].

A.2

As an alternative to Required Actions A.1.1 and A.1.2, the operator may adjust the affected values of F^c_{xy} used in the COLSS and the CPC to a value equal to or greater than F^m_{xy}. [For this facility, the justification for the 6-hour Completion Time is as follows:]

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

A.3

If Required Actions A.1.1 and A.1.2 or A.2 cannot be accomplished within 6 hours, the core power must be reduced. Reduction to 20% RTP or less ensures that the core is operating within the specified thermal limits and places the core in a conservative condition based on the trip setpoints generated by the CPCs and COLSS operating limits; these limits are established assuming a minimum core power of 20% RTP. Six hours is a reasonable time to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.2.1

This periodic surveillance is for determining, using the incore detector system, that F^m_{xy} is less than or equal to the F^c_{xy} used in the COLSS and CPCs. It provides assurance that the F^c_{xy} values used remain valid throughout the fuel cycle. A frequency of 31 effective full power days is acceptable since the power distribution should change only slightly with the amount of fuel burnup. Determining the F^m_{xy} after each fuel loading when the THERMAL POWER is > 40% RTP, but prior to exceeding 70% RTP, provides additional assurance that the core was properly loaded.

This SR is modified by a Note which states that SR 3.0.4 does not apply because this surveillance cannot be accomplished prior to increasing THERMAL POWER > 20% RTP because COLSS assumes a minimum THERMAL POWER of 20% RTP.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

2. Title 10, Code of Federal Regulations, Part 50.46, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 10, "Reactor Design."

3. [Unit Name] FSAR, Core Operating Limits Report, "[Title]."

(continued)

(continued)

BASES (continued)

REFERENCES (continued)

4. [Unit Name] FSAR, Section [15], "Accident Analysis."

5. [Unit Name] FSAR, Section [6], "Emergency Core Cooling System."

6. CE-1 Correlation for DNBR.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 AZIMUTHAL POWER TILT (T_q) (Digital)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of full-length (or part-length) CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions that cause margin degradations (e.g., a CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analyses (Refs. 4 and 5), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in axial power distribution control.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the Departure from Nucleate Boiling (DNB).

Proximity to the DNB condition is expressed by the Departure from Nucleate Boiling Ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 6) and corrected for such factors as rod bows and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two core power distribution monitoring systems, the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs), which monitor the core power distribution and are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by [ ].

A DNBR penalty factor is included in the COLSS and CPC DNBR calculation to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup will experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup will experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty that is applied to the batch's maximum integrated planar radial power peak. This penalty is correlated with the amount of rod bow that is determined from a batch's maximum average assembly burnup. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The COLSS will indicate continuously to the operator how far the core is from the operating limits and provide an audible alarm should an operating limit be exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continue to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux data, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies which indicate CEA position. In this case, the CPCs assume a minimum core power of 20% RATED THERMAL POWER (RTP). This threshold is set at 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS will initiate a reactor trip prior to exceeding fuel design limits.

The limits on the AXIAL SHAPE INDEX (ASI), the Planar Radial Peaking Factor (F_{xy}), and the (T_q) represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation (Condition 1) and AOOs (Condition 2) (Ref. 2). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from occurring that would violate the following fuel design criteria:

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (10 CFR 50.46) (Ref. 1);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (GDC 10) (Ref. 2), referred to hereafter as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [ ]); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn (GDC 26), (Ref. [ ]).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 1 and 2). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analysis (Ref. 4) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 1). High peak cladding temperatures exceeding 2200°F will cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the RCS ensure that these criteria are met as long as the core is operated within the ASI, F_{xy}, and T_q limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 3). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses (Ref [ ]).

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Fuel-cladding damage does not occur from conditions outside the limits of these LCOs (for the ASI, F_{xy}, and T_q) during normal operation. However, fuel-cladding damage could result should an accident occur from initial conditions outside the limits of these LCOs. The potential for fuel-cladding damage exists because changes in the power distribution cause increased power peaking and correspondingly increased local LHRs.

The T_q satisfies Criterion 2 of the NRC Interim Policy Statement.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

The limitations on the T_q are provided to ensure that design operating margins are maintained. A $T_q > 0.10$ is not expected. Should it occur, the ACTIONS to be taken ensure that operation is restricted to only those conditions required to identify the cause of the tilt. It is necessary to explicitly account for power asymmetries because the radial peaking factors used in the core power distribution calculations are based on an untilted power distribution.

[For this facility, an OPERABLE COLSS and an OPERABLE CPC consists of the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure the COLSS and the CPCs are OPERABLE:]

[For this facility, those required support systems, which upon their failure do not result in the inoperability of the COLSS and CPCs, and their justifications are as follows:]

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs however, are only applicable in MODE 1 > 20% RTP. The reasons these LCOs are not applicable < 20% RTP are:

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate due to the poor signal-to-noise ratio which they experience at relatively low core power levels.

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the local power density (LPD) and DNBR trip signals. When the core power is below this level, the core is operating well below its thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1

If the measured T_q is greater than the T_q allowance used in the CPCs but $\leq$ 0.10, non-conservative trip setpoints may be calculated. Required Action A.1 will restore the T_q to within its specified limits by repositioning the CEAs, and the reactor may return to normal operation. A Completion Time of 2 hours is sufficient time to allow the operator to reposition the CEAs because significant radial xenon redistribution will not occur within this time.

A.2

If the T_q cannot be restored within 2 hours, the T_q allowance in the CPCs must be adjusted per this Required Action, to be equal to or greater than the measured value of T_q to ensure that the design safety margins are maintained.

[For this facility, T_q is restored to within its limits by the following actions:]

B.1

If the measured T_q > 0.10, the measured T_q must be verified to be equal to or less than the T_q allowance used in the CPCs. The Completion Time of 2 hours provides sufficient time to perform SR 3.2.3.2 (verifying T_q is within its specified limit), and yet limits the probability of operation with a power distribution out of limits.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

In the case of a tilt generated by a CEA misalignment, this ACTION statement allows recovery of the CEA misalignment, since a measured $T_q > 0.10$ is not expected. If it should occur, continued operation of the reactor may be necessary to discover the cause of the tilt. If this occurs, operation is restricted to only those conditions required to identify the cause of the tilt. It is necessary to explicitly account for power asymmetries because the radial power peaking factors used in the core power distribution calculation are based on an untilted power distribution.

[For this facility, T_q is restored to within its limits by the following actions:]

B.2.2.1, B.2.2.2, and B.2.2.3

If the measured T_q is not restored to within its specified limits, the reactor will continue to operate with an axial power distribution mismatch. Continued operation in this configuration may induce an axial xenon oscillation, which will result in increased linear heat generation rates when the xenon redistributes. If the measured T_q cannot be restored to within its limit within 2 hours, reactor power must be reduced. Reducing THERMAL POWER to < 50% RTP within 4 hours provides an acceptable level of protection from increased power peaking due to potential xenon redistribution (Ref. [ ]). Required Action B.2.2.1 is modified by two Notes that require that all subsequent actions be performed once Required Action B.2.2.1 is entered. This ensures that corrective action is taken before unrestricted power operation resumes.

The linear power level—high trip setpoints are reduced to ≤ 55% RTP to ensure that the assumptions of the accident analysis regarding power peaking are maintained. For this facility, 16 hours is a reasonable time considering the required reduction in THERMAL POWER because [ ].

THERMAL POWER is restricted to 50% RTP until the measured T_q is restored to within its specified limit by correcting the out-of-limit condition. This action prevents the operator from increasing THERMAL POWER above the conservative limit when a significant T_q has existed, but allows the unit to continue operation for diagnostic purposes.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

The Completion Time of Required Action B.2.2.3 is modified by a Note governing subsequent power increases. After a THERMAL POWER increase following restoration of T_q, operation may proceed provided the measured T_q is determined to remain within its specified limit at the increased THERMAL POWER level.

The provision to allow discontinuation of the surveillance after verifying that $T_q \leq 0.10$ is within its specified limit at least once per hour for 12 hours or until T_q is verified to be within its specified limit at a THERMAL POWER $\geq$ 95% RTP provides an acceptable exit from this ACTION after the measured T_q has been returned to an acceptable value.

[For this facility, T_q is restored to within its limits by the following actions:]

C.1

If the measured T_q cannot be restored or determined within its specified limit, core power must be reduced. Reduction to $\geq$ 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on the trip setpoints generated by the CPCs, which assume a minimum core power of 20% RTP. Six hours is a reasonable time to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.3.1

Continuous monitoring of the measured T_q by the incore nuclear detectors is provided by the COLSS. A COLSS alarm is annunciated in the event that the measured T_q exceeds the value used in the CPCs.

This SR is modified by two Notes. The first states that SR 3.0.4 is not applicable, and the second states that this surveillance is only applicable when the COLSS is in service.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.2.3.2

With the COLSS out of service (Note 2), the operator must calculate the T_q and verify that it is within its specified limit. For this facility, a 12-hour Frequency allowing the operator to identify developing tilts is justified because [ ]. In addition, the 12-hour Frequency prevents significant xenon redistribution. However, some tilt-causing events are detectable in their own right. Therefore, [ ].

This SR is modified by a Note which states that SR 3.0.4 is not applicable (Note 1).

SR 3.2.3.3

Verification that the COLSS T_q alarm actuates at a value less than the value used in the CPCs ensures that the operator will be alerted should T_q approach its operating limit. [For this facility, a 31-day Frequency is justified as follows:].

This SR is modified by a Note which states that SR 3.0.4 is not applicable.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."

2. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 10, "Reactor Design."

3. [Unit Name] FSAR, Core Operating Limits Report, "[Title]."

4. [Unit Name] FSAR, Section [15], "[Accident Analysis]."

5. [Unit Name] FSAR, Section [6], "[Emergency Core Cooling System]."

6. CE-1 Correlation for DNBR.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 Departure from Nucleate Boiling Ratio (DNBR) (Digital)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial value assumed in the accident analyses. Specifically, operation within the limits imposed by this LCO limits potential fuel cladding failures that could breach the primary fission product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA) or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of full-length (or part-length) CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., a CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (e.g., CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings and this LCO are based on the accident analysis (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Limiting power distribution skewing over time also minimizes the xenon distribution skewing, which is a significant factor in axial power distribution control.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the Departure from Nucleate Boiling (DNB).

Proximity to the DNB condition is expressed by the DNBR, defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bows and grid spacers and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two core power distribution monitoring systems, the Core Operating Limits Supervisory System (COLSS) and the core protection calculators (CPCs), which monitor the core power distribution and are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by [ ].

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculation to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup will experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than the average burnup will experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty that is applied to the batch's maximum integrated planar radial power peak. This penalty is correlated with the amount of rod bow that is determined from a batch's maximum average assembly burnup. A single net penalty for the COLSS and CPCs is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The COLSS will indicate continuously to the operator how far the core is from the operating limits and provide an audible alarm should an operating limit be exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies which indicate CEA position. In this case, the CPCs assume a minimum core power of 20% RATED THERMAL POWER (RTP). This threshold is set at 20% RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS will initiate a reactor trip prior to exceeding fuel design limits.

The limits on the AXIAL SHAPE INDEX (ASI), the Planar Radial Peaking Factor (F_{xy}), and the AZIMUTHAL POWER TILT (T_q) represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 4). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions from reaching levels that would violate the following fuel design criteria:

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (10 CFR 50.46) (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (GDC 10) (Ref. 4), hereafter referred to as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 6); and

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn. (GDC 26) (Ref. 7).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures exceeding 2200°F may cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI, and the RCS ensure that these criteria are met as long as the core is operated within the ASI, F_{xy}, and T_q limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 8). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual values are within the range used in the accident analyses (Ref. 1).

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

Fuel-cladding damage does not occur from conditions outside the limits of these LCOs during normal operation. However, fuel-cladding damage could result should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs. The minimum DNBR ratio satisfies Criterion 2 of the NRC Interim Policy Statement in that it is an initial condition assumed in the safety analyses.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

With the COLSS in service and one or both of the Control Element Assembly Calculators (CEACs) OPERABLE, the DNBR will be maintained by ensuring that the core power calculated by the COLSS is equal to or less than the permissible core power operating limit calculated by the COLSS. In the event that the COLSS is in service but neither of the two CEACs is OPERABLE, the DNBR will be maintained by ensuring that the core power calculated by the COLSS is equal to or less than a reduced value of the permissible core power operating limit calculated by the COLSS. In this condition, the calculated operating limit shall be reduced by 13.0% RTP.

For those instances when the COLSS is out of service and either one or both of the CEACs are OPERABLE, the DNBR will be maintained by operating within the acceptable region specified in the COLR as shown in Figure 3.2.4-1 and using any OPERABLE CPC channel. Alternatively, when the COLSS is out of service and neither of the two CEACs is OPERABLE, the DNBR will be maintained by operating within the acceptable region specified in the COLR for this condition as shown in Figure 3.2.4-2 and using any OPERABLE CPC channel.

With the COLSS out of service, the limitation on DNBR as a function of the ASI represents a conservative envelope of operating conditions consistent with the analysis

(continued)

(continued)

BASES (continued)

LCO (continued)

assumptions which have been analytically demonstrated adequate to maintain an acceptable minimum DNBR for all AOOs. Of these, the postulated loss-of-flow transient is the most limiting. Operation of the core with a DNBR at, or above, this limit provides assurance that an acceptable minimum DNBR will be maintained in the event of a loss-of-flow transient.

[For this facility, an OPERABLE COLSS, an OPERABLE CEAC and an OPERABLE CPC consists of the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure the COLSS, CEAC and the CPCs are OPERABLE:]

[For this facility, those required systems, which upon their failure do not result in the inoperability of the COLSS, CEAC and CPCs, and their justifications are as follows:]

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs, however, are only applicable in MODE 1 > 20% RTP. The reasons these LCOs are not applicable < 20% RTP are:

a. The incore neutron detectors which provide input to the COLSS which then calculates the operating limits are inaccurate due to the poor signal-to-noise ratio which they experience at relatively low core power levels; and

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the local power density (LPD) and DNBR trip signals. When the core power is below this level, the core is operating well below the thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

(continued)

BASES (continued)

ACTIONS

A.1

Operating the core at or above the minimum required value of the DNBR provides assurance that an acceptable minimum DNBR will be maintained in the event of a postulated loss-of-flow transient. If the core power as calculated by the COLSS exceeds the core power limit calculated by the COLSS based on the DNBR, fuel design limits may not be maintained following a loss of flow and prompt action must be taken to restore the DNBR above its minimum Allowable Value. With the COLSS in service, 15 minutes is a reasonable time to allow the operator to initiate corrective actions to restore the DNBR above its specified limit, because of the low probability of a severe transient occurring in this relatively short time.

A.2

With the COLSS in service, the actions to restore DNBR should be completed within 1 hour per this Required Action to limit the time that the plant is operated outside the initial conditions assumed in the analyses.

B.1 and B.2

With the COLSS out of service, the operator is again required to take prompt action (i.e., within 15 minutes) to restore the DNBR above its minimum Allowable Value. However, in this instance, 2 hours are allowed to restore the DNBR above its minimum Allowable Value because of additional conservatisms in the CPCs (Ref. [ ]). [For this facility, the Completion Time of 2 hours to restore DNBR above its minimum value, determined with the CPCs, is justified as follows:]

C.1

If the DNBR cannot restored or determined within the allowed times of Conditions A and B, core power must be reduced. Reduction to < 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on the trip setpoints generated by the CPCs which assume a minimum core power of 20% RTP.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Six hours is a reasonable Completion Time to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.4.1

Continuous monitoring of the DNBR is provided by the COLSS, which calculates core power and core power operating limits based on the DNBR and continuously displays these limits to the operator. A COLSS margin alarm is annunciated in the event that the THERMAL POWER exceeds the core power operating limit based on the DNBR.

This SR is modified by a Note that states that SR 3.0.4 does not apply because surveillance cannot be accomplished prior to increasing THERMAL POWER > 20% RTP because the COLSS assumes a minimum THERMAL POWER of 20% RTP. In addition, the surveillance is only applicable when COLSS is in service and is so indicated by Note 2.

SR 3.2.4.2

With the COLSS out of service (Note 2), the operator must monitor the DNBR as indicated on any of the OPERABLE DNBR channels of the CPCs to verify that the DNBR is within the specified limits, shown in either Figure 3.2.4-1 or 3.2.4-2, as applicable. A 2-hour Frequency is adequate to allow the operator to identify trends in conditions that would result in an approach to the DNBR limit because [ ].

This SR is also modified by a Note that states that SR 3.0.4 does not apply because surveillance cannot be accomplished prior to increasing THERMAL POWER > 20% RTP because [ ].

SR 3.2.4.3

Verification that the COLSS margin alarm actuates at a power level equal to or less than the core power operating limit, as calculated by the COLSS, based on the DNBR, ensures that the operator will be alerted should operating conditions approach the DNBR operating limit. A 31-day Frequency is adequate because [ ].

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

This SR is also modified by a Note that states that SR 3.0.4 does not apply because surveillance cannot be accomplished prior to increasing THERMAL POWER > 20% RTP because the COLSS assumes a minimum THERMAL POWER of 20% RTP.

REFERENCES

1. [Unit Name] FSAR, Section [15], "[Accident Analysis]."
2. [Unit Name] FSAR, Section [6], "[Emergency Core Cooling System]."
3. C-E 1 Correlation for DNBR.
4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 10, "Reactor Design."
5. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
6. [Unit Name] FSAR, Section [ ], "[Title]."
7. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 26, "Reactivity Control System Redundancy and Capability."
8. [Unit Name] FSAR, Core Operating Limits Report, "[Title]."

B 3.2 CONTAINMENT SYSTEMS

B 3.2.5 AXIAL SHAPE INDEX (ASI) (Digital)

BASES

BACKGROUND

The purpose of this MODE 1 LCO is to limit the core power distribution to the initial values assumed in the accident analysis. Specifically, operation within the limits imposed by this LCO limits potential fuel-cladding failures that could breach the primary fission-product barrier and release fission products to the reactor coolant in the event of a loss-of-coolant accident (LOCA), loss-of-flow, ejected control element assembly (CEA), or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the amount of damage to the fuel cladding during an accident by assuring the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. The use of full-length (or part-length) CEAs to alter the axial power distribution;

b. Decreasing CEA insertion by boration, thereby improving the radial power distribution; and

c. Correcting off-optimum conditions which cause margin degradations (e.g., a CEA drop or misoperation of the unit).

The core power distribution is controlled so that, in conjunction with other core operating parameters (CEA insertion and alignment limits), the power distribution does not result in violation of this LCO. The limiting safety system settings are based on the accident analyses (Refs. 1 and 2), so that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences (AOOs) and the limits of acceptable consequences are not exceeded for other postulated accidents.

Minimizing power distribution skewing over time also minimizes the xenon distribution skewing which is a significant factor in axial power distribution control.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Power distribution is a product of multiple parameters, various combinations of which may produce acceptable power distributions. Operation within the design limits of power distribution is accomplished by generating operating limits on the linear heat rate (LHR) and the Departure from Nucleate Boiling (DNB).

Proximity to the DNB condition is expressed by the Departure from Nucleate Boiling Ratio (DNBR), defined as the ratio of the cladding surface heat flux required to cause DNB to the actual cladding surface heat flux. The minimum DNBR value during both normal operation and AOOs is [ ] as calculated by the CE-1 Correlation (Ref. 3), and corrected for such factors as rod bows and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two core power distribution monitoring systems, the Core Operating Limit Supervisory System (COLSS) or the core protection calculators (CPCs), which monitor the core power distribution and are capable of verifying that the LHR and the DNBR do not exceed their limits. The COLSS performs this function by continuously monitoring the core power distribution and calculating core power operating limits corresponding to the allowable peak LHR and DNBR. The CPCs perform this function by [ ].

A DNBR penalty factor is included in both the COLSS and CPC DNBR calculations to accommodate the effects of rod bow. The amount of rod bow in each assembly is dependent upon the average burnup experienced by that assembly. Fuel assemblies that incur higher than average burnup will experience a greater magnitude of rod bow. Conversely, fuel assemblies which receive lower than average burnup will experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty which is applied to the batch's maximum integrated planar radial power peak. This penalty is correlated with the amount of rod bow that is determined from a batch's maximum average assembly burnup. A single net penalty for the COLSS and CPC is then determined from the penalties associated with each batch that comprises a core reload, accounting for the offsetting margins due to the lower radial power peaks in the higher burnup batches.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The COLSS will indicate continuously to the operator how far the core is from the operating limits and provide an audible alarm should an operating limit be exceeded. Such a condition signifies a reduction in the capability of the plant to withstand an anticipated transient, but does not necessarily imply an immediate violation of fuel design limits. If the margin to fuel design limits continues to decrease, the RPS ensures that the specified acceptable fuel design limits are not exceeded for AOOs by initiating a reactor trip.

The COLSS continually generates an assessment of the calculated margin for LHR and DNBR specified limits. The data required for these assessments include measured incore neutron flux, CEA positions, and Reactor Coolant System (RCS) inlet temperature, pressure, and flow.

In addition to the monitoring performed by the COLSS, the RPS (via the CPCs) continually infers the core power distribution and thermal margins by processing reactor coolant data, signals from excore neutron flux detectors, and input from redundant reed switch assemblies which indicate CEA position. In this case, the CPCs assume a minimum core power of 20% RATED THERMAL POWER (RTP). This threshold is set at 20% of RTP because the power range excore neutron flux detecting system is inaccurate below this power level. If power distribution or other parameters are perturbed as a result of an AOO, the high local power density or low DNBR trips in the RPS will initiate a reactor trip prior to exceeding fuel design limits.

The limits on the ASI, the Planar Radial Peaking Factors (F_{xy}) and the AZIMUTHAL POWER TILT (T_q) represent limits within which the LHR and DNBR algorithms are valid. These limits are obtained directly from the initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of operation (Condition 1) or AOOs (Condition 2) (Ref. 4). The Power Distribution and CEA Insertion and Alignment LCOs

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

preclude core power distributions from reaching levels that would violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed a limit of 2200°F (10 CFR 50.46) (Ref. 5);

b. During a loss-of-flow accident, there must be at least a 95% probability at a 95% confidence level that the hot fuel rod in the core does not experience a DNB condition (GDC 10) (Ref. 4), hereafter referred to as the 95/95 DNB criterion;

c. During an ejected rod accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 6);

d. The control rods must be capable of shutting down the reactor with a minimum required SHUTDOWN MARGIN with the highest worth control rod stuck fully withdrawn. (GDC 26) (Ref. 7).

The power density at any point in the core must be limited to maintain the fuel design criteria (Refs. 4 and 5). This is accomplished by maintaining the power distribution and reactor coolant conditions so that the peak LHR and DNB parameters are within operating limits supported by the accident analyses (Ref. 1) with due regard for the correlations between measured quantities, the power distribution, and uncertainties in the determination of power distribution.

Fuel-cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate so that the peak cladding temperature does not exceed 2200°F (Ref. 5). High peak cladding temperatures exceeding 2200°F may cause severe cladding failure by oxidation due to a Zircaloy-water reaction.

The LCOs governing the LHR, the ASI and the RCS ensure that these criteria are met as long as the core is operated within the ASI, F_{xy}, and T_q limits specified in the CORE OPERATING LIMITS REPORT (COLR) (Ref. 8). The latter are process variables that characterize the three-dimensional power distribution of the reactor core. Operation within the limits for these variables ensures that their actual

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

values are within the range used in the accident analysis (Ref. 1).

Fuel-cladding damage does not occur from conditions outside these LCOs during normal operation. However, fuel-cladding damage could result should an accident occur from initial conditions outside the limits of these LCOs. This potential for fuel-cladding damage exists because changes in the power distribution can cause increased power peaking and correspondingly increased local LHRs. The limits on the ASI satisfy Criterion 2 of the NRC Interim Policy Statement in that they are initial conditions assumed in the safety analysis.

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNBR operating limits. The power distribution LCO limits are provided in the COLR.

The limitation on ASI ensures that the actual ASI value is maintained within the range of values used in the accident analysis. The ASI limits ensure that with T_q at its maximum upper limit, the DNBR will not drop below the DNBR Safety Limit for AOOs.

[For this facility, an OPERABLE COLSS and an OPERABLE CPC consists of the following:]

[For this facility, the following support systems are required to be OPERABLE to ensure the COLSS and the CPCs are OPERABLE:]

[For this facility, those required support systems, which upon their failure do not result in the inoperability of the COLSS and CPCs, and their justifications are as follows:]

APPLICABILITY

Power distribution is a concern any time the reactor is critical. The power distribution LCOs however, are only applicable in MODE 1 > 20% RTP. The reasons these LCOs are not applicable < 20% RTP are:

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

a. The incore neutron detectors which provide input to the COLSS which then calculates the operating limits are inaccurate due to the poor signal-to-noise ratio which they experience at relatively low core power levels; and

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the local power density (LPD) and DNBR trip signals. When the core power is below this level, the core is operating well below the thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1

The ASI limits specified in the COLR ensure that the LOCA and loss-of-flow accident criteria assumed in the accident analyses remain valid. If the ASI exceeds its limit, a Completion Time of 2 hours is allowed to restore the ASI to within its specified limit. This gives the operator sufficient time to reposition the regulating or part-length CEAs to reduce the axial power imbalance. The magnitude of any potential xenon oscillation is significantly reduced if the condition is not allowed to persist for more than 2 hours because [ ].

[For this facility, ASI is restored to within its limits by the following actions:]

B.1

If the ASI is not restored to or determined to be within its specified limits within the required Completion Time, the reactor will continue to operate with an axial power distribution mismatch. Continued operation in this configuration would induce an axial xenon oscillation, and would result in increased linear heat generation rates when the xenon redistributes. Reducing thermal power to ≤ 20% RTP reduces the maximum LHR to a value which will not exceed the fuel design limits should a design basis event occur. The 4-hour Completion Time allows for an orderly reduction in power without challenging plant systems.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

SR 3.2.5.1

The ASI can be monitored by both the incore (COLSS) and excore (CPC) neutron detector systems. The COLSS provides the operator with an alarm should an ASI limit be approached.

Verification of the ASI every 12 hours ensures that the operator is aware of changes in the ASI as they develop. A 12-hour Frequency for this surveillance is acceptable because the mechanisms which affect the ASI, such as xenon redistribution or CEA drive mechanism malfunctions, cause slow changes in the ASI and will be discovered before the limits are exceeded. [For this facility, ASI is verified using the following instrumentation:]

REFERENCES

1. [Unit Name] FSAR, Section [15], "[Accident Analysis]."
2. [Unit Name] FSAR, Section [6], "[Emergency Core Cooling System]."
3. CE-1 Correlation for DNBR.
4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 10, "Reactor Design."
5. Title 10, Code of Federal Regulations, Part 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light Water Nuclear Power Reactors."
6. [Unit Name] FSAR, Section [ ], "[Title]."
7. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 26, "Reactivity Control System Redundancy and Capability."
8. [Unit Name] FSAR, Core Operating Limits Report "[Title]."

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protection System (RPS) Instrumentation (Analog)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core fuel design limits and reactor coolant pressure boundary integrity during anticipated operational occurrences (AOOs), and to assist the engineered safety features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to assure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS, defined in this specification as the ALLOWABLE VALUE, in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits during Design Basis Accidents (DBAs).

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limit is:

1. The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling;

2. Fuel centerline melting shall not occur; and

3. The Reactor Coolant System pressure SL of [2750] psia shall not be exceeded.

Maintaining the SLs within the above values assures that offsite dose will be within the 10 CFR 50 and 10 CFR 100 criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits. Different accident categories are allowed a different fraction of these limits based on probability of

(continued)

(continued)

BACKGROUND (continued)

occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels;
- Bistables;
- RPS Logic; and
- Reactor Trip Circuit Breakers (RTCBs).

The role of each of these modules in the RPS is discussed below.

<u>Measurement Channels</u>

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

The excore nuclear instrumentation and the analog core protection calculators (CPCs) are considered components in the measurement channels. The wide-range nuclear instruments (NIs) provide a Power Rate of Change--High Trip. Three RPS trips use a power level designated as Q power as an input. Q power is the higher of NI power and primary calorimetric power (ΔT power) based on RCS hot-leg and cold-leg temperatures. Trips using Q power as an input include the Variable High Power Trip (VHPT)--High, Thermal Margin/Low Pressure (TM/LP), and the Axial Power Distribution (APD)--High trips.

The analog CPCs provide the complex signal processing necessary to calculate the TM/LP trip setpoint, APD trip setpoint, VHPT trip setpoint, and Q power calculation.

The excore NIs (wide range and power range) and the analog CPCs (TM/LP and APD calculators) are mounted in the RPS cabinet, with one channel of each in each of the four RPS bays.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the direct generation of trip signals. These are designated channels A through D. Measurement channels provide input to one or more RPS bistables within the same RPS channel. In addition, some measurement channels may also be used as inputs to Engineered Safety Feature Actuation System (ESFAS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS are never used for control functions.

When a channel monitoring a parameter exceeds a predetermined setpoint indicating an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter de-energizes matrix logic, which in turn de-energizes the initiation logic. This causes all eight RTCBs to open, interrupting power to the control element assemblies (CEAs), allowing them to fall into the core.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in 10 CFR 50, Appendix A (Ref. 1). The fourth channel provides additional flexibility, by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing, while still maintaining a minimum two-out-of-three logic. Thus, even with a channel inoperable, no single additional failure in the RPS can either cause an inadvertent trip, nor prevent a required trip from occurring.

In order to take full advantage of the four-channel design, adequate channel-to-channel independence must be demonstrated, approved by the NRC staff, and this approval documented by an NRC Safety Evaluation Report (SER). Adequate channel-to-channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants that have demonstrated adequate channel-to-channel independence, as documented by the NRC SER (Ref. 2) may operate in a two-out-of-three logic configuration, with one channel removed from service, for the time stated in Reference 2.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of Institute of Electrical and Electronic Engineers (IEEE) 279-1971 (Ref. 3).

Many of the RPS trips are generated by comparing a single measurement to a fixed bistable setpoint. Certain functions, however, make use of more than one measurement to provide a trip. The following trips use multiple measurement channel inputs:

- <u>Steam Generator (SG) Water Level--Low</u>

  This trip uses the lower of the two SG levels as an input to a common bistable.

- <u>Steam Generator Pressure--Low</u>

  This trip uses the lower of the two SG pressures as an input to a common bistable.

- <u>Variable High Power Trip--High</u>

  The VHPT uses Q power as its only input. Q power is the higher of NI power and ΔT power. It has a trip setpoint which tracks power levels downwards so that it is always within a fixed increment above current power, subject to a minimum value. On power increases, the trip setpoint remains fixed unless manually reset, at which point it increases to the new setpoint, a fixed increment above Q power at the time of reset, subject to a maximum value. Thus, during power escalation, the trip setpoint must be repeatedly reset to avoid a reactor trip.

- <u>Thermal Margin/Low Pressure and Asymmetric Steam Generator Transient Protective Trip Function (ASGTPTF)</u>

  Q power is only one of several inputs to the TM/LP trip. Other inputs include internal AXIAL SHAPE INDEX (ASI) and cold-leg temperature based on the higher of two cold-leg resistance temperature detectors (RTDs). The TM/LP trip setpoint is a complex function of these

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

inputs and represents a minimum acceptable RCS pressure to be compared to actual RCS pressure in the TM/LP trip unit.

SG pressure is also an indirect input to the TM/LP trip via the ASGTPTF. This function provides a reactor trip when the secondary pressure in either SG exceeds that of the other generator by greater than a fixed amount. The trip is implemented by biasing the TM/LP trip setpoint upward so as to assure TM/LP trip if an asymmetric SG transient is detected.

<u>Axial Power Distribution--High</u>

Q power and ASI are inputs to the APD trip. The APD trip setpoint is a function of Q power, being more restrictive at higher power levels. It provides a reactor trip if actual ASI exceeds the APD trip setpoint.

<u>Bistables</u>

Bistable trip units, mounted in the RPS cabinet, receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the matrix logic. They also provide local trip indication, and remote annunciation.

There are four channels of bistable trip units, designated A through D, for each RPS function, one for each measurement channel. Bistable output relays de-energize when a trip occurs.

The contacts from these bistable relays are arranged into six coincidence matrices, comprising the matrix logic. If bistables monitoring the same parameter in at least two channels trip, the matrix logic will generate a reactor trip (two-out-of-four logic).

Some of the RPS measurement channels provide contact outputs to the RPS, so the comparison of an analog input to a trip setpoint is not necessary. In these cases, the bistable trip unit is replaced with an auxiliary trip unit. The auxiliary trip units provide contact multiplication so the

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

single input contact opening can provide multiple contact outputs to the coincidence logic, as well as trip indication and annunciation.

Trips employing auxiliary trip units include the loss-of-load trip and the APD--High trip. The loss-of-load trip is a contact input from the Electro-Hydraulic Control System control oil pressure on each of the four high pressure stop valves.

The APD trip, described above, is a complex function, in which the actual trip comparison is performed within the CPC. Therefore the APD--High trip unit employs a contact input from the CPC.

All RPS trips with the exception of the loss-of-load trip generate a pretrip alarm as the trip setpoint is approached.

The trip setpoints used in the bistables are based on the analytical limits stated in Reference 4. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors—for those RPS channels that must function in harsh environments, as defined by 10 CFR 50.49 (Ref. 5)—ALLOWABLE VALUES specified in Table 3.3.1 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 6). The nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the ALLOWABLE VALUE, to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the Surveillance interval. If the measured setpoint does not exceed the ALLOWABLE VALUE, the bistable is considered OPERABLE.

Setpoints in accordance with the ALLOWABLE VALUE will assure that SLs of Specification 2.0 are not violated during AOOs, and the consequences of DBAs will be acceptable, providing

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

the plant is operated from within the LCOs at the onset of the AOO or DBA, and the equipment functions as designed.

Note that in LCO 3.3.1, the ALLOWABLE VALUES of Table 3.3.1-1 are the LSSS. These ALLOWABLE VALUES are established to prevent violation of the SLs during normal plant operation and AOOs.

The ALLOWABLE VALUES listed in Table 3.3.1-1 are based upon the methodology described in Reference 6, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

Each channel of the process control equipment can be tested on line to verify that the signal or setpoint accuracy is within the specified allowance requirements. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated.

Reactor Protection System Logic

The RPS logic, consisting of matrix and initiation logic, employs a scheme that provides a reactor trip when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic. This logic and the RTCB configuration are shown in Figure B 3.3.1-1.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same function in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

(continued)

(continued)

This figure for illustration only. Do not use for operation.

Figure B 3.3.1-1
Functional Diagram of the Two-Out-of-Four Logic and RTCB Configuration

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The matrix relay contacts are arranged into trip paths, with one of the four matrix relays in each matrix opening contacts in one of the four trip paths. Each trip path provides power to one of the four normally energized RTCB control relays (K1, K2, K3, and K4). The trip paths thus each have six contacts in series, one from each matrix, and perform a logical OR function, opening the RTCBs if any one or more of the six logic matrices indicate a coincidence condition.

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized, interrupt power to the breaker undervoltage trip attachments and simultaneously apply power to the shunt trip attachments on each of the two breakers. Actuation of either the undervoltage or shunt trip attachment is sufficient to open the RTCB and interrupt power from the motor-generator (MG) sets to the control element drive mechanisms (CEDMs).

When a coincidence occurs in two RPS channels, all four matrix relays in the affected matrix de-energize. This in turn de-energizes all four breaker control relays, which simultaneously de-energize the undervoltage and energize the shunt trip attachments in all eight RTCBs, tripping them open.

Matrix logic refers to the matrix power supplies, bistable auxiliary relay contacts, and interconnecting wiring up to, but not including, the matrix relays.

The initiation logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and solid state (auxiliary) relays through the K-relay contacts in the RTCB control circuitry.

It is possible to change the two-out-of-four RPS logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the matrix logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but a reactor trip will not occur unless two additional channels indicate a trip condition. Trip channel

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

bypassing can be simultaneously performed to any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

For those plants that have demonstrated sufficient channel-to-channel independence, two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures a reactor trip would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent trips caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select RPS trips. Some of these bypasses are enabled manually, others automatically in all four RPS channels, when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Trips with operating bypasses include Power Rate of Change--High, Reactor Coolant Flow--Low, SG Pressure--Low, APD--High, TM/LP, and ASGTF. The loss- of-load trip operating bypass is automatically enabled and disabled.

<u>Reactor Trip Circuit Breakers</u>

The reactor trip switchgear, shown in Figure B 3.3.1-2, consists of eight RTCBs, which are operated in four sets of two breakers (four channels). Power input to the reactor trip switchgear comes from two full-capacity MG sets operated in parallel such that the loss of either MG set does not de-energize the CEDMs. There are two separate CEDM power supply buses, each bus powering half of the CEDMs. Power is supplied from the MG sets to each bus via two redundant paths (trip legs). Trip legs 1A and 1B supply power to CEDM bus 1. Trip legs 2A and 2B supply power to CEDM bus 2. This ensures that a fault or the opening of a breaker in one trip leg (i.e., for testing purposes) will not interrupt power to the CEDM buses.

(continued)

(continued)

BASES (continued)

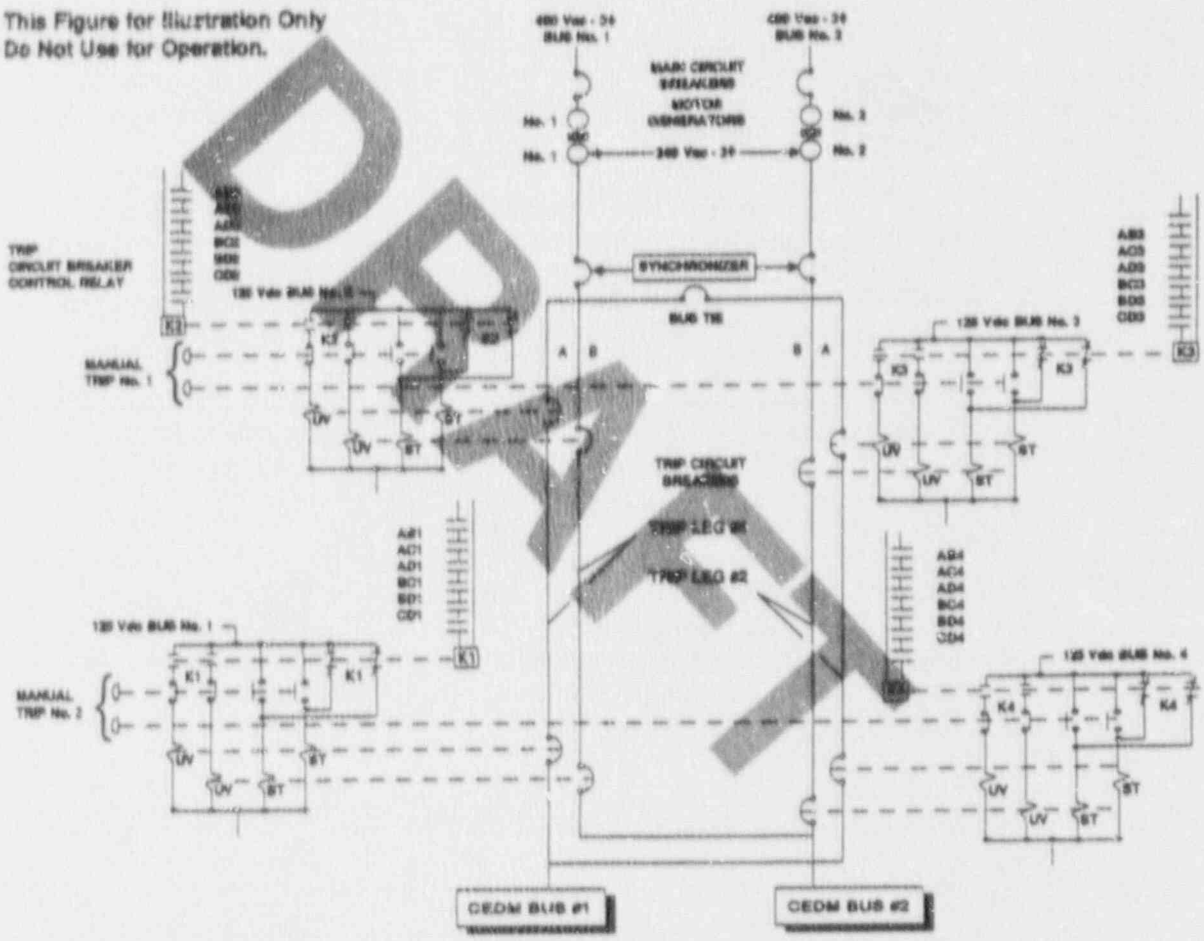

Figure B 3.3.1-2
Simplified Functional Diagram of the RPS Trip Switchgear

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Each of the four trip legs consists of two RTCBs in series. The two RTCBs within a trip leg are actuated by separate initiation circuits.

The eight RTCBs are operated as four sets of two breakers (four channels). For example, if a breaker receives an open signal in trip leg A (for CEDM bus 1), an identical breaker in trip leg B (for CEDM bus 2) will also receive an open signal. This arrangement ensures that power is interrupted to both CEDM buses, thus preventing trip of only one half of the CEAs (a half-trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

Each set of RTCBs is operated by either a manual reactor trip push button or an RPS-actuated K-relay. There are four Manual Reactor Trip push buttons, arranged in two sets of two, as shown in Figure B 3.3.1-2. Depressing both push buttons in either set will result in a reactor trip.

When a Manual Reactor Trip is initiated using the control room push buttons, the RPS trip paths and K-relays are bypassed, and the RTCB undervoltage and shunt trip attachments are actuated independent of the RPS.

Manual Reactor Trip circuitry includes the push button and interconnecting wiring to both RTCBs necessary to actuate both the undervoltage and shunt trip attachments, but excludes the K-relay contacts and their interconnecting wiring to the RTCBs, which are considered part of the Initiation Logic.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown, and is normally performed on a quarterly basis. Nuclear instrumentation and the CPCs can be similarly tested. Process transmitter calibration is normally performed on a refueling basis.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents and transients can be detected by one or more RPS functions. The accident analysis contained in Reference 4 takes credit for most RPS trip functions. Functions not specifically credited in the accident analysis were qualitatively credited in the safety

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

analysis and the NRC staff-approved licensing basis for the plant. These functions may provide protection for conditions which do not require dynamic transient analysis to demonstrate function performance. These functions may also serve as backups to functions that were credited in the safety analysis.

The specific safety analyses applicable to each protective function are identified below:

1. <u>Variable High Power Trip--High</u>

   The VHPT provides reactor core protection against positive reactivity excursions that are too rapid for a Pressurizer Pressure--High, or TM/LP trip to protect against. The following events require VHPT protection:

   a. uncontrolled CEA withdrawal event,
   b. excess load,
   c. excess feedwater heat-removal event,
   d. CEA ejection event, and
   e. main steam line break (MLSB)(outside containment).

   The first three events are AOOs, and fuel integrity is maintained. The fourth and fifth are accidents and limited fuel damage may occur.

   The VHPT--High ensures that low DNBR, high linear power density and the RCS pressure SLs are maintained during normal operation and AOOs and, in conjunction with the ESFAS, the consequences of the MSLB and CEA ejection accidents will be acceptable.

2. <u>Power Rate of Change--High</u>

   The Power Rate of Change--High trip is used to trip the reactor when excore wide range power indicates an excessive rate of change. The Power Rate of Change--High provides a backup to the VHPT to ensure that low DNBR, high linear power density, and the RCS pressure SLs are maintained. The Power Rate of Change--High function minimizes transients for events such as a continuous CEA withdrawal or a boron

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

dilution event from low power levels. The trip may be bypassed when THERMAL POWER is < 1E-4% RTP, when poor counting statistics may lead to erroneous indication. It is also bypassed > 15% RTP where moderator temperature coefficient and fuel temperature coefficient make high rate of change of power unlikely. With the RTCBs open, the Power Rate of Change--High trip is not required to be OPERABLE; however, the indication and alarm functions of at least two channels are required by LCO 3.3.7 to be OPERABLE. LCO 3.3.7 assures the wide-range channels are available to detect and alert the operator to a boron dilution event.

3. Reactor Coolant Flow--Low

The Reactor Coolant Flow--Low trip provides protection during the following events:

a. loss of RCS flow,
b. loss of non-emergency AC power,
c. reactor coolant pump (RCP) seized shaft,
d. RCP sheared shaft, and
e. certain MSLB events.

The loss of RCS flow and the loss of non-emergency AC power events are AOOs, and fuel integrity is maintained. The RCP seized shaft, sheared shaft, and MSLBs are accidents that may result in fuel damage. The Reactor Coolant Flow--Low trip is provided to trip the reactor, thus assisting the ESFAS in the event of a sheared RCP shaft accident. Since this is an accident, SLs may be violated. However, the consequences of the accident will be acceptable.

4. Pressurizer Pressure--High

The Pressurizer Pressure--High trip, in conjunction with pressurizer safety valves and main steam safety valves (MSSVs), provides protection against over pressure conditions in the RCS during the following events:

a. loss of condenser vacuum with a concurrent loss of offsite power,
b. loss of condenser vacuum with a concurrent loss of one 6.9 kV bus,

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

c. isolation of turbine at 102% power,
d. Feedwater System pipe breaks between the steam generator and check valve,
e. CEA withdrawal, and
f. loss of feedwater flow.

The Pressurizer Pressure--High trip assures that the RCS pressure SL will not be exceeded during AOOs, and in conjunction with the ESFAS, that the consequences of accidents will be acceptable.

5. Containment Pressure--High

The Containment Pressure--High trip prevents exceeding the containment design pressure during certain loss-of-coolant accidents (LOCAs) or feedwater line break accidents. It assures a reactor trip prior to, or concurrent with, a LOCA, thus assisting the ESFAS in the event of a LOCA or MSLB. Since these are accidents, SLs may be violated. However, the consequences of the accident will be acceptable.

6. Steam Generator Pressure--Low

The SG Pressure--Low trip provides protection against an excessive rate of heat extraction from the SGs, which would result in a rapid uncontrolled cooldown of the RCS. This trip is needed to shut down the reactor and assist the ESFAS in the event of an MSLB. Since these are accidents, SLs may be violated. However, the consequences of the accident will be acceptable.

7. Steam Generator Water Level--Low

The SG Water Level--Low trip is required for the following events to help prevent exceeding the RCS design pressure due to a loss of heat sink:

a. Steam System piping failures,
b. Feedwater System pipe breaks,
c. inadvertent opening of an SG atmospheric dump valve (ADV),

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

d. loss of normal feedwater, and
e. asymmetric loss of feedwater.

The SG Water Level--Low ensures that low DNBR, high linear power density,and the RCS pressure SLs are maintained during normal operation and AOOs and, in conjunction with the ESFAS, the consequences of the Feedwater System pipe break accident will be acceptable.

8. <u>Axial Power Distribution--High</u>

The APD--High trip ensures that excessive axial peaking, such as that due to axial xenon oscillations, will not cause fuel damage. It ensures that neither a DNBR less than the SL nor a peak linear heat rate (LHR) which corresponds to the temperature for fuel centerline melting will occur. This trip is the primary protection against fuel centerline melting.

9a. <u>Thermal Margin/Low Pressure</u>

The TM/LP trip prevents exceeding the DNBR SL during AOOs and aids the ESFAS during certain accidents. The following events require TM/LP protection:

a. excess load (inadvertent opening of an SG ADV),
b. RCS depressurization (inadvertent safety or power-operated relief valves (PORVs) opening,
c. SG tube rupture, and
d. LOCA accident.

The first two events are AOOs, and fuel integrity is maintained. The third and fourth are accidents, and limited fuel damage may occur. The trip is initiated whenever the RCS pressure signal drops below a minimum value (P_{min}) or a computed value (P_{var}) as described below, whichever is higher. The computed value is a function Q power, ASI, as determined from the axially-split excore detectors, reactor inlet (cold-leg) temperature, and the number of RCPs operating.

The minimum value of reactor coolant flow rate, the maximum AZIMUTHAL POWER TILT, and the maximum CEA

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

deviation permitted for continuous operation are assumed in the generation of this trip function. In addition, CEA group sequencing in accordance with LCO 3.1.7, "Regulating CEA Limits," is assumed. Finally, the maximum insertion of CEA banks that can occur during any AOO prior to a VHPT is assumed.

9b. Asymmetric Steam Generator Transient Protective Trip Function

The ASGTPTF provides protection for those AOOs associated with secondary system malfunctions which result in asymmetric primary coolant temperatures. The most limiting event is closure of a single main steam isolation valve. ASGTPF is provided by comparing the secondary pressure in both SGs in the TM/LP calculator. If the pressure in either exceeds that in the other by the trip setpoint, a TM/LP trip will result.

10. Loss of Load

The loss-of-load (turbine stop valve (TSV) control oil pressure) trip is anticipatory for the loss of heat-removal capabilities of the secondary system following a turbine trip. The loss-of-load trip prevents lifting the pressurizer safety valves, PORVs, and MSSVs in the event of a turbine-generator trip. Thus the trip minimizes the pressure and temperature transients on the reactor by initiating trip well before reaching Pressurizer Pressure--High trip and pressurizer safety valve setpoints. The four RPS loss-of-load reactor trip channels receive their input from sensors mounted on the high-pressure TSV actuators. Since there are four high-pressure TSVs, one actuator per valve and one sensor per actuator, each sensor sends its signal to a different RPS channel. When the turbine trips, control oil is dumped from the high-pressure TSVs. When the control oil pressure drops to the appropriate setpoint, a reactor trip signal is generated.

11. Reactor Protection System Logic

The RPS logic provides for automatic trip initiation to maintain the SLs during AOOs and assist the ESF

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

systems in assuring acceptable consequences during accidents. All transients and accidents that call for a reactor trip assume the RPS logic is functioning as designed.

12. Reactor Trip Circuit Breakers

All of the transient and accident analyses which call for a reactor trip assume that the RTCBs operate and interrupt power to the CEDMs.

13. Manual Reactor Trip

The Manual Reactor Trip is part of the RPS circuitry. It is used by the operator to shut down the reactor whenever any parameter is rapidly trending toward its trip setpoint. A manual trip accomplishes the same results as any one of the automatic trip functions.

14. Interlocks/Bypasses

The automatic bypass removal features must function as a backup to manual actions for all safety-related trips to assure the trip functions are not operationally bypassed when the safety analysis assumes the functions are not bypassed. These are:

14a. Zero power mode bypass (ZPMB) removal on the TM/LP, ASGTPTF, and reactor coolant low flow trips when THERMAL POWER is < 1E-4% RATED THERMAL POWER (RTP). This bypass is manually enabled below the specified setpoint to permit low-power testing. The wide-range NI Level 1 bistable in the wide-range drawer permits manual bypassing below the setpoint and removes the bypass above the setpoint.

14b,c. Power rate of change bypass removal. The Power Rate of Change--High trip is automatically bypassed at < 1E-4% RTP, as sensed by the wide-range NI Level 2 bistable, and at > 12% RTP by the power-range NI Level 1 bistable mounted in their respective NI drawers. Automatic bypass

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

removal is also effected by these bistables when conditions are no longer satisfied.

14d. Loss of Load and APD--High bypass removal. The Loss of Load and APD--High trips are automatically bypassed when at < 15% RTP as sensed by the power-range NI Level 1 bistable. The bypass is automatically removed by this bistable above the setpoint. This same bistable is used to bypass the Power Rate of Change--High trip.

14e. SG Pressure--Low bypass removal. The SG Pressure--Low trip is manually enabled below the pre-trip setpoint. The permissive is removed, and the bypass automatically removed, when the SG Pressure--Low pre-trip clears.

The RPS Instrumentation satisfies Criterion 3 of the NRC Interim Policy Statement.

LCO

The LCO requires all instrumentation performing an RPS function to be OPERABLE. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected functions. The specific criteria for determining channel OPERABILITY differ slightly between functions. These criteria are discussed on a function-by-function basis below.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same function bypassed. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the function to four-channel operation (two-out-of-four logic) or placing the channel in trip (one-out-of-three logic). At plants where adequate channel-to-channel independence has been demonstrated, specific exceptions have been approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed, for an extended period of time.

Only the ALLOWABLE VALUES are specified for each RPS trip function in the LCO. Nominal trip setpoints are specified

(continued)

(continued)

BASES (continued)

LCO (continued)

in the plant-specific setpoint calculations. The nominal setpoints are selected to ensure the setpoints measured by CHANNEL FUNCTIONAL TESTS do not exceed the ALLOWABLE VALUE if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its ALLOWABLE VALUE, is acceptable provided that operation and testing is consistent with the assumptions of the plant-specific setpoint calculations. Each ALLOWABLE VALUE specified is more conservative than the analytical limit assumed in the safety analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 6).

The trip functions specified in TABLE 3.3.1-1 are considered OPERABLE when:

1. All channel components necessary to provide a reactor trip are functional and in service;
2. Channel measurement uncertainties are known (via test, analysis, or design information) to be within the assumptions of the setpoint calculations;
3. Required Surveillance testing is current and has demonstrated performance within each Surveillance test's acceptance criteria; and
4. The associated operational bypass is not enabled except under the conditions specified in the LCO Applicability for the function.

The following bases for each trip function identify the above RPS trip-function criteria items which are applicable to establish the trip function OPERABILITY:

1. <u>Variable High Power Trip--High</u>

   This LCO requires all four channels of the VHPT to be OPERABLE in MODES 1 and 2.

(continued)

(continued)

BASES (continued)

LCO (continued)

VHPT--High trip channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is high enough to provide an operating envelope that prevents unnecessary linear power level high reactor VHPT--High trips during normal plant operations. ALLOWABLE VALUE is low enough for the system to maintain a margin to unacceptable fuel-cladding damage should a CEA ejection accident occur.

The VHPT setpoint is operator adjustable and can be set at a fixed increment above the indicated THERMAL POWER level. Operator action is required to increase the trip setpoint as THERMAL POWER is increased. The trip setpoint is automatically decreased as THERMAL POWER decreases. The trip setpoint has a maximum and a minimum setpoint.

Adding to this maximum value the possible variation in trip point due to calibration and instrument errors, the maximum actual steady-state THERMAL POWER level at which a trip would be actuated is 112% of RTP, which is the value used in the safety analyses.

To account for these errors, the safety analysis minimum value is 40% RTP. The 10% step is a maximum value assumed in the safety analyses. There is no uncertainty applied to the step.

2. Power Rate of Change--High

This LCO requires [four] channels of the Power Rate of Change--High to be OPERABLE in MODES 1 and 2, as well as in MODES 3, 4, and 5 when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

Power Rate of Change--High channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The high power rate of change trip serves as a backup to the administratively enforced startup rate limit. [For this facility, the basis for the ALLOWABLE VALUE is as follows:]

(continued)

(continued)

BASES (continued)

LCO (continued)

3. Reactor Coolant Flow--Low

This LCO requires four channels of the Reactor Coolant Flow--Low to be OPERABLE in MODES 1 and 2.

Reactor Coolant Flow--Low channels are OPERABLE when OPERABILITY requirements 1, 2, and 3, and 4 are satisfied.

The trip may be manually bypassed when THERMAL POWER falls below 1E-4% RTP. This bypass is part of the ZPMB circuitry, which also bypasses the TM/LP trip and provides a low power block signal to the Q power select logic. This ZPMB allows low-power physics testing at reduced RCS temperatures and pressures. It also allows heatup and cooldown with shutdown CEAs withdrawn.

This trip is set high enough to maintain fuel integrity during a loss-of-flow condition. The setting is low enough to allow for normal operating fluctuations from offsite power. To account for analysis uncertainties, the value in the safety analysis is 93% RTP.

4. Pressurizer Pressure--High

This LCO requires four channels of Pressurizer Pressure--High to be OPERABLE in MODES 1 and 2.

Pressurizer Pressure--High channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

This ALLOWABLE VALUE is set high enough to allow for pressure increases in the RCS during normal operation (i.e., plant transients) not indicative of an abnormal condition. The setting below the lift setpoint of the pressurizer safety valves and low enough to initiate a reactor trip when an abnormal condition is indicated. The difference between the ALLOWABLE VALUE and the analysis setpoint of 2470 psia includes allowance for harsh environment.

This trip concurrent with PORVs operation avoids the undesired operation of the pressurizer safety valves.

(continued)

(continued)

BASES (continued)

LCO (continued)

5. Containment Pressure--High

This LCO requires four channels of Containment Pressure--High to be OPERABLE in MODES 1 and 2.

Containment Pressure--High trip channels are OPERABLE when requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup), and not indicative of an abnormal condition. The setting is low enough to initiate a reactor trip to prevent containment pressure from exceeding design pressure following a DBA. The 4 psig setpoint is also assumed in the safety analysis and includes an uncertainty of +.75 and -.25 psig.

6. Steam Generator Pressure--Low

This LCO requires four channels of SG Pressure--Low per SG to be OPERABLE in MODES 1 and 2.

SG Pressure--Low channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE is sufficiently below the full-load operating value for steam pressure so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of excessive steam demand. Since excessive steam demand causes the RCS to cool down, resulting in positive reactivity [illegible] to the core, a reactor trip is required to of[illegible] that effect.

The difference between the ALLOWABLE VALUE and the safety analysis value of 600 psia includes harsh environment uncertainties.

The function may be manually bypassed as SG pressure is reduced during controlled plant shutdowns. This bypass is permitted at a preset SG pressure. The

(continued)

(continued)

BASES (continued)

LCO (continued)

bypass, in conjunction with the ZPMB, allows testing at low temperatures and pressures, and heatup and cooldown with the shutdown CEAs withdrawn. From a bypass condition the trip will be reinstated automatically as SG pressure increases above the preset pressure.

7. Steam Generator Water Level--Low

This LCO requires four channels of SG Water Level--Low per SG to be OPERABLE in MODES 1 and 2.

SG Water Level--Low channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is sufficiently below the normal operating level for the SGs so as not to cause a reactor trip during normal plant operations. The trip setpoint is high enough to ensure a reactor trip signal is generated before water level drops below the narrow range instrumentation tap (with a 5% allowance for instrument error). The reactor trip will remove the heat source (except decay heat), thereby conserving the reactor heat sink.

8. Axial Power Distribution--High

This LCO requires four channels of APD--High to be OPERABLE in MODE 1.

APD--High channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The APD--High trip function ALLOWABLE VALUES ensure that neither a DNBR less than the SL nor a peak LHR, which corresponds to the temperature for fuel centerline melting, will exist as a consequence of axial power maldistributions. This trip is the primary protection against fuel centerline melting.

The ALLOWABLE VALUE curve was derived from an analysis of many axial power shapes with allowances for instrumentation inaccuracies and the uncertainty associated with the excore to incore ASI relationship.

(continued)

(continued)

BASES (continued)

LCO (continued)

The APD trip is automatically bypassed < 15% RTP, where it is not required for reactor protection.

9a. Thermal Margin/Low Pressure

This LCO requires four channels of TM/LP to be OPERABLE in MODES 1 and 2.

TM/LP channels are OPERABLE when the OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE includes allowances for equipment response time, measurement uncertainties, processing error and a further allowance to compensate for the time delay associated with providing effective termination of the occurrence that exhibits the most rapid decrease in margin to the SL.

This trip may be manually bypassed when THERMAL POWER falls below 1E-4% RTP. This bypass is part of the ZPMB circuitry, which also bypasses the Reactor Coolant Flow-Low trip and provides a ΔT power block signal to the Q power select logic. This ZPMB allows low-power physics testing at reduced RCS temperatures and pressures. It also allows heatup and cooldown with shutdown CEAs withdrawn.

9b. Asymmetric Steam Generator Transient Protective Trip Function

This LCO requires four channels of ASGTPTF to be OPERABLE in MODES 1 and 2.

ASGTPTF channels are considered OPERABLE when OPERABILITY requirements 1, 2, 3 and 4 are satisfied.

The ALLOWABLE VALUE is high enough to avoid trips caused by normal operation and minor transients, but assures DNBR protection in the event of Design Basis Events. The difference between the ALLOWABLE VALUE and the 175 psia analysis setpoint allows for 40 psia of measurement uncertainty.

The trip may be bypassed when THERMAL POWER falls below 1E-4% RTP. The ASGTPTF is subject to the ZPMB,

(continued)

(continued)

BASES (continued)

LCO (continued)

since it is an input to the TM/LP trip, and is not required for protection at low-power levels.

10. Loss of Load

This LCO requires [four] of the loss-of-load trip channels to be OPERABLE in MODE 1.

The loss-of-load channels are considered OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

[For this facility, the basis for ALLOWABLE VALUE is as follows:]

The loss-of-load trip may be bypassed when THERMAL POWER falls below 15%, since it is no longer needed to prevent lifting of the pressurizer safety valves, SG safety valves, or ADVs in the event of a loss of load. The Nuclear Steam Supply System (NSSS) and the Steam Dump System are capable of accommodating the loss of load without requiring the use of the above equipment.

11. Reactor Protection System Logic

Failures of individual bistable relays and their contacts are addressed in Functions 1 through 10. This specification addresses failures of the matrix logic not addressed in the above, such as the failure of matrix relay power supplies or the failure of the trip channel bypass contact in the bypass condition.

Loss of a single vital bus will de-energize one of the two power supplies in each of three matrices. This will result in four RTCBs opening; however, the remaining four closed RTCBs will prevent a reactor trip. For the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure is to be treated as a single channel failure, providing the affected matrix relays de-energize as designed, opening the affected RTCBs.

(continued)

(continued)

LCO (continued)

Each of the four initiation logic channels opens one set of RTCBs if any of the six coincidence matrices de-energize their associated matrix relays. They thus perform a logical OR function. Each initiation logic channel has its own power supply and is independent of the others. An initiation logic channel includes the matrix relay through to the K-relay contacts, which open the RTCB.

It is possible for two initiation logic channels affecting the same trip leg to de-energize if a matrix power supply or vital instrument bus fails. This will result in opening the two affected sets of RTCBs.

If one set of RTCBs has been opened in response to a single RTCB channel, initiation logic channel, or Manual Reactor Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance testing on the OPERABLE initiation logic, RTCB, and manual trip channels. In this case the redundant set of RTCBs will provide protection if a trip should be required. It is unlikely that trip will be required during the Surveillance testing, coincident with a failure of the remaining series RTCB channel. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, manual trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

11a. Matrix Logic

This LCO requires six channels of matrix logic to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when the RTCBs are closed and CEA Drive System is capable of CEA withdrawal.

Matrix logic channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

11b. Initiation Logic

This LCO requires four channels of initiation logic to be OPERABLE in MODES 1 and 2, and in MODES 3, 4, and 5 when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

(continued)

(continued)

LCO (continued)

Initiation logic channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

12. Reactor Trip Circuit Breakers

The LCO requires four RTCB channels to be OPERABLE in MODES 1 and 2, as well as in MODES 3, 4, and 5 when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

RTCB channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

Each channel consists of two breakers operated in a single set by the initiation logic or Manual Reactor Trip circuitry. This ensures that power is interrupted at identical locations in the trip legs for both CEDM buses, thus preventing power removal to only one CEDM bus (a half trip).

Failure of a single breaker affects the entire channel, and both breakers in the set must be opened.

Without reliable RTCBs and associated support circuitry, a reactor trip cannot occur whether initiated automatically or manually.

Each channel of RTCBs starts at the contacts which are actuated by the K-relay, and the contacts which are actuated by the Manual Reactor Trip, for each set of breakers. The K-relay actuated contacts and the upstream circuitry are considered to be RPS logic and fall under the requirements of Function 11. Manual Reactor Trip contacts and upstream circuitry are considered to be Manual Reactor Trip circuitry and fall under the requirements of Function 13.

If one set of RTCBs has been opened in response to a single RTCB channel, initiation logic channel, or Manual Reactor Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance testing on the OPERABLE initiation logic, RTCB, and manual trip channels. In this case the redundant set of RTCB will provide protection. If a single matrix power supply or vital bus failure has

(continued)

(continued)

DRAFT

BASES (continued)

LCO (continued)

opened two sets of RTCBs, manual trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

13. Manual Reactor Trip

The LCO requires all [four] Manual Reactor Trip channels to be OPERABLE in MODES 1 and 2, and MODES 3, 4, and 5 when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

Manual reactor trip channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

Two independent sets of two adjacent push buttons are provided at separate locations. Each push button is considered a channel and operates two of the eight RTCBs. Depressing both push buttons in either channel will cause an interruption of power to the CEDMs, allowing the CEAs to fall into the core. This design ensures that no single failure in any push button circuit can either cause or prevent a reactor trip.

Manual Reactor Trip push buttons are also provided at the reactor trip switchgear (locally) in case the control room push buttons become inoperable, or the control room becomes uninhabitable. These are not part of the RPS and cannot be credited in fulfilling the LCO OPERABILITY requirements. Furthermore, LCO Actions need not to be entered due to failure of a local manual trip.

14. Interlocks/Bypasses

The LCO on bypass permissive removal channels requires that the automatic bypass removal feature of all [four] operating bypass channels be OPERABLE for each RPS function with an operating bypass in the MODES addressed in the specific LCO for each function. All [four] bypass removal channels must be OPERABLE to ensure that none of the four RPS channels is inadvertently bypassed.

Interlock channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

(continued)

(continued)

BASES (continued)

LCO (continued)

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue.

Interlock function ALLOWABLE VALUES are based on analysis of functional requirements for the bypassed functions. These are discussed above as part of the LCO discussion for the affected functions.

[For this facility, the following support systems are required OPERABLE to ensure RPS instrumentation OPERABILITY.]

[For this facility, those required support systems which upon their failure, do not require declaring the RPS instrumentation inoperable and their justification are as follows:]

[For this facility, the supported systems impacted by the inoperability of the RPS instrumentation and the justification of whether or not each supported system is declared inoperable are as follows:] It should be noted that LCO 3.3.1 may need to be augmented with additional conditions, if it is determined that the RPS provides support to other systems.

APPLICABILITY

Most RPS trips are required to be OPERABLE in MODES 1 and 2 because the reactor is critical in these MODES. The trips are designed to take the reactor subcritical, which maintains the SLs during AOOs, and assists the ESFAS in providing acceptable consequences during accidents. Exceptions to this are:

- The APD--High Trip (Function 8) and loss of load (Function 10) are only applicable in MODE 1, because they are automatically bypassed below at < 15% RTP, where they are no longer needed.
- The Power Rate of Change--High trip, RPS Logic (Function 11), RTCBs (Function 12), and Manual Reactor Trip (Function 13) are also required in MODES 3, 4,

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events.

Most trips are not required to be OPERABLE in MODES 3, 4, and 5. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by assuring adequate SHUTDOWN MARGIN.

A Note has been added to provide clarification that for this LCO, each function specified in Table 3.3.1-1 is treated as an independent entity with an independent Completion Time.

ACTIONS

A protection function channel is inoperable when it does not satisfy the OPERABILITY criteria for the functions channels. These criteria are outlined for each function, in the LCO section of Bases. The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis. Typically the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is less conservative than the ALLOWABLE VALUE in Table 3.3.1-1, the channel is declared inoperable immediately, and the appropriate Condition(s) from Table 3.3.1-1 must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the ALLOWABLE VALUE, or the transmitter, instrument loop, signal-processing electronics, or RPS bistable is found inoperable, then all affected functions provided by that channel must be declared inoperable and the unit must enter the Condition for the particular protection function affected.

When the number of inoperable channels in a trip function exceeds that specified in any related Condition associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered, if applicable in the current MODE of operation.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition A

Condition A is applicable to all RPS protection functions. Condition A addresses the situation where one or more channels for one or more functions are inoperable at the same time. The Required Action is to refer to Table 3.3.1-1 and immediately take the Required Actions for the protection functions affected.

Condition B

Condition B applies to the failure of a single channel in any of the following RPS functions: VHPT--High; Power Rate of Change--High; Reactor Coolant Flow--Low; Pressurizer Pressure--High; Containment Pressure--High; SG Pressure--Low; SG Water Level--Low; APD--High; TM/LP; ASGTPTF; or loss of load. RPS coincidence logic is normally two-out-of-four.

Required Action B.1 is the preferred action as it restores full functional capability of the RPS.

If one RPS channel is inoperable, startup or power operation is allowed to continue providing the inoperable channel is placed in bypass or trip within 1 hour (Required Action B.2.1). By specifying either option, the possibility of inadvertently bypassing a redundant channel is eliminated. The provision of four trip channels allows one channel to be bypassed (removed from service) during operations, placing the RPS in two-out-of-three coincidence logic. It is preferable to place an inoperable channel in bypass rather than trip, since no additional random failure of a single channel can either spuriously trip the reactor or prevent it from tripping.

The Completion Time of 1 hour allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

For plants that have not demonstrated sufficient channel-to-channel independence, the failed channel is restored to OPERABLE status or is placed in trip within 48 hours (Required Action B.2.2.1 or Required Action

(continued)

(continued)

ACTIONS (continued)

B.2.2.2). Required Action B.2.2.1 restores the full capability of the function. Required Action B.2.2.2 places the function into a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip.

The 48-hour Completion Time is based on operating experience, which has demonstrated that a random failure of a second channel occurring during the 48-hour period is a low-probability event.

<u>Condition C</u>

Condition C applies to the failure of two channels in any of the following RPS functions: VHPT--High; Power Rate of Change--High; Reactor Coolant Flow--Low; Pressurizer Pressure--High; Containment Pressure--High; SG Pressure--Low; SG Water Level--Low; APD--High; TM/LP; ASGTPTF; or loss of load.

Required Action C.1 is the preferred action as it improves the functional reliability of the RPS. The allowed Completion Time of 1 hour is sufficient time to perform the Required Action.

Required Action C.2.1 and Required Action C.2.2 provide for placing one inoperable channel in bypass, and the other channel in trip within the 1-hour Completion Time. This time is sufficient to allow the operator to take all appropriate actions for the failed channels and still ensures the risk involved in operating with the failed channels is acceptable. With one channel of protective instrumentation bypassed, the RPS is in a two-out-of-three logic; but with another channel failed, the RPS may be operating in a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

The bypassed channel should be restored to OPERABLE status within 48 hours, for reasons similar to those stated under Condition B. After one channel is restored to OPERABLE, the provisions of Condition B still apply to the remaining

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action C.2.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.

Condition D

Condition D applies to one initiation logic channel (Function 11.b), RTCB channel (Function 12) or Manual Reactor Trip channel (Function 13), in MODES 1 and 2, since they have the same actions. MODES 3, 4, and 5 with the RTCBs shut are addressed in Condition R. These actions involve either repairing the channel or opening the affected RTCBs. The latter removes the need for the affected channel by performing its associated safety function. With an RTCB open, the affected functions are in one-out-of-two logic, which meets redundancy requirements, but testing on the OPERABLE channels cannot be performed without causing a reactor trip, unless the RTCBs in the inoperable channels are closed to permit testing. Therefore, the RTCBs associated with one inoperable channel may be closed for up to 1 hour for the performance of an RPS CHANNEL FUNCTIONAL TEST. The specific actions allowed are as follows:

Required Action D.1 is the preferred action, as it restores the functional reliability of the RPS.

Required Action D.2 provides for opening the RTCBs associated with the inoperable channel within a 1-hour Completion Time. This action is conservative since depressing the manual reactor trip push button associated with either set of breakers in the other trip leg will cause a reactor trip. With this configuration, a single channel failure will not prevent a reactor trip. The allotted Completion Time is adequate to open the affected RTCBs, while maintaining the risk of having them closed at an acceptable level.

Condition E

Conditions E and K apply to one automatic bypass removal channel inoperable. They differ only in the shutdown track invoked if the required actions and associated Completion Times are not met. If the bypass removal channel for any operating bypass cannot be restored to OPERABLE, the

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise the affected RPS channel must be declared inoperable, as in Condition B, and the bypass either removed, or the bypass removal channel repaired. The bases for Required Actions and Completion Times are the same as discussed for Condition B.

Condition F

Conditions F and L apply to two inoperable automatic bypass removal channels. If the bypass removal channels for two operating bypasses cannot be restored to OPERABLE, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise the affected RPS channels must be declared inoperable, as in Condition C, and the bypass either removed, or the bypass removal channel repaired. Also, Required Action F.3.2 provides for the restoration of the one affected automatic trip channel to OPERABLE status within the rules of Completion Time specified under Condition C. Completion Times are consistent with Condition C.

Condition G

Condition G is entered when the Required Actions and associated Completion Times of Condition B, C, D, E, or F are not met.

If the Required Actions associated with these Conditions cannot be completed within the required Completion Times, the reactor must be brought to a MODE in which the Required Actions do not apply. Six hours is a reasonable time, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

Condition H

The excore detectors are used to generate the internal ASI used as an input to the TM/LP, and APD--High trips. Incore detectors provide a more accurate measurement of ASI. If one or more excore detectors cannot be calibrated to match incore detectors, power is restricted or reduced during subsequent operations because of increased uncertainty associated with using uncalibrated excore detectors.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Calibration need only be performed above 15% RTP because uncertainties in the ASI measurement process make it unreliable below this power level.

[For this facility, the 24-hour Completion Time is justified as follows:]

Condition I

Condition I is identical to Condition B except for the shutdown track invoked if the Required Actions and associated Completion Times are not met. Since Condition I applies to MODES 3, 4, and 5 with the RTCBs closed, the shutdown track imposed by Condition M requires opening the RTCBs.

Condition J

Condition J is identical to Condition C except for the shutdown track invoked if the Required Actions and associated Completion Times are not met. Since Condition J applies to MODES 3, 4, and 5 with the RTCBs closed, the shutdown track imposed by Condition M requires opening the RTCBs.

Condition K

Condition K is identical to Condition [illegible] except for the shutdown track invoked if the Required Actions and associated Completion Times are not met. Since Condition K applies to MODES 3, 4, and 5 with the RTCBs closed, the shutdown track imposed by Condition M requires opening the RTCBs.

Condition L

Condition L is identical to Condition F except for the shutdown track invoked if the Required Actions and associated Completion Times are not met. Since Condition L applies to MODES 3, 4, and 5 with the RTCBs closed, the shutdown track imposed by Condition M requires opening the RTCBs.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition M

Condition M is entered when the Required Actions and associated Completion Times of Conditions I, J, K, or L are not met.

If actions associated with these conditions cannot be completed within the required Completion Time, opening the RTCBs brings the reactor to a MODE where the Required Actions do not apply, and ensures no CEA withdrawal will occur. [For this facility, the basis for the 6-hour Completion Time is as follows:]

Condition N

Condition N applies if one matrix logic channel (Function 11.a) is inoperable in MODES 1 and 2. MODES 3, 4, and 5 with the RTCBs closed are addressed in Condition Q. Loss of a single vital instrument bus will de-energize one of the two matrix power supplies in up to three matrices. This is considered a single matrix failure, providing the matrix relays associated with the failed power supplies de-energize as required.

[For this facility, the consequences for the matrix relays not de-energizing as required are as follows:]

The channel must be restored to OPERABLE status within 48 hours. The 48-hour Completion Time provides the operator time to take appropriate actions and still assure that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second matrix logic channel is low during any given 48-hour interval. If the channel cannot be restored to OPERABLE status within 48 hours, Condition P is entered.

Condition O

Condition O applies to the failure of both initiation logic channels (Function 11.b) affecting the same trip leg. Since this will open two channels of RTCBs, this Condition is also applicable to the two affected RTCBs. This condition allows for loss of a single vital instrument bus or matrix power supply, which will de-energize both initiation logic

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

channels in the same trip leg. This will open both sets of RTCBs in the affected trip leg, satisfying the Required Action of opening the affected RTCBs.

Of greater concern is the failure of the initiation circuit in a non-trip condition (e.g., due to two initiation (K) relay failures). With only one initiation logic channel failed in a non-trip condition, there is still the redundant set of RTCBs in the trip leg. With both failed in a non-trip condition, the reactor will not trip automatically when required. In either case, the affected RTCBs must be opened immediately by using the appropriate manual trip push buttons, since each of the four push buttons opens one set of RTCBs, independent of the initiation circuitry. Caution must be exercised, since depressing the wrong push buttons may result in a reactor trip.

If the affected RTCB(s) cannot be opened, Condition P is entered. This would only occur if there is a failure in the manual trip circuitry, or the RTCB(s).

<u>Condition P</u>

Condition P is entered if actions associated with Conditions N or O are not met within the required Completion Time.

If the RTCBs associated with the inoperable channel cannot be opened, the reactor must be shut down within 6 hours and all the RTCBs open. Six hours is a reasonable time, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

<u>Condition Q</u>

Condition Q applies to one matrix logic channel inoperable in MODES 3, 4, or 5. In these MODES the probability of most accidents or transients occurring (and their associated consequences) is significantly reduced. Therefore, there is no need to move to a different MODE if one channel is inoperable. Opening the RTCBs will not cause a transient. The channel must be restored to OPERABLE status within 48 hours.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

If the inoperable channel cannot be restored to OPERABLE status within 48 hours, all RTCBs must be opened, placing the plant in a MODE where the LCO does not apply, and ensuring no CEA withdrawal occurs.

[For this facility, the basis for the 48-hour Completion Time is as follows:]

<u>Condition R</u>

Condition R applies to the failure of one initiation logic channel (Function 11.b), RTCB channel (Function 12), or manual reactor trip channel (Function 13) affecting the same trip leg in MODES 3, 4, or 5 with the RTCBs closed. The channel must be restored to OPERABLE status within 48 hours. If the inoperable channel cannot be restored to OPERABLE status within 48 hours, all RTCBs must be opened, placing the plant in a MODE in which the LCO does not apply, and ensuring no CEA withdrawal occurs.

[For this facility, the basis for the 48-hour Completion Time is as follows:]

<u>Condition S</u>

Condition S applies to two initiation logics, RTCB channels, or Manual Reactor Trip channels inoperable in MODES 3, 4, or 5, with the RTCBs closed. Condition S is similar to Condition O in that it allows for loss of a single vital instrument bus or matrix power supply, which will de-energize both initiation logic channels in the same trip leg. This will open both sets of RTCBs in the affected trip leg, satisfying the Required Action of opening the affected RTCBs.

In the event that two channels fail in a non-trip condition, the affected RTCBs must be opened immediately to restore reactor trip capability. In these MODES the probability of most accidents or transients occurring (and their associated consequences) is significantly reduced. Therefore, there is no need to move to a different MODE if one channel is inoperable. Opening the affected RTCBs restores automatic and manual reactor trip capability in a one-out-of-two logic in the remaining trip leg.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition T

Condition T is applicable to each one of the RPS functions presented in Table 3.3.1-1.

Required Action T.1 verifies that all required support features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 must be immediately entered. However, if the support feature LCO or RPS LCO takes into consideration the loss-of-function situation, then LCO 3.0.3 may not need to be entered.

SURVEILLANCE REQUIREMENTS

The SRs for any particular RPS function are found in the SR column of Table 3.3.1-1 for that function. Most functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION and response-time testing.

In order for a facility to take credit for topical reports as the basis for justifying Surveillance Frequencies, topical reports must be supported by an NRC Staff safety evaluation report that establishes the acceptability of each topical report for that facility.

SR 3.3.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

(continued)

(continued)

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal-processing equipment has drifted outside its limits. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Surveillance Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited to 12 hours. Since the probability of two random failures in redundant channels in any 12-hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

<u>SR 3.3.1.2</u>

A daily calibration (heat balance) is performed when THERMAL POWER is $\geq$ 15%. The daily calibration shall consist of adjusting the "nuclear power calibrate" potentiometers to agree with calorimetric calculation if the absolute difference is > 1.5%. The "ΔT power calibrate" potentiometers are then used to null the "nuclear power—ΔT power" indicators on the RPS Reactor Power and Indication panel. Performance of the daily calibration ensures that the two inputs to the Q power measurement are indicating accurately with respect to the much more accurate secondary calorimetric. The Frequency of 24 hours is based on plant operating experience and takes into account indications and alarms located in the control room to detect deviations in channel outputs. The Surveillance Frequency is modified by a Note indicating this test need only be performed when THERMAL POWER is $\geq$ 15% RTP. The secondary calorimetric is

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

inaccurate at lower power levels. A second Note indicates the daily calibration may be suspended during PHYSICS TESTS. [At this facility, the basis for this Note is as follows:]

SR 3.3.1.3

It is necessary to calibrate the excore power range channel upper and lower subchannel amplifiers such that the internal ASI used in the TM/LP and APD--High trips reflects the true core power distribution as determined by the incore detectors. A Note to the Surveillance Frequency indicates the test is only required when THERMAL POWER is ≥ 15% RTP. Uncertainties in the excore and incore measurement process make it unnecessary to calibrate when below 15% RTP. If the excores are not properly calibrated to agree with the incores, power is restricted during subsequent operations because of increased uncertainty associated with using uncalibrated excore detectors. The 31-day Surveillance Frequency is adequate, based on operating experience of the excore linear amplifiers and the slow burnup of the detectors. The excore readings are a strong function of the power produced in the peripheral fuel bundles, and do not represent an integrated reading across the core. Slow changes in neutron flux during the fuel cycle can also be detected at this interval.

SR 3.3.1.4

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed.

In addition to power supply tests, The RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 7. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

Bistable Tests. "As found" and "as left" values for bistable trip setpoints are recorded. The bistable setpoint must be found to trip within the ALLOWABLE VALUES specified in the LCO. The difference between the current "as found" and the previous test "as left" values must be consistent with the drift allowance used in the setpoint analysis. Wherever these tolerances are not met, a recalibration can

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

be performed to establish OPERABILITY of the channel. However, repeated consecutive failures would be indicative of a failure that cannot be corrected by recalibration alone.

A test signal is then superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS channel trip channel bypassed.

[For this facility, the justification for the 92-day Frequency for bistables is as follows:]

Matrix Logic Tests. This test is performed one matrix at a time. It verifies that a coincidence in the two input channels for each function removes power from the matrix relays. During testing, power is applied to the matrix relay test coils, and prevents the matrix relay contacts from assuming their de-energized state. This test will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

[For this facility, the justification for the 92-day Frequency for matrix logics is as follows:]

Trip Path Tests. These tests are similar to the matrix logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The Surveillance Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

SR 3.3.1.5

A CHANNEL CALIBRATION of the excore power range channels every 92 days ensures that the channels are reading accurately and within tolerance. A Note is added stating that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices, with minimal drift, and because of the difficulty of simulating a

(continued)

(continued)

SURVEILLANCE REQUIREMENTS (continued)

meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3). In addition, associated control room indications are continuously monitored by the operators.

The Surveillance Frequency of 92 days is acceptable, based on plant operating experience, and takes into account indications and alarms available to the operator in the control room.

SR 3.3.1.6

A CHANNEL FUNCTIONAL TEST on the loss of load, power rate of change and manual reactor trip channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. The loss-of-load pressure sensor cannot be tested during reactor operation without closing the high-pressure TSV, which would result in a turbine trip or reactor trip. The Power Rate of Change--High trip function is required during startup operation, and is bypassed when shut down or > 15% RTP. The Manual Reactor Trip function can either be tested at power or shut down; however, the simplicity of this circuitry and the absence of drift concern makes this interval adequate. Additionally, operating experience has shown that these components usually pass the Surveillance when performed on the 7 day Frequency prior to each reactor startup.

SR 3.3.1.7

SR 3.3.1.7 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.1.4, except SR 3.3.1.7 is applicable only to bypass functions and is performed once within 92 days prior to each startup. Proper operation of bypass permissives is critical during plant startup because the bypasses must be in place to allow startup operation and must be removed at the appropriate points during power ascent to enable certain reactor trips. Consequently, the appropriate time to verify bypass removal function OPERABILITY is just prior to startup. The allowance to conduct this test within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

Evaluation" (Ref. 8). Once the operating bypasses are removed the bypasses must not fail in such a way that the associated trip function gets inadvertently bypassed. This feature is verified by the trip function CHANNEL FUNCTIONAL TEST, SR 3.3.1.4. Therefore, further testing of the bypass function after startup is unnecessary.

SR 3.3.1.8

Each RTCB is actuated by an undervoltage coil and a shunt trip coil. The system is designed so that either de-energizing the undervoltage coil or energizing the shunt trip coil will cause the circuit breaker to open. When an RTCB is opened, either during an automatic reactor trip or by using the manual push buttons in the control room, the undervoltage coil is de-energized and the shunt trip coil is energized. This makes it difficult to determine if one of the coils or associated circuitry is defective.

Therefore, once per 18 months a CHANNEL FUNCTIONAL TEST is performed which tests all four sets of undervoltage coils, and all four sets of shunt trip coils, individually. During undervoltage coil testing, the shunt trip coils shall remain de-energized, preventing their operation. Conversely, during shunt trip coil testing, the undervoltage coils shall remain energized, preventing their operation. This test ensures that every undervoltage coil, and every shunt trip coil is capable of performing its intended function, and that no single active failure of any RTCB component will prevent a reactor trip. The 18-month Frequency was developed considering it is prudent that these surveillances be performed only during a plant outage. This is due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the 18-month Frequency.

If one set of RTCBs has been opened in response to a single RTCB channel, initiation logic channel, or manual reactor trip channel failure, the affected set of RTCBs may be closed for up to 1 hour in accordance with LCO 3.0.5 for Surveillance testing on the OPERABLE initiation logic, RTCB, and manual trip channels. In this case the redundant set of

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

RTCBs will provide protection if a trip should be required. It is unlikely that a trip will be required during the Surveillance testing, coincident with a failure of the remaining series RTCB channel. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, manual trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

SR 3.3.1.9

SR 3.3.1.9 is the performance of a CHANNEL CALIBRATION every 18 months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to the measured parameter with the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive tests, to ensure that the instrument channel remains operational with the setpoint within the assumptions of the plant-specific setpoint analysis. Transmitter "as found" values and "as left" values are recorded and used to verify drift assumptions. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint errors are within the assumptions of the plant-specific setpoint analysis. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis.

Recalibration restores the OPERABILITY of an otherwise functional component found to have errors larger than assumed by the setpoint analysis. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure that cannot be corrected by recalibration.

Field transmitters may be calibrated in place, removed and calibrated in a laboratory, or replaced with an equivalent, laboratory-calibrated, unit. RTD channels may be calibrated in place, using cross-calibration techniques, or in a test bath after removal from piping. For cross-calibration, at least one RTD should be replaced with a newly calibrated RTD

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

during each refueling cycle to ensure accurate RTD cross-cross-calibration. This replacement RTD must be the same model as the remaining RTDs. Using a newly calibrated RTD as a reference assures RTD signal drift continues to remain random rather than systematic, and is within the limits specified in the plant-specific setpoint analysis. The replacement interval may be extended to alternate refueling, if it is demonstrated that over the extended interval the RTDs drift is random rather than systematic, and is bounded by the plant-specific setpoint analyses assumptions. This determination may use results of statistical analysis of operating data and calibration data from similar plants using the same model of RTD in the same environmental conditions.

The Surveillance Frequency is based on the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

The Surveillance is modified by a Note to indicate that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices, with minimal drift, and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3).

SR 3.3.1.10

This SR ensures that the RPS RESPONSE TIMES are verified to be less than or equal to the maximum values assumed in the safety analysis. Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor, to the point at which the RTCBs open. Response Times are conducted on an 18-month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n x 18 months, where n is the number of channels in the function. The 18-month Frequency is based upon operating experience, which has shown that random failures of instrumentation components causing serious response-time degradation, but not channel failure, are infrequent occurrences. Also, response times cannot be determined at power, since equipment operation is required. Testing may

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

be performed in one measurement or in overlapping segments, with verification that all components are tested.

A Note is added to indicate that the neutron detectors may be excluded from RPS RESPONSE TIME testing because they are passive devices, with minimal drift, and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3).

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50 Appendix A, "General Design Criteria for Nuclear Power Plants."

2. [Unit Name], [NRC Safety Evaluation Report, (Date)].

3. Institute of Electrical and Electronic Engineers, IEEE-279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," April 5, 1972.

4. [Unit Name] FSAR, Chapter [14], "[Accident Analysis]."

5. Title 10, Code of Federal Regulations, Part 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."

6. [Unit Name], "[Plant Protection System Selection of Trip Setpoint Values.]"

7. [Unit Name] FSAR, Chapter [ ], "[Instrumentation and Control]."

8. CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protection System (RPS) Instrumentation (Digital)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core fuel design limits and the reactor coolant pressure boundary during (RCPB) anticipated operational occurrences (AOOs), and to assist the Engineered Safety Features (ESF) Systems in mitigating accidents.

The protection and monitoring systems have been designed to assure safe operation of the reactor. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the RPS, as well as LCOs on other reactor system parameters and equipment performance.

The LSSS, defined in this specification as the ALLOWABLE VALUE, in conjunction with the LCOs, establish the threshold for protective system action to prevent exceeding acceptable limits during design basis accidents (DBAs).

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limit is:

1. The departure from nucleate boiling ratio (DNBR) shall be maintained above the safety limit (SL) value, to prevent departure from nucleate boiling;

2. Fuel centerline melting shall not occur; and

3. The Reactor Coolant System (RCS) pressure SL of [2750] psia shall not be exceeded.

Maintaining the SLs within the above values assures that offsite dose will be within the 10 CFR 50 and 10 CFR 100 criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 limits.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Different accident categories are allowed a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered as having acceptable consequences for that event.

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels;
- Bistables;
- RPS logic; and
- Reactor trip circuit breakers (RTCBs).

The role of each of these modules in the RPS is discussed below.

<u>Measurement Channels</u>

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

The excore nuclear instrumentation, the core protection calculators (CPCs), and the control element assembly calculators (CEACs) are considered components in the measurement channels of the Linear Power Level--High, Log Power Level--High, DNBR--Low, and Local Power Density (LPD)--High trips.

Four identical measurement channels, designated channels A through D, with electrical and physical separation are provided for each parameter used in the generation of trip signals, with the exception of the control element assembly (CEA) position indication used in the CPCs. Each measurement channel provides input to one or more RPS bistables within the same RPS channel. In addition, some measurement channels are used as inputs to Engineered Safety Features Actuation System (ESFAS) bistables, and most provide indication in the control room.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Measurement channels used as an input to the RPS are not used for control functions.

When a channel monitoring a parameter exceeds a predetermined setpoint, indicating an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping bistables monitoring the same parameter in two or more channels will de-energize Matrix Logic, which in turn de-energizes the Initiation Logic. This causes all eight RTCBs to open, interrupting power to the CEAs, allowing them to fall into the core.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of 10 CFR 50, Appendix A, GDC 21 (Ref. 1). The fourth channel provides additional flexibility, by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing, while still maintaining a minimum two-out-of-three logic.

In order to take full advantage of the four channel design, adequate channel-to-channel independence must be demonstrated, approved by the NRC staff, and this approval documented by an NRC Safety Evaluation Report (SER). Adequate channel-to-channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants that have demonstrated adequate channel-to-channel independence, as documented by the NRC SER (Ref. 2) may operate in a two-out-of-three logic configuration, with one channel removed from service, for the time stated in Reference 2.

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of IEEE 279-1971 (Ref. 3).

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. Four separate CPCs perform the calculations independently, one for each of the four RPS channels. The CPCs provide outputs to drive display indications (DNBR margin, LPD margin, and calibrated neutron flux power levels) and provide low DNBR and high LPD pretrip and trip signals. The

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

CPC channel outputs for the DNBR-Low and LPD-High trips operate contacts in the Matrix Logic, in a manner identical to the other RPS trips.

Each CPC receives the following inputs:

- Hot leg and cold leg temperatures;
- Pressurizer pressure;
- Reactor coolant pump (RCP) speed;
- Excore neutron flux levels;
- Target CEA positions; and
- CEAC penalty factors.

Each CPC is programmed with "addressable constants." These are various alignment values, correction factors, etc., that are required for the CPC computations. They can be accessed for display or for the purpose of changing them as necessary.

The CPCs use this constant and variable information to perform a number of calculations. These include the calculation of CEA group and subgroup deviations (and the assignment of conservative penalty factors) correction and calculation of average axial power distribution (based on excore neutron flux levels and CEA positions) calculation of coolant flow (based on pump speed) and calculation of calibrated average power level (based on excore neutron flux levels and ΔT-power).

The DNBR calculation considers primary pressure, inlet temperature, coolant flow, average power, axial power distribution, radial peaking factors, and CEA deviation penalty factors from the CEACS, to calculate the state of the limiting (hot) coolant channel in the core. A DNBR--Low trip occurs when the calculated value reaches the minimum DNBR trip setpoint.

The LPD calculation considers axial power distribution, average power, and radial peaking factors (based upon target CEA position) and CEAC penalty factors to calculate the

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

current value of compensated peak power density. A LPD--High trip occurs when the calculated value reaches the trip setpoint. The four CPC channels provide input to the four DNBR--Low and four LPD--High RPS trip channels. They effectively act as the sensor (using many inputs) for these trips.

The CEACs perform the calculations required to determine the position of CEAs within their subgroups for the CPCs. Two independent CEACs compare the position of each CEA to its subgroup position. If a deviation is detected by either CEAC, an annunciator sounds and appropriate "penalty factors" are transmitted to all CPCs. These penalty factors conservatively adjust the effective operating margins to the DNBR--Low and LPD--High trips. Each CEAC also drives a single CRT, which is switchable between CEACs. The CRT displays individual CEA positions and current values of the penalty factors from the selected CEAC.

Each CEA has two separate reed switch assemblies mounted outside the RCPB. Each of the two CEACs receives CEA position input from one of the two reed switch position transmitters on each CEA, so that the position of all CEAs is independently monitored by both CEACs.

<u>Bistables</u>

Bistable trip units, mounted in the Plant Protective System (PPS) cabinet, receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Matrix Logic. They also provide local trip indication and remote annunciation.

There are four channels of bistable trip units, designated A through D, for each RPS function, one for each measurement channel. Bistable output relays de-energize when a trip occurs, in turn de-energizing bistable relays mounted in the PPS relay card racks.

The contacts from these bistable actuated relays are arranged into six coincidence matrices, comprising the Matrix Logic. If bistables monitoring the same parameter in at least two channels trip, the Matrix Logic will generate a reactor trip (two-out-of-four logic).

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Some of the RPS measurement channels provide contact outputs to the RPS, so the comparison of an analog input to a trip setpoint is not necessary. In these cases, there is no bistable card, and opening the contact input directly de-energizes the associated relays. These include the loss of load trip, and the CPC-generated DNB--Low and LPD--High trips.

The trip setpoints and ALLOWABLE VALUES used in the bistables are based on the analytical limits stated in Reference 4. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors, for those RPS channels which must function in harsh environments as defined by 10 CFR 50.49 (Ref. 5), ALLOWABLE VALUES specified in Table 3.3.1-1 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the plant protection selection of trip setpoint values (Ref. 6). The nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the ALLOWABLE VALUE, to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the ALLOWABLE VALUE, the bistable is considered OPERABLE.

Setpoints in accordance with the ALLOWABLE VALUE will assure that SLs of Specification 2.0 are not violated during AOOs, and the consequences of DBAs will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA, and the equipment functions as designed.

Note that in LCO 3.3.1, the ALLOWABLE VALUES of Table 3.3.1-1 are the LSSS. These ALLOWABLE VALUES are established to prevent violation of the SLs during normal plant operation and AOOs.

Each channel of the process control equipment can be tested on line to verify that the signal or setpoint accuracy is within the specified allowance requirements of Reference 7.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated.

The ALLOWABLE VALUES listed in Table 3.3.1-1 are based upon the methodology described in Reference 6, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

RPS Logic

The RPS logic, consisting of Matrix Logic and Initiation Logic, employs a scheme that provides a reactor trip when bistables in any two of the four channels sensing the same input parameter trip. This is called a two-out-of-four trip logic. This logic and the RTCB configuration are shown in Figure B 3.3.1-1.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each Logic Matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices, to reflect the bistable channels being monitored. Each Logic Matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same function in the two channels being monitored by a Logic Matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one of the four matrix relays in each matrix opening contacts in one of the four trip paths. Each trip path provides power to one of the four normally energized RTCB control relays (K1, K2, K3, K4). The trip paths thus each have six contacts in series, one from each matrix, and perform a logical "OR" function, opening the RTCBs if any one or more of the six logic matrices indicate a coincidence condition.

(continued)

(continued)

BASES (continued)

Figure B 3.3.1-1
Simplified Functional Diagram of RPS Trip Logic

(continued)

BASES (continued)

BACKGROUND (continued)

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized, interrupt power to the breaker undervoltage trip attachments and simultaneously apply power to the shunt trip attachments on each of the two breakers. Actuation of either the undervoltage or shunt trip attachment is sufficient to open the reactor trip breaker and interrupt power from the motor-generator (MG) sets to the control element drive mechanisms (CEDM).

When a coincidence occurs in two RPS channels, all four matrix relays in the affected matrix de-energize. This in turn de-energizes all four breaker control relays, which simultaneously de-energize the undervoltage and energize the shunt trip attachments in all eight RTCBs, tripping them open.

Matrix Logic refers to the matrix power supplies, bistable relay contacts, and interconnecting wiring up to, but not including the matrix relays.

The Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring and solid-state (auxiliary) relays through the K-relay contacts in the RTCB control circuitry.

It is possible to change the two-out-of-four RPS logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but a reactor trip will not occur unless two additional channels indicate a trip condition. Trip channel bypassing can be simultaneously performed to any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

For those plants that have demonstrated sufficient channel-to-channel independence, two-out-of-three logic is the

(continued)

(continued)

BACKGROUND (continued)

minimum that is required to provide adequate plant protection, since a failure of one channel still ensures a reactor trip would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent trips caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select RPS trips. These bypasses are enabled manually, in all four RPS channels, when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Operating bypasses normally are implemented in the bistable, so that normal trip indication is also disabled. Trips with operating bypasses include Pressurizer Pressure--Low, Logarithmic Power Level--High, Reactor Coolant Flow--Low, Steam Generator (SG) Level--High or Low, and CPC (DNBR--Low and LPD--High).

The loss of load trip operating bypass is automatically enabled and disabled.

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear, shown in Figure B 3.3.1-2, consists of eight RTCBs which are operated in four sets of two breakers (four channels). Power input to the reactor trip switchgear comes from two full capacity MG sets operated in parallel such that the loss of either MG set does not de-energize the CEDMs. There are two separate CEDM power supply buses, each bus powering half of the CEDMs. Power is supplied from the MG sets to each bus via two redundant paths (trip legs). Trip legs 1A and 1B supply power to CEDM bus number 1. Trip legs 2A and 2B supply power to CEDM bus number 2. This ensures that a fault or the opening of a breaker in one trip leg (i.e. for testing purposes) will not interrupt power to the CEDM buses.

Each of the four trip legs consists of two RTCBs in series. The two RTCBs within a trip leg are actuated by separate initiation circuits.

The eight RTCBs are operated as four sets of two breakers (four channels). For example, if a breaker receives an open

(continued)

(continued)

BASES (continued)

Figure B 3.3.1-2
Simplified Functional Diagram of the RPS Trip Switchgear

(continued)

BASES (continued)

BACKGROUND (continued)

signal in trip leg A (for CEDM bus number 1), an identical breaker in trip leg B (for CEDM bus number 2) will also receive an open signal. This arrangement ensures that power is interrupted to both CEDM buses, thus preventing the tripping of only one half of the CEAs (a half trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

Each set of RTCBs is operated by either a manual reactor trip push button or an RPS-actuated K-relay. There are four manual reactor trip push buttons, arranged in two sets of two, as shown in Figure B 3.3.1-2. Depressing both push buttons in either set will result in a reactor trip.

When a manual reactor trip is initiated using the control room push buttons, the RPS trip paths and K-relays are bypassed, and the RTCB undervoltage and shunt trip attachments are actuated independent of the RPS.

Manual reactor trip circuitry thus includes the push button and interconnecting wiring to both RTCBs necessary to actuate both the undervoltage and shunt trip attachments, but excludes the K-relay contacts and their interconnecting wiring to the RTCBs, which are considered part of the initiation logic.

Functional testing of the entire RPS, from bistable input through the opening of individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. Nuclear instrumentation, the CPCs, and the CEACs can be similarly tested. Process transmitter calibration is normally performed on a refueling basis.

APPLICABLE SAFETY ANALYSES

The RPS functions to maintain the SLs during all AOOs and mitigates the consequences of DBAs in all MODES in which the RTCBs are closed.

Each of the analyzed accidents and transients can be detected by one of more RPS functions. The accident analysis contained in Reference 4 takes credit for most RPS trip functions. Functions not specifically credited in the accident analysis were qualitatively credited in the safety

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

analysis and the NRC staff-approved licensing basis for the plant. These functions may provide protection for conditions which do not require dynamic transient analysis to demonstrate function performance. These functions may also serve as backups to functions that were credited in the safety analysis.

The specific safety analyses applicable to each protective function are identified below:

1. Linear Power Level--High:

The portions of the RPS instrumentation that develop signals and trips for linear power level provide plant protection during certain AOOs, and assist the ESFs in the mitigation of certain accidents.

The Linear Power Level--High trip provides protection against core damage during the following events:

- uncontrolled CEA withdrawal from low power (AOO),
- uncontrolled CEA withdrawal at power (AOO), and
- CEA ejection (accident).

The Linear Power Level--High trip ensures that low DNBR, high LPD, and the RCS pressure SLs are maintained during normal operation and AOOs and, in conjunction with the ESFAS, the consequences of the CEA ejection accident will be acceptable.

2. Logarithmic Power Level--High:

The Logarithmic Power Level--High trip protects the integrity of the fuel cladding and helps protect the RCPB in the event of an unplanned criticality from a shutdown condition.

In MODES 2, 3, 4, and 5 with the RTCBs closed and the CEA Drive System capable of CEA withdrawal, protection is required for CEA withdrawal events originating when THERMAL POWER is < 1E-4% RATED THERMAL POWER (RTP). For events originating above this power level, other RPS trips provide adequate protection.

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

In MODES 3, 4, and 5 with the RTCBs open, or the CEAs not capable of withdrawal, the Log Power Level--High trip does not have to be OPERABLE. However, the indication and alarm portion of two log power level channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. The indication and alarm functions are addressed in LCO 3.3.7.

3. Pressurizer Pressure--High:

The Pressurizer Pressure--High trip provides protection for the high RCS pressure SL. In conjunction with the pressurizer safety valves and the main steam safety valves, it provides protection against overpressurization of the RCS pressure boundary during the following events:

- Loss of electrical load without a reactor trip being generated by the turbine trip (AOO),
- Loss of condenser vacuum (AOO),
- CEA withdrawal from low power conditions (AOO),
- Chemical and Volume Control System malfunction (AOO), and
- Main Feedwater System pipe break (accident).

The Pressurizer Pressure--High trip assures that the RCPB SL will not be exceeded during AOOs, and, in conjunction with the ESFAS, the consequences of accidents will be acceptable.

4. Pressurizer Pressure--Low:

The Pressurizer Pressure--Low trip is provided to trip the reactor to assist the ESF systems in the event of loss-of-coolant accidents (LOCAs). During a LOCA, the SLs are challenged, however, the consequences of the accident will be acceptable. A safety injection actuation signal (SIAS) and containment isolation actuation signal (CIAS) are initiated simultaneously.

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

5. Containment Pressure--High:

The Containment Pressure--High trip prevents exceeding the containment design pressure during a design basis LOCA or main steam line break (MSLB) accident. During a LOCA, the SLs are challenged; however, the consequences of the accident will be acceptable. An SIAS and CIAS are initiated simultaneously.

6. Steam Generator Pressure--Low:

The SG Pressure--Low trip provides protection against an excessive rate of heat extraction from the SGs which would result in a rapid, uncontrolled cooldown of the RCS. This trip is needed to shut down the reactor and assist the ESF systems in the event of an MSLB, or main feedwater line break (MFLB) accidents. A main steam isolation signal (MSIS) is initiated simultaneously.

7. Steam Generator Level--Low:

The SG Water Level--Low trip ensures that a reactor trip signal is generated for the following events to help prevent exceeding the design pressure of the RCS due to the loss of the heat sink:

- inadvertent opening of an SG atmospheric dump valve (AOO),
- loss of normal feedwater event (AOO), and
- feedwater system pipe break (accident).

The SG Water Level--Low function ensures that low DNBR, high LPD, and the RCS pressure SLs are maintained during normal operation and AOOs and, in conjunction with the ESF systems, the consequences of the feedwater line break accident will be acceptable.

8. Steam Generator Water Level--High:

The SG Level--High trip is provided to protect the turbine from excessive moisture carryover in case of an SG overfill event.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

9. Reactor Coolant Flow--Low:

The Reactor Coolant Flow--Low trip provides protection against an RCP sheared shaft event. The DNBR limit is expected to be exceeded during this event; however, the trip ensures the consequences are acceptable.

10. Loss of Load:

The loss of load (turbine stop valve (TSV) control oil pressure) trip is anticipatory for the loss of heat removal capabilities of the secondary system following a turbine trip. The loss of load trip prevents lifting the pressurizer safety valves and the main steam line safety valves in the event of a turbine generator trip. Thus, the trip minimizes the pressure or temperature transient on the reactor by initiating a trip well before the Pressurizer Pressure--High and safety valve setpoints are reached.

The four RPS loss of load reactor trip channels receive their input from sensors mounted on high pressure TSV actuators. Since there TCV are four high pressure TSV, one actuator per valve, and one sensor per actuator, each sensor sends its signal to a different RPS channel. When the turbine trips, control oil is dumped from the high pressure turbine stop valves. When the control oil pressure drops to the appropriate setpoint, a reactor trip signal is generated.

11. Core Protection Calculators:

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. The DNBR--Low and the LPD--High trips provide plant protection during the following AOOs and assist the ESF systems in the mitigation of the following accidents:

a. Local Power Density--High:

The LPD--High trip provides protection against fuel centerline melting due to the occurrence of excessive LPD peaks during the following AOOs:

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

- decrease in feedwater temperature,
- increase in feedwater flow,
- increased main steam flow (not due to steam line rupture) without turbine trip,
- uncontrolled CEA withdrawal from low power,
- uncontrolled CEA withdrawal at power, and
- CEA misoperation resulting in a single part-length CEA drop.

For the events listed above (except CEA misoperation, resulting in a single part-length CEA drop), DNBR—Low will trip the reactor first since DNB would occur before fuel centerline melting would occur.

b. <u>Departure from Nucleate Boiling Ratio--Low</u>:

The DNBR—Low trip provides protection against core damage due to the occurrence of locally saturated conditions in the limiting (hot) channel during the following events and is the primary reactor trip (trips the reactor first) for these events:

- decrease in feedwater temperature,
- increase in feedwater flow,
- increased main steam flow (not due to steam line rupture) without turbine trip,
- increased main steam flow (not due to steam line rupture) with a concurrent single failure of an active component,
- steam line break with concurrent loss of offsite AC power,
- loss of normal AC power,
- partial loss of forced reactor coolant flow,

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

- total loss of forced reactor coolant flow,
- single RCP shaft seizure,
- uncontrolled CEA withdrawal from low power,
- uncontrolled CEA withdrawal at power,
- CEA misoperation resulting in a full-length CEA drop,
- CEA misoperation resulting in a part-length CEA subgroup drop,
- primary sample or instrument line break, and
- SG tube rupture.

In the above list, only the SG tube rupture, the RCP shaft seizure, and the sample or instrument line break are accidents. The rest are AOOs.

12. Control Element Assembly Calculators:

These calculators provide inputs to the DNBR--Low and LPD--High trips, and are, therefore, required to be OPERABLE in the same MODES on the basis provided for those trip functions.

The effect of any misoperated CEA within a subgroup on the core power distribution is assessed by the CEACs, and an appropriately augmented power distribution penalty factor will be supplied as input to the CPCs. As the reactor core responds to the reactivity changes caused by the misoperated CEA and the ensuing reactor coolant and doppler feedback effects, the CPCs will initiate a DNBR--Low or LPD--High trip signal, if fuel design limits are approached. Each CPC also directly monitors one "target CEA" from each subgroup, and uses this information to account for excessive radial peaking factors, events involving CEA groups out of sequence, and subgroup deviations within a group, without the need for CEACs.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

13. Reactor Protection System Logic:

The RPS logic provides for automatic trip initiation to maintain the DNBR, LPD, and RCS pressure SLs during AOOs and assist the ESF systems in assuring acceptable consequences during accidents. All transients and accidents that call for a reactor trip assume the RPS logic is functioning as designed.

14. Reactor Trip Circuit Breakers:

All of the transient and accident analyses which call for a reactor trip assume that the RTCBs operate and interrupt power to the CEDMs.

15. Manual Reactor Trip:

The manual reactor trip is part of the RPS circuitry. It is used by the operator to shut down the reactor whenever any parameter is rapidly trending toward its trip setpoint. A manual reactor trip accomplishes the same results as any of the automatic trip functions.

16. Interlocks/Bypasses:

The operational bypasses are not explicitly modeled in the safety analysis. The automatic bypass removal features must function as a backup to manual actions for all safety-related trips to assure the trip functions are not operationally bypassed when the safety analysis assumes the functions are not bypassed. The bases for each of these bypasses is discussed under individual trips in the LCO section.

a. loss of load,

b. Logarithmic Power Level--High,

c. Reactor Coolant Flow--Low,

d. CPC (DNBR--Low and LPD--High),

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

e. SG Level (High and Low), and

f. Pressurizer Pressure--Low.

The RPS instrumentation satisfies Criterion 3 of the NRC Interim Policy Statement.

LCO

The LCO requires all instrumentation performing an RPS function to be OPERABLE. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected functions. The specific criteria for determining channel OPERABILITY differ slightly between functions. These criteria are discussed on a function-by-function basis below.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same function bypassed. For those designs approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time, the plant may operate for the time stated in Reference 2, with one channel in each function trip channel bypassed, effectively placing the plant in a two-out-of-three logic configuration in those functions. In other cases, plants are restricted to 48 hours in a trip channel bypass condition before either restoring the function to four channel operation (two-out-of-four logic), or placing the channel in trip (one-out-of-three logic).

Only the ALLOWABLE VALUES are specified for each RPS trip function in the LCO. Nominal trip setpoints are specified in the plant-specific setpoint calculations. The nominal setpoints are selected to ensure the setpoint measured by CHANNEL FUNCTIONAL TESTS does not exceed the ALLOWABLE VALUE if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its ALLOWABLE VALUE, is acceptable provided that operation and testing is consistent with the assumptions of the plant-specific setpoint calculations. Each ALLOWABLE VALUE specified is more conservative than the analytical limit assumed in the safety analysis in order to

(continued)

(continued)

BASES (continued)

LCO (continued)

account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the PPS selection of trip setpoint values (Ref. 6).

The trip functions specified in Table 3.3.1-1 are considered OPERABLE when:

1. All channel components necessary to provide a reactor trip signal are functional and in service;

2. Channel measurement uncertainties are known via test, analysis, or design information to be within the assumptions of the setpoint calculations;

3. Required Surveillance testing is current and has demonstrated performance within each Surveillance test's acceptance criteria; and

4. The associated operational bypass is not enabled except under the Conditions specified by the LCO's Applicability for the function.

The following bases for each trip function identify the above RPS trip function criteria items which are applicable to establish the trip function OPERABILITY requirements.

Bases for the individual function requirements are as follows:

1. <u>Linear Power Level--High</u>

This LCO requires all four channels of the Linear Power Level--High to be OPERABLE in MODE 1 or 2.

Linear Power Level--High trip channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is high enough to provide an operating envelope that prevents unnecessary Linear Power Level--High reactor trips during normal plant operations. The ALLOWABLE VALUE is low enough for the system to maintain a margin to unacceptable fuel cladding damage should a CEA ejection accident occur.

(continued)

(continued)

BASES (continued)

LCO (continued)

2. Logarithmic Power Level--High

This LCO requires four channels of the Logarithmic Power Level--High to be OPERABLE in MODE 2, and in MODE 3, 4, or 5 when the RTCBs are shut and the CEA Drive System is capable of CEA withdrawal.

Logarithmic Power Level--High trip channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE is hign enough to provide an operating envelope that prevents unnecessary Logarithmic Power Level--High reactor trips during normal plant operations. The ALLOWABLE VALUE is low enough for the system to maintain a margin to unacceptable fuel cladding damage should a CEA withdrawal event occur.

The Logarithmic Power Level--High trip may be bypassed when THERMAL POWER is above 1E-4% RTP to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when THERMAL POWER decreases below 1E-4% RTP. Above 1E-4% RTP, the Linear Power Level--High trip provides adequate protection for reactivity transients.

The trip may also be manually bypassed during physics testing pursuant to LCO 3.4.17, "Reactor Coolant System (RCS) Loops—Test Exceptions." [At this facility, the reasons for this bypass and the basis for allowing bypass are as follows:]

3. Pressurizer Pressure--High

This LCO requires four channels of Pressurizer Pressure-High to be OPERABLE in MODE 1 or 2.

Pressurizer Pressure--High trip channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is set below the nominal lift setting of the pressurizer code safety valves and its operation avoids the undesirable operation of these

(continued)

(continued)

BASES (continued)

LCO (continued)

valves during normal plant operation. In the event of a complete loss of electrical load from 100% power, this function ensures the reactor trip will take place, thereby limiting further heat input to the RCS and consequent pressure rise. The pressurizer safety valves lift to prevent overpressurization of the RCS.

4. Pressurizer Pressure--Low

This LCO requires four channels of Pressurizer Pressure--Low to be OPERABLE in MODE 1 or 2.

Pressurize Pressure--Low trip channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE is set low enough to prevent a reactor trip during normal plant operation and pressurizer pressure transients. However, the setpoint is high enough that with a LOCA, the reactor trip will occur soon enough to allow the ESF systems to perform as expected in the analyses and mitigate the consequences of the accident.

The trip setpoint may be manually decreased to a minimum value of 300 psia as pressurizer pressure is reduced during controlled plant shutdowns, provided the margin between the pressurizer pressure and the setpoint is maintained less than or equal to 400 psi. This allows for controlled depressurization of the RCS while still maintaining an active trip setpoint until the time is reached when the trip is no longer needed to protect the plant. Since the same Pressurizer Pressure-Low bistable is also shared with the SIAS, an inadvertent SIAS actuation is also prevented. The setpoint increases automatically as pressurizer pressure increases until the trip setpoint is reached.

The Pressurizer Pressure--Low trip and the SIAS function may be simultaneously bypassed when RCS pressure is below 400 psia, when neither the reactor trip nor an inadvertent SIAS actuation are desirable, and these functions are no longer needed to protect the plant. The bypass is automatically removed as RCS

(continued)

(continued)

BASES (continued)

LCO (continued)

pressure increases above 500 psia. The difference between the bypass enable and removal features allows for bypass permissive bistable hysteresis, and allows setting the bypass setpoint close enough to the limit so as to avoid inadvertent actuation at the 300 psia trip setpoint minimum value.

5. <u>Containment Pressure--High</u>

This LCO requires four channels of Containment Pressure--High to be OPERABLE in MODE 1 or 2.

Containment Pressure--High trip channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and not indicative of an off-normal condition. It is set low enough to initiate a reactor trip when an off-normal condition is indicated.

6. <u>Steam Generator Pressure--Low</u>

This LCO requires four channels for each SG of SG Pressure--Low to be OPERABLE in MODE 1 or 2.

SG Pressure--Low channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

The ALLOWABLE VALUE is sufficiently below the full load operating value for steam pressure so as not to interfere with normal plant operation, but still high enough to provide the required protection in the event of excessive steam demand. Since excessive steam demand causes the RCS to cool down resulting in positive reactivity addition to the core, a reactor trip is required to offset that effect.

The trip setpoint may be manually decreased as SG pressure is reduced during controlled plant cooldown, provided the margin between SG pressure and the setpoint is maintained less than 200 psi. This allows

(continued)

(continued)

BASES (continued)

LCO (continued)

for controlled depressurization of the secondary system while still maintaining an active reactor trip setpoint and MSIS setpoint until the setpoints are no longer needed to protect the plant. The setpoint increases automatically as SG pressure increases until the specified trip setpoint is reached.

7. <u>Steam Generator Water Level--Low</u>

This LCO requires four channels of SG Water Level--Low for each SG to be OPERABLE in MODE 1 or 2.

SG Water Level--Low channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE is sufficiently below the normal operating level for the SGs so as not to cause a reactor trip during normal plant operations. The same bistable providing the reactor trip also initiates emergency feedwater to the affected generator, via the emergency feedwater actuation signal (EFAS). The minimum setpoint is governed by EFAS requirements. The reactor trip will remove the heat source (except decay heat) thereby conserving the reactor heat sink.

This trip and the SG Water Level--High trip may be manually bypassed simultaneously when cold leg temperature is below the specified limit to allow for CEA withdrawal during testing. The bypass is automatically removed when cold leg temperature reaches 200°F. [For this facility, the basis for allowing bypass below 200°F is as follows:]

8. <u>Steam Generator Water Level--High</u>

This LCO requires four channels for each SG of SG Water Level--High to be OPERABLE in MODE 1 or 2.

SG Water Level--High channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE is high enough to allow for normal plant operation and transients without causing a reactor trip. It is set low enough to ensure a

(continued)

(continued)

LCO (continued)

reactor trip occurs before the water level reaches the steam dryers. Having SG water level at the trip value is indicative of the plant not being operated in a controlled manner.

This trip and the SG Water Level--Low trip may be manually bypassed simultaneously when cold leg temperature is below the specified limit to allow for CEA withdrawal during testing with the SGs in wet layup. The bypass is automatically removed when cold leg temperature reaches 200°F. [For this facility, the basis for allowing bypass below 200°F is as follows:]

9. Reactor Coolant Flow--Low

This LCO requires four channels of Reactor Coolant Flow--Low to be OPERABLE in MODES 1 and 2.

Reactor Coolant Flow--Low channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The ALLOWABLE VALUE is set low enough to allow for the slight variations in reactor coolant flow during normal plant operations, while providing the required protection. Tripping the reactor ensures that the resultant power-to-flow ratio provides adequate core cooling under the expected pressure conditions for this event.

The Reactor Coolant Flow--Low trip may be manually bypassed when reactor power is less than 1E-4% RTP. This allows for the de-energization of one or more reactor coolant pumps (RCPs) (e.g., for plant cooldown), while maintaining the ability to keep the shutdown CEA banks withdrawn from the core if desired.

LCO 3.4.5, "Reactor Coolant System (RCS) Loops—MODE 3," LCO 3.4.6, "Reactor Coolant System (RCS) Loops—MODE 4," and LCO 3.4.7, "Reactor Coolant System (RCS) Loops—MODE 5, Loops Filled" ensure adequate RCS flow rate is maintained. The bypass is automatically removed when THERMAL POWER increases above 1E-4% RTP,

(continued)

(continued)

BASES (continued)

LCO (continued)

as sensed by the wide range (logarithmic) nuclear instrumentation. [For this facility, the basis for allowing bypass when THERMAL POWER is below 1E-4% RTP is as follows:]

10. Loss of Load

This LCO requires four channels of the Loss of Load trip to be OPERABLE in MODE 1.

Loss of load channels are OPERABLE when OPERABILITY requirements 1, 2, 3, and 4 are satisfied.

The Steam Bypass Control System (SBCS) is capable of passing [45%] of the full power main steam flow ([45%] RTP bypass capability) directly to the condenser without causing the main steam safety valves to lift. The Nuclear Steam Supply System (NSSS) is capable of absorbing a 10% step change in power when a primary to secondary system energy mismatch occurs, without causing the pressurizer safety valves to lift. This means that the plant can sustain a turbine trip without causing the pressurizer safety valves or the main steam safety valves to lift, provided power is ≤ [55]% RTP. Therefore, the loss of load trip may be bypassed when reactor power is ≤ [55]% RTP, as sensed by the power range nuclear instrumentation. When above 55% RTP both the bypass enable and bypass removal are automatically performed.

11. Core Protection Calculators

a. Local Power Density--High, and

b. Departure from Nucleate Boiling Ratio--Low.

This LCO requires four channels for each function to be OPERABLE in MODE 1 or 2.

The LCO on the CPCs ensures that the SLs are maintained during all AOOs, and the consequences of accidents are acceptable.

(continued)

(continued)

BASES (continued)

LCO (continued)

CPCs are OPERABLE when the following OPERABILITY\ requirements are satisfied:

- the CPC hardware is functional and in service,
- an approved version of CPC software is installed and running,
- addressable constants are installed and are equal to or more conservative than the values specified in Reference [ ],
- required Surveillance testing is current and has demonstrated performance within each Surveillance test's acceptance criteria, and
- the associated operational bypass is not enabled except under the conditions specified by the LCO Applicability for the function.

LPD and DNBR input channels are OPERABLE when OPERABILITY requirements 1, 2, and 3 are satisfied.

A CPC is not considered inoperable if CEAC, LPD, or DNBR inputs are inoperable. The actions required in the event of CEAC, LPD, and DNBR input channel failures ensure the CPCs remain capable of performing their safety function.

The CPC channels may be manually bypassed below 1E-4% RTP, as sensed by the wide range (logarithmic) nuclear instrumentation. This bypass is manually instated in all four CPC channels, when plant conditions do not warrant the trip protection. The bypass effectively removes the DNBR—Low and LPD—High trips from the RPS logic circuitry. The operating bypass is automatically removed when enabling bypass conditions are no longer satisfied.

This operating bypass is required to perform a plant startup, since both CPC-generated trips will be in effect whenever shutdown CEAs are inserted. It also allows system tests at low power when pressurizer

(continued)

(continued)

BASES (continued)

LCO (continued)

pressure may be low, or RCPs may be off. [At this facility, the basis for allowing bypass below 1E-4% RTP is as follows:]

During special testing pursuant to LCO 3.4.17, "RCS Loops—Test Exceptions" the CPC channels may be manually bypassed when THERMAL POWER is below 5% RTP. [At this facility, the reasons for this bypass and the basis for allowing the bypass are as follows:]

The CPCs have no setpoints but provide inputs to the DNBR--Low and LPD--High trips. [For this facility, the basis for the DNBR--Low and LPD--High trip ALLOWABLE VALUES for the CPCs are as follows:]

12. Control Element Assembly Calculators

This LCO requires two channels associated with the CEACs to be OPERABLE when in MODE 1 or 2.

The LCO on the CEACs ensures that the CPCs are either informed of individual CEA position within each subgroup, using one or both CEACs, or that appropriate conservatism is included in the CPC calculations to account for anticipated CEA deviations. Each CEAC provides an identical input into all four CPC channels. Each CPC uses the larger of the two CEAC transmitted CEA deviation penalty factors. Thus, only one OPERABLE CEAC is required to provide CEA deviation protection. This LCO requires both CEACs to be OPERABLE, so that no single CEAC failure can prevent a required reactor trip from occurring.

CEACs are OPERABLE when:

- the CEAC hardware is functional and in service,
- an approved version of CEAC software is installed and running,
- Required Surveillance testing is current and has demonstrated performance within each Surveillance test's acceptance criteria,

(continued)

(continued)

BASES (continued)

LCO (continued)

- all input bistable actuated relay channels are functional and in service,
- all reed switch positions are OPERABLE.

The CFACs have no setpoints but provide inputs to the DNBR--Low and LPD--High trips.

13. Reactor Protection System Logic

The LCO on the RPS logic channels ensures that each of the following requirements are met:

a. a reactor trip will be initiated when necessary,

b. the required protection system coincidence logic is maintained (minimum two-out-of-three, normal two-out-of-four), and

c. sufficient redundancy is maintained to permit a channel to be out of service for testing or maintenance.

RPS logic channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

Failures of individual bistable relays and their contacts are addressed in functions 1 through 11. This specification addresses failures of the matrix logic not addressed in the above, such as the failure of matrix relay power supplies, or the failure of the trip channel bypass contact in the bypass condition. Loss of a single vital bus will de-energize one of the two power supplies in each of three matrices. This will result in four RTCBs opening; however, the remaining four closed RTCBs will prevent a reactor trip. For the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure is to be treated as a single channel failure, providing the affected matrix relays de-energize as designed, opening the affected RTCBs.

(continued)

(continued)

BASES (continued)

LCO (continued)

Each of the four initiation logic channels opens one set of RTCBs if any of the six coincidence matrices de-energize their associated matrix relays. They thus perform a logical or function. Each initiation logic channel has its own power supply and is independent of the others. An initiation logic channel includes the matrix relay through to the K-relay contacts, which open the RTCB.

It is possible for two initiation logic channels affecting the same trip leg to de-energize if a matrix power supply or vital instrument bus fails. This will result in opening the two affected sets of RTCBs.

If one set of RTCBs has been opened in response to a single RTCB channel, initiation logic channel, or manual reactor trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance testing on the OPERABLE initiation logic, RTCB, and manual trip channels. In this case the redundant set of RTCBs will provide protection if a trip should be required. It is unlikely that a trip will be required during the Surveillance testing, coincident with a failure of the remaining series RTCB channel. If a single matrix power supply or vital bus failure has opened two sets of RTCBs, manual trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

13.a. Matrix Logic

This LCO requires six channels of Matrix Logic to be OPERABLE in MODE 1 or 2, and in MODE 3, 4, or 5, when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

Matrix Logic channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

13.b. Initiation Logic Channels

This LCO requires four channels of initiation logic to be OPERABLE in MODE 1 or 2, and in MODE 3, 4, or 5, when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

(continued)

(continued)

BASES (continued)

LCO (continued)

Initiation logic channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

14. Reactor Trip Circuit Breakers

The LCO requires four RTCB channels to be OPERABLE in MODE 1 or 2, and in MODE 3, 4, or 5 when the PTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

RTCB channels are OPERABLE when OPERABILITY requirements 1 or 3 are satisfied.

Each channel consisting of two breakers operated in a single set by the initiation logic or manual reactor trip circuitry. This ensures that power is interrupted at identical locations in the trip legs for both CEDM buses, thus preventing power removal to only one CEDM bus (a half trip).

Failure of a single breaker affects the entire channel, and both must be bypassed.

Without reliable RTCBs and associated support circuitry, a reactor trip cannot occur when either initiated automatically or manually.

Each channel of RTCBs starts at the contacts which are actuated by the K-relay and the contacts which are actuated by the manual reactor trip for each set of breakers. The K-relay actuated contacts and the upstream circuitry is considered to be RPS logic and falls under the requirements of function 13. Manual reactor trip contacts and upstream circuitry is considered to be manual reactor trip circuitry and falls under the requirements of function 15.

If one set of RTCBs has been opened in response to a single RTCB channel, initiation logic channel, or manual reactor trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance testing on the OPERABLE initiation logic, RTCB, and manual trip channels. In this case the redundant set of RTCBs will provide protection. If a

(continued)

(continued)

BASES (continued)

LCO (continued)

single matrix power supply or vital bus failure has opened two sets of RTCBs, manual trip and RTCB testing on the closed breakers cannot be performed without causing a trip.

15. Manual Reactor Trip

The LCO requires all four Manual Reactor Trip channels to be OPERABLE in MODE 1 or 2, and in MODE 3, 4, or 5, when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal.

Manual Reactor Trip channels are OPERABLE when OPERABILITY requirements 1 and 3 are satisfied.

Two independent sets of two adjacent push buttons are provided at separate locations. Each push button is considered a channel and operates two of the eight RTCBs. Depressing both push buttons in either set will cause an interruption of power to the CEDMs allowing the CEAs to fall into the core. This design ensures that no single failure in any push button circuit can neither cause nor prevent a reactor trip.

Manual reactor trip push buttons are also provided at the reactor trip switchgear (locally) in case the control room push buttons become inoperable, or the control room becomes uninhabitable. These are not part of the RPS and cannot be credited in fulfilling the LCO OPERABILITY requirements. Furthermore, LCO Actions need not to be entered due to failure of a local manual trip.

The affected set of RTCBs may be closed for up to 1 hour for Surveillance testing on the OPERABLE initiation logic, RTCB, and manual trip channels. In this case the redundant RTCB will provide protection.

16. Interlocks/Bypasses

The LCO on bypass permissive removal channels requires that the automatic bypass removal feature of all four operating bypass channels be OPERABLE for each RPS function with an operating bypass in the MODES addressed in the specific LCO for each function.

(continued)

(continued)

BASES (continued)

LCO (continued)

Therefore all four bypass removal channels must be OPERABLE to ensure that none of the four RPS channels are inadvertently bypassed.

Interlock channels are OPERABLE when the OPERABILITY requirements 1, 2, and 3 are satisfied.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. In the case of the Logarithmic Power Level—High trip (function b), the absence of a bypass will limit maximum power to below the trip setpoint.

The interlock function ALLOWABLE VALUES are based upon analysis of functional requirements for the bypassed functions. These are discussed above as part of the LCO discussion for the affected functions.

[For this facility, the following support systems are required to be OPERABLE to ensure RPS instrumentation OPERABILITY:]

[For this facility, those required support systems which, upon their failure, do not require declaring the RPS instrumentation inoperable and their justification are as follows:]

[For this facility, the supported systems impacted by the inoperability of the RPS instrumentation and the justification of whether or not each supported system is declared inoperable are as follows:] It should be noted that LCO 3.3.1 may need to be augmented with additional Conditions, if it is determined that the RPS provides support to other systems included in the STS.

APPLICABILITY

Most RPS trips are required to be OPERABLE in MODE 1 or 2 because the reactor is critical in these modes. The trips are designed to take the reactor subcritical, which maintains the SLs during AOOs and assists the ESFAS in providing acceptable consequences during accidents. Most trips are not required to be OPERABLE in MODES 3, 4, and 5.

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by assuring adequate SHUTDOWN MARGIN. Exceptions to this are:

1. Logarithmic Power Level--High (Function 2), RPS Logic (Function 13), RTCBs (Function 14), and Manual Reactor Trip (Function 15). These functions are also required to be OPERABLE in MODE 3, 4, or 5 with the RTCBs closed and the CEA Drive System capable of withdrawal. This is required to provide protection from boron dilution and CEA withdrawal events.

Several trips have operating bypasses, discussed in the preceding LCO section. The interlocks that allow these bypasses shall be OPERABLE whenever the RPS function they support is OPERABLE.

ACTIONS

A protection function channel is inoperable when it does not satisfy the OPERABILITY criteria for the functions channels. These criteria are outlined for each function, in the LCO section of the Bases. The most common causes of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis. Typically the drift is found to be small and results in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is less conservative than the ALLOWABLE VALUE in Table 3.3.1-1, the channel is declared inoperable immediately, and the appropriate Condition(s) from Table 3.3.1-1 must be entered immediately.

In the event a channel's trip setpoint is found non-conservative with respect to the ALLOWABLE VALUE, or the transmitter, instrument loop, signal processing electronics, or the bistable is found inoperable, then all affected functions provided by that channel must be declared inoperable and the unit must enter the Condition for the particular protection function affected.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

When the number of inoperable channels in a trip function exceeds those specified in one or other related Conditions associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered, if applicable in the current MODE of operation.

Condition A

Condition A is applicable to all RPS protection functions and addresses the situation where one or more channels for one or more functions are inoperable at the same time. The Required Action is to refer to Table 3.3.1-1 and immediately take the Required Actions for the protection functions affected.

Condition B

Condition B applies to the failure of a single channel in any of the following RPS functions: Linear Power Level--High; Logarithmic Power Level--High; Pressurizer Pressure--High; Pressurizer Pressure--Low; Containment Pressure--High; SG Pressure--Low; SG Water Level--Low; SG Water Level--High; Reactor Coolant Flow--Low; Loss of Load; and CPC; LPD--High and DNBR--Low. RPS coincidence logic is normally two-out-of-four.

Required Action B.1 is the preferred action as it restores full functional capability of the RPS.

If one RPS channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip within 1 hour (Required Action B.2.1).

The 1 hour allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensure that the risk involved in operating with the failed channel is acceptable.

For plants that have not demonstrated sufficient channel-to-channel independence, the failed channel is restored to OPERABLE status or is placed in trip within 48 hours

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

(Required Action B.2.2.1 or B.2.2.2). Required Action B.2.2.1 restores the full capability of the function. Required Action B.2.2.2 places the function into a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent a trip. The 48-hour Completion Time is based upon operating experience that has demonstrated that a random failure of a second channel occurring during the 48-hour period is a low probability event.

<u>Condition C</u>

Condition C applies to the failure of two channels in any of the following RPS functions: Linear Power Level--High; Logarithmic Power Level--High; Pressurizer Pressure--High; Pressurizer Pressure--Low; Containment Pressure--High; SG Pressure--Low; SG Water Level--Low; SG Water Level--High; Reactor Coolant Flow--Low; Loss of Load; and CPC, LPD--High; DNBR--Low.

Required Action C.1 is the preferred action as it improves the functional reliability of the RPS.

Required Action C.2.1 and Required Action C.2.2 provide for placing one inoperable channel in bypass, and the other channel in trip within 1-hour Completion Time. This time is sufficient to allow the operator to take all appropriate actions for the failed channels and still ensure the risk involved in operating with the failed channels is acceptable. With one channel of protective instrumentation bypassed the RPS function is in a two-out-of-three logic, but with another channel failed the RPS may be operating with a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

The bypassed channel should be restored to OPERABLE status within 48 hours, for reasons similar to those stated under Condition B. After one channel is restored to OPERABLE, the provisions of Condition B apply to the remaining inoperable channel. Therefore, the channel that is still inoperable

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

after completion of Required Action C.2.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.

Condition D

Condition D applies to one automatic bypass removal channel inoperable. If the bypass removal channel for any operating bypass cannot be restored to OPERABLE status, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise the affected RPS channel must be declared inoperable, as in Condition B, and the bypass either removed or the bypass removal channel repaired. The Bases for Required Actions and Completion Times are the same as discussed for Condition B.

Condition E

Condition E applies to two inoperable automatic bypass removal channels. If the bypass removal channels for two operating bypasses cannot be restored to OPERABLE status, the associated RPS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise the affected RPS channels must be declared inoperable, as in Condition C, and the bypass either removed, or the bypass removal channel repaired. Also, Required Action E.3.2 provides for the restoration of the affected bypassed automatic trip channel to OPERABLE status within the rules of Completion Time specified under Condition C. Completion Times are consistent with Condition C.

Condition F

Condition F is entered when the Required Actions and associated Completion Times of Condition B, C, D, or E are not met.

If the Required Actions associated with these Conditions cannot be completed within the required Completion Time, the reactor must be brought to a MODE where the Required Actions do not apply. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition G

Condition G applies to the failure of a single CEAC channel. There are only two CEACs, each providing CEA deviation input into all four CPC channels. With one failed CEAC, the CPC will receive CEA deviation penalty factors from the remaining (operable) CEAC. If the second CEAC should fail (Condition H), the CPC will use large preassigned penalty factors. The specific actions allowed are as follows:

Required Action G.1 is the preferred action as it restores the functional reliability of the RPS.

The allowed Completion Time of 4 hours takes into account the other redundant OPERABLE CEA and frequent verification (4 hours) of CEA derivatives.

With one CEAC inoperable, the second CEAC still provides a comprehensive set of comparison checks on individual CEAs within subgroups, as well as outputs to all CPCs, CEA deviation alarms, and position indications for display. Verification that each CEA is within 7 inches of other CEAs in its group once every 4 hours provides a check on the proper position of all CEAs and verifies operation of the remaining CEAC. An OPERABLE CEAC will not generate penalty factors until deviations greater than 7 inches are encountered.

The Completion Time of once per 4 hours is adequate, based on operating experience, considering the low probability of an undetected CEA deviation coincident with an undetected failure in the remaining CEAC channel within this limited time frame.

As long as Required Action G.2.1 is accomplished as specified, the inoperable CEAC can be restored to OPERABLE status within 7 days. [For this facility, the basis for the 7-day Completion Time is as follows:]

Condition H

Condition H applies if the Required Actions and associated Completion Times of Condition G are not met, or if both CEACs are inoperable. Actions associated with this

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition involve disabling the CEA Drive System, while providing increased assurance that CEA deviations are not occurring, and informing all OPERABLE CPC channels, via a software flag, that both CEACs are failed. This will assure that the large penalty factor associated with two CEAC failures will be applied to CPC calculations. The penalty factor for two failed CEACs is sufficiently large that power must be maintained significantly below 100% RTP if CPC generated reactor trips are to be avoided. The specific actions allowed are as follows:

[For this facility, the basis for the 4-hour Completion Time provided for all the Required Actions is as follows:]

H.1 is the preferred action as it improves the functional reliability of the RPS.

H.2.1

Meeting the DNBR margin requirements of LCO 3.2.5 ensures that power level and AXIAL SHAPE INDEX are within a conservative region of operation based on actual core conditions. [In addition, the Reactor Power Cutback (RPCB) System must be disabled. This ensures that CEA position will not be affected by RPCB operation.]

H.2.2

The "full out" CEA reed switches provide acceptable indication of CEA position. Therefore, the CEAs will remain fully withdrawn, except as required for specified testing [or flux control via CEA group number 6]. This verification ensures that undesired perturbations in local fuel burnup are prevented.

H.2.3

The "RSPT/CEAC Inoperable" addressable constant in each of the CPCs is set to indicate that both CEACs are inoperable. This provides a conservative penalty factor to ensure that a conservative effective margin is maintained by the CPCs in the computation of DNBR and LPD trips.

(continued)

(continued)

ACTIONS (continued)

H.2.4

The CEDM Control System is placed and maintained in "OFF" to prevent inadvertent motion and possible misalignment of the CEAs.

H.2.5

A comprehensive set of comparison checks on individual CEAs within groups must be made once every 4 hours. Verification that each CEA is within 7 inches of other CEAs in its group provides a check that no CEA has deviated from its proper position within the group.

Condition I

Condition I applies if an OPERABLE CPC or CEAC has three or more auto restarts in a 12-hour period.

CPCs and CEACs will attempt to auto restart if they detect a fault condition, such as a calculator malfunction or loss of power. A successful auto restart restores the calculator to operation; however, excessive auto restarts might be indicative of a calculator problem.

If a nonbypassed CEAC has three or more auto restarts, it may not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed on the CEAC to ensure it is functioning properly.

Based on plant operating experience, the 24 hours is adequate and reasonable to perform the test while still keeping the risk of operating in this condition at an acceptable level, since overt channel failure will most likely be indicated and annunciated in the control room by CPC on-line diagnostics.

Condition J

Condition J applies if any CPC cabinet receives a high temperature alarm. There is one temperature sensor in each of the four CPC bays. Since CPC bays B and C also house CEAC calculators 1 and 2 respectively, a high temperature in either of these bays may also indicate a problem with the associated CEAC.

(continued)

(continued)

ACTIONS (continued)

If a CPC cabinet high temperature alarm is received, it is possible for the CPC to be affected and not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed within 12 hours.

[For this facility, the basis for the 12-hour Completion Time is as follows:]

Condition K

Condition K applies to one Initiation Logic channel (Function 13.b), RTCB channel (Function 14), or Manual Reactor Trip channel (Function 15), in MODE 1 or 2, since they have the same actions. MODE 3, 4, or 5 with the RTCBs shut are addressed in Condition Q. These actions involve either repairing the channel or opening the affected RTCBs. The latter removes the need for the affected channel by performing its associated safety function. With an RTCB open. the affected functions are in one-out-of-two logic, which meets redundancy requirements, but testing on the OPERABLE channels cannot be performed without causing a reactor trip, unless the RTCBs in the inoperable channels are closed to permit testing. Therefore, the RTCBs associated with one inoperable channel may be closed for up to 1 hour for the performance of an RPS CHANNEL FUNCTIONAL TEST.

Required Action K.1 is the preferred action, as it restores the functional reliability of the RPS.

In MODE 1 or 2, Required Action K.2 provides for opening the RTCBs associated with the inoperable channel within 1 hour. This action is conservative since depressing the manual reactor trip push button associated with either set of breakers in the other trip leg will cause a reactor trip. With this configuration, a single channel failure will not prevent a reactor trip. The allotted Completion Time is adequate to open the affected RTCBs, while maintaining the risk of having them closed at an acceptable level.

Condition L

Condition L is entered when the Required Actions and associated Completion Times of Condition H, I, J, or K are not met.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

If Required Actions associated with these Conditions cannot be completed within the required Completion Time, the reactor must be brought to a MODE where the Required Actions do not apply. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

Condition M

Condition M applies if one Matrix Logic channel (Function 13.a) is inoperable in MODE 1 or 2. MODES 3, 4, and 5 with the RTCBs closed are addressed in Condition P. Loss of a single vital instrument bus will de-energize one of the two matrix power supplies in up to three matrices. This is considered a single matrix failure, providing the matrix relays associated with the failed power supplies de-energize as required. [For this facility, the consequences for the matrix relays not de-energizing as required are as follows:]

The channel must be restored to OPERABLE status within 48 hours. This provides the operator time to take the appropriate actions and still ensure that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second Matrix Logic channel is low during any given 48 hour interval. If the channel cannot be restored to OPERABLE status within 48 hours, Condition O is entered.

Condition N

Condition N applies to the failure of both Initiation Logic channels (Function 13.b) affecting the same trip leg. Since this will open two channels of RTCBs, this Condition is also applicable to the two affected RTCBs. This condition allows for loss of a single vital instrument bus or matrix power supply, which will de-energize both Initiation Logic channels in the same trip leg. This will open both sets of RTCBs in the affected trip leg, satisfying the Required Action of opening the affected RTCBs.

Of greater concern is the failure of the initiation circuit in a non-trip condition (e.g., due to two initiation relay

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

failures). With only one Initiation Logic channel failed in a non-trip condition, there is still the redundant set of RTCBs in the trip leg. With both failed in a non-trip condition, the reactor will not trip automatically when required. In either case, the affected RTCBs must be opened immediately by using the appropriate manual trip push buttons, since each of the four push buttons opens one set of RTCBs, independent of the initiation circuitry. Caution must be exercised, since depressing the wrong push buttons may result in a reactor trip.

If the affected RTCB(s) cannot be opened, Condition O is entered. This would only occur if there is a failure in the manual trip circuitry or the RTCB(s).

<u>Condition O</u>

Condition O is entered if Actions associated with Condition M or N are not met.

If the RTCBs associated with the inoperable channel cannot be opened, the reactor must be shut down within 6 hours and all the RTCBs opened. The Completion Time of 6 hours is reasonable, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

<u>Condition P</u>

Condition P applies to one Matrix Logic channel inoperable in MODE 3, 4, or 5. In these MODES the probability of most accidents or transients occurring (and their associated consequences) is significantly reduced. Therefore, there is no need to move to a different mode if one channel is inoperable. Opening the RTCBs will not cause a transient.

The channel must be restored to OPERABLE status within 48 hours. If the inoperable channel cannot be restored to OPERABLE status within 48 hours, all RTCBs must be opened, placing the plant in a MODE where the LCO does not apply, and ensuring no CEA withdrawal occurs.

[For this facility, the basis for the 48-hour Completion Time is as follows:]

(continued)

(continued)

ACTIONS (continued)

Condition Q

Condition Q applies to the failure of one Initiation Logic channel (function 13.b), RTCB channel (function 14), or manual reactor trip channel (function 15) in MODES 3, 4, or 5 with the RTCBs closed. The channel must be restored to OPERABLE status within 48 hours. If the inoperable channel cannot be restored to OPERABLE status within 48 hours, all RTCBs must be opened, placing the plant in a MODE where the LCO does not apply, and ensuring no CEA withdrawal occurs.

[For this facility, the basis for the 48-hour Completion Time is as follows:]

Condition R

Condition R applies to two Initiation Logics, RTCB channels, or Manual Reactor Trip channels affecting the same trip leg inoperable in MODE 3, 4, or 5, with the RTCBs closed. Condition R is similar to Condition N in that it allows for loss of a single vital instrument bus or matrix power supply, which will de-energize both initiation logic channels in the same trip leg. This will open both sets of RTCBs in the affected trip leg, satisfying the Required Action of opening the affected RTCBs.

In the event that two channels fail in a non-trip condition, the affected RTCBs must be opened immediately to restore reactor trip capability. In these MODES the probability of most accidents or transients occurring (and their associated consequences) is significantly reduced. Therefore, there is no need to move to a different MODE if one channel is inoperable. Opening the affected RTCBs restores automatic and manual reactor trip capability in one-out-of-two logic in the remaining trip leg.

Condition S

Condition S applies to the Logarithmic Power Level--High trip during operation in MODE 3, 4, or 5 with the RTCBs closed and the CEA Drive System capable of CEA withdrawal.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition S is identical to Condition B except that if the Required Actions or associated Completion Times of Condition S are not met, Condition U is entered. The Bases for the Required Actions and Completion Times are as discussed under Condition B.

Condition T

Condition T applies to the Logarithmic Power Level--High trip during operation in MODE 3, 4, or 5 with the RTCBs closed and the CEA Drive System capable of CEA withdrawal. Condition T is identical to Condition C except that if the Required Actions or associated Completion Times of Condition T are not met, Condition U is entered. The Bases for Required Actions and Completion Times are as discussed under Condition C.

Condition U

Condition U is entered when the Required Actions and associated Completion Times of Condition S or T are not met.

If the Required Actions of S or T cannot be completed within the required Completion Time, all RTCBs must be opened placing the plant in a condition where the log power trip channels are not required to be OPERABLE. One hour is a reasonable time to perform the Required Action, which maintains the risk at an acceptable level while having one or two channels inoperable.

Condition V

Condition V is applicable to each one of the RPS functions presented in Table 3.3.1-1.

Required Action V.1 verifies that all required support features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 must be immediately entered. However, if the support feature LCO or RPS LCO takes into consideration the loss of function situation, then LCO 3.0.3 may not need to be entered.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

The SRs for any particular RPS function are found in the SRs column of Table 3.3.1-1 for that function. Most functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, and CHANNEL CALIBRATION and response time testing.

In order for a facility to take credit for topical reports as the basis for justifying Surveillance Frequencies, topical reports must be supported by an NRC staff SER that establishes the acceptability of each topical report for that facility.

SR 3.3.1.1

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the indicated parameter for instrument channels of a similar parameter. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment have drifted outside their limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off-scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off-scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Surveillance Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

to 12 hours. Since the probability of two random failures in redundant channels in any 12-hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

In the case of RPS trips with multiple inputs, such as the DNBR and LPD inputs to CPC, a CHANNEL CHECK must be performed on all inputs.

SR 3.3.1.2

The RCS flow rate indicated by each CPC is verified to be less than or equal to the RCS total flow rate every 12 hours with THERMAL POWER greater than or equal to 70% RTP. The Surveillance compares CPC indicated flow. [For this facility, the flow measurement used for this comparison is as follows:] This check ensures that the DNBR setpoint is conservatively adjusted with respect to actual flow indications [as determined by the Core Operating Limits Supervisory System (COLSS)]. The Surveillance Frequency, about once every shift, is based on plant operating experience and is further justified by the fact that parameters are continuously monitored in the control room.

SR 3.3.1.3

The CPC and CEAC auto restart count is checked every 12 hours to monitor the CPC and CEAC for normal operation. If three or more auto restarts of a non-bypassed CPC or CEAC occurs within a 12-hour period, the CPC or CEAC may not be completely reliable. Therefore, the Required Action of Condition I must be performed. The Surveillance Frequency is based upon operating experience that demonstrates the rarity of more than one channel failing within the same 12-hour interval.

SR 3.3.1.4

A daily calibration (heat balance) is performed when THERMAL POWER is ≥ 15%. The linear power level signal and the CPC

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

addressable constant multipliers are adjusted to make the CPC ΔT power and nuclear power calculations agree with the calorimetric calculation if the [absolute] difference is ≥ [2]%. The value of [2]% is adequate because this value is assumed in the safety analysis. These checks are adequate to ensure that the accuracy of these CPC calculations is maintained within the analyzed error margins. The power level must be > 15% RTP to obtain accurate data. At lower power levels, the accuracy of calorimetric data is questionable.

The Frequency of 24 hours is based on plant operating experience and takes into account indications and alarms located in the control room to detect deviations in channel outputs. The Surveillance Frequency is modified by a Note indicating this test need only be performed when THERMAL POWER is > 15% RTP. The secondary calorimetric is inaccurate at lower power levels. Note 1 to the SR indicates the daily calibration may be suspended during PHYSICS TESTS. [At this facility the basis for this note is as follows:] Note 2 to the SR indicates SR 3.0.4 is not applicable. The Note exempting SR 3.0.4 is required, because power must be above 15% RTP before the Surveillance can be performed.

SR 3.3.1.5

The three vertically mounted excore nuclear instrumentation detectors in each channel are used to determine axial power distribution for use in the DNBR and LPD calculations. Because the detectors are mounted outside the reactor vessel, a portion of the signal from each detector is from core sections not adjacent to the detector. This is termed "shape annealing," and is compensated for after every refueling by performing SR 3.3.1.15, which adjusts the gains of the three detector amplifiers for shape annealing. SR 3.3.1.5 assures that the preassigned gains are still proper. Power must be above 15% because the CPCs do not use the excore generated signals for axial flux shape information at low power levels. The Note exempting SR 3.0.4 is required, because power must be above 15% RTP before the Surveillance can be performed. The 31-day

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

Frequency is adequate because operating experience which demonstrates long-term drift of the instrument channels is minimal and the fuel burnup is a slow and easily monitored parameter.

SR 3.3.1.6

The RCS flow rate indicated by each CPC is verified to be less than or equal to the RCS total flow rate every 31 days. This check ensures that the DNBR setpoint is conservatively adjusted with respect to actual flow indications as determined by a calorimetric calculation. Operating experience has shown the specified 31-day interval is adequate as instrument drift is minimal and changes in actual flow rate are minimal over core life.

SR 3.3.1.7

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 7. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

Bistable Tests. "As found" and "as left" values for bistable trip setpoints are recorded. The bistable setpoints must be found to trip within the ALLOWABLE VALUES specified in the LCO. The difference between the current "as found" and the previous test "as left" values must be consistent with the drift allowance used in the setpoint analysis. Wherever these tolerances are not met, a recalibration can be performed to establish OPERABILITY of the channel. However, repeated consecutive failures would be indicative of a failure that cannot be corrected by recalibration alone.

A test signal is then superimposed on the input in one channel at time to verify that the bistable trips within the specified tolerance around the setpoint.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

This is done with the affected RPS channel trip channel bypassed.

Matrix Logic Tests. This test is performed one matrix at a time. It verifies that coincidence in the two input channels for each function removes power to the matrix relays. During testing, power is applied to the matrix relay test coils and prevents the matrix relay contacts from assuming their energized state. This test will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

Trip Path Tests. These tests are similar to the matrix logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening the affected set of RTCBs. The RTCBs must then be closed prior to testing the other three initiation circuits, or a reactor trip may result.

The CPC and CEAC channels and excore nuclear instrumentation channels are tested separately.

The excore neutron detector channels use preassigned test signals to verify proper channel alignment. The excore logarithmic channel test signal is inserted into the preamplifier input, so as to test the first active element downstream of the detector. The power range excore test signal is inserted at the drawer input, since there is no preamplifier.

A quarterly CPC CHANNEL FUNCTIONAL TEST is performed using test software. This software includes preassigned addressable constant values which may differ from the current values. Provisions are made to store the addressable constant values onto a computer disk prior to testing and to reload them after testing. A Note is added to verify the CPC CHANNEL FUNCTIONAL TEST includes the correct value of addressable constants.

The Surveillance Frequency of 92 days is based upon the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.8

A CHANNEL CALIBRATION of the excore power range channels every 92 days ensures that the channels are reading accurately and within tolerance. A Note is added the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices, with minimal drift, and because of the difficulty of simulating a meaningful signal.

Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.4) and the monthly linear subchannel gain check (SR 3.3.1.5).

In addition, associated control room indications are continuously monitored by the operators.

The Surveillance Frequency of 92 days is based upon the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

SR 3.3.1.9

The characteristics and basis for this test are as described for SR 3.3.1.7. This test differs from SR 3.3.1.7 only in that the CHANNEL FUNCTIONAL TEST on the loss of load functional unit is only required above 55% RTP. When above 55%, and the trip is in effect, the CHANNEL FUNCTIONAL TEST ensures the channel will perform its equipment protective function if needed.

SR 3.3.1.10

SR 3.3.1.10 is the performance of a CHANNEL CALIBRATION every 18 months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to measured parameters with the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive tests, to ensure that the instrument channel remains operational with the setpoint with the assumptions of the plant-specific setpoint analysis. Transmitter "as found"

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

values and "as left" values are recorded and used to verify drift assumptions. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint analysis. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis.

Recalibration restores the OPERABILITY of an otherwise functional component found to have errors larger than assumed by the setpoint analysis. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure that cannot be corrected by recalibration.

Field transmitters may be calibrated in place, removed and calibrated in a laboratory, or replaced with an equivalent laboratory calibrated unit. Resistance temperature detector (RTD) channels may be calibrated in place using cross-calibration techniques, or in a test bath after removal from piping. For cross-calibration, at least one RTD should be replaced with a newly calibrated RTD during each refueling cycle to ensure accurate RTD cross-calibration. This replacement RTD must be the same model as the remaining RTDs. Using a newly calibrated RTD as a reference assures RTD signal drift continues to remain random rather than systematic and is within the limits specified in the plant setpoint analysis. The replacement interval may be extended to alternate refueling if it is demonstrated that over the extended interval, the RTD drift is random rather than systematic, and is bounded by the plant-specific setpoint analyses assumptions. This determination may use results of statistical analysis of operating data and calibration data from similar plants using the same model of RTD in the same environmental conditions.

The Surveillance Frequency is based upon the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

The SR is modified by a Note to indicate that the neutron detectors are excluded from CHANNEL CALIBRATION because they are passive devices, with minimal drift, and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.4) and the monthly linear subchannel gain check (SR 3.3.1.5).

SR 3.3.1.11

The isolation characteristics of each CEAC CEA position isolation amplifier and each optical isolator for CEAC to CPC data transfer is verified once per 18 months to ensure that a fault in a CEAC or a CPC channel will not render another CEAC or CPC channel inoperable. [For this facility, the test acceptance criteria is contained in the following reference or is as follows:] The CEAC CEA position isolation amplifiers, mounted in CPC cabinets A and D, prevent a CEAC fault from propagating back to CPC A or D. the optical isolators for CPC to CEAC data transfer prevent a fault originating in any CPC channel from propagating back to any CEAC through this data link.

[For this facility, the basis for the 18-month Frequency is as follows:]

SR 3.3.1.12

Each RTCB is actuated by an undervoltage coil and a shunt trip coil. The system is designed so that either de-energizing the undervoltage coil or energizing the shunt trip coil will cause the circuit breaker to open. When an RTCB is opened, either during an automatic reactor trip or by using the manual push buttons in the control room, the undervoltage coil is de-energized and the shunt trip coil is energized. This makes it impossible to determine if one of the coils or associated circuitry is defective.

Therefore, once per 18 months, a CHANNEL FUNCTIONAL TEST is performed which tests all four sets of undervoltage coils, and all four sets of shunt trip coils, individually. During undervoltage coil testing, the shunt trip coils shall remain de-energized, preventing their operation. Conversely, during shunt trip coil testing, the undervoltage coils shall

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

remain energized, preventing their operation. This test ensures that every undervoltage coil and every shunt trip coil is capable of performing its intended function, and that no single active failure of any RTCB component will prevent a reactor trip. The 18-month Frequency was developed considering it was prudent that these Surveillances only be performed during a plant outage. This was due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 18-month Frequency.

SR 3.3.1.13

Every 18 months, a CHANNEL FUNCTIONAL TEST is performed on the CPCs, CEACs, and manual reactor trip.

For the manual reactor trip circuitry, this test verifies that the trip push buttons are capable of opening the RTCBs as required. The 18-month Frequency was developed considering it was prudent that these Surveillances only be performed during a plant outage. This was due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 18-month Frequency.

The CHANNEL FUNCTIONAL TEST on the CPCs and CEACs shall include the injection of simulated process signals into the channel as close to the sensors as practicable to verify OPERABILITY including alarm and trip functions.

The basis for the 18-month Frequency for the CPCs and CEACs is because CPCs and CEACs perform a continuous self-monitoring function which eliminates the need for frequent CHANNEL FUNCTIONAL TESTS. This CHANNEL FUNCTIONAL TEST essentially validates the self-monitoring function and checks for a small set of failure modes that are undetectable by the self-monitoring function. Operating experience has shown that undetected CPC or CEAC failures usually do not occur in any given 18-month interval.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.14

SR 3.3.1.14 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.1.7, except SR 3.3.1.14 is only applicable to bypass functions. Proper operation of bypass permissives is critical during plant startup because the bypasses must be in place to allow startup operation and must be removed at the appropriate points during power ascent to enable certain reactor trips. Consequently, the appropriate time to verify bypass function operability is just before startup. The allowance to conduct this test within 92 days of startup is based upon the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8). Once the operating bypasses are removed, the bypasses must not fail in such a way that the associated trip function is inappropriately bypassed. This feature is verified by the trip function CHANNEL FUNCTIONAL TEST, SR 3.3.1.7 or SR 3.3.1.9. Therefore, further testing of the bypass function after startup is unnecessary.

SR 3.3.1.15

The three excore detectors used by each CPC channel for axial flux distribution information are far enough from the core to be exposed to flux from all heights in the core, although it is desired that they only read their particular level. The CPCs adjust for this flux overlap by using the predetermined shape annealing matrix elements in the CPC software. After refueling, it is necessary to re-establish the shape annealing matrix elements for the excore detectors based on more accurate incore detector readings. This is necessary because refueling could possibly produce a significant change in shape annealing matrix coefficients.

Incore detectors are inaccurate at low power levels. THERMAL POWER should be significant, but less than 70% to perform an accurate axial shape calculation used to derive the shape annealing matrix elements.

By restricting power to ≤ 70% until shape annealing matrix elements are verified, excessive local power peaks within the fuel are avoided.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.16

This SR ensures that the RPS RESPONSE TIME is verified to be less than or equal to the maximum values assumed in the safety analysis. Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor, to the point at which the RTCBs open. Response times are demonstrated on an 18-month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n times 18 months, where n is the number of channels in the function. The 18-month Frequency is based upon operating experience, which has shown that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Also, response times cannot be determined at power, since equipment operation is required. Testing may be performed in one measurement or in overlapping segments, with verification that all components are tested.

A Note is added to indicate that the neutron detectors may be excluded from RPS RESPONSE TIME testing because they are passive devices, with minimal drift, and because of the difficulty of simulating a meaningful signal. Slow changes in detector sensitivity are compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3).

(continued)

(continued)

BASES (continued)

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

2. [Unit Name] [NRC Staff Safety Evaluation Report, Date].

3. IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," April 5, 1972.

4. [Unit Name] Updated FSAR, Section [14], "[Accident Analysis]."

5. Title 10, Code of Federal Regulations, Part 50.49, "Environmental Qualifications of Electric Equipment Important to Safety for Nuclear Power Plants."

6. [Unit Name] "[Plant Protection, System Selection of Trip Setpoint Values]."

7. [Unit Name] Updated FSAR, Section [ ], "[Instrumentation and Control]."

8. CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," June 2, 1986 including Supplement 1, March 3, 1986.

B 3.3 INSTRUMENTATION

B 3.3.2 Engineered Safety Features Actuation System (ESFAS) Instrumentation (Analog)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits, Reactor Coolant System (RCS) pressure boundary, and to mitigate accidents.

The ESFAS contains devices and circuitry which generate the following signals when the monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS);
2. Containment Spray Actuation Signal (CSAS);
3. Containment Isolation Actuation Signal (CIAS);
4. Main Steam Isolation Signal (MSIS);
5. Recirculation Actuation Signal (RAS); and
6. Auxiliary Feedwater Actuation Signal (AFAS).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS Instrumentation Systems is segmented into three interconnected modules. These modules are:

- Measurement channels;
- Bistables; and
- ESFAS Logic.

The role of each of these modules in the ESFAS is discussed below.

(continued)

(continued)

BACKGROUND (continued)

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the generation of trip signals. These are designated Channels A through D. Measurement channels provide input to ESFAS bistables within the same ESFAS channel. In addition, some measurement channels may also be used as inputs to Reactor Protection System (RPS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS or ESFAS are not used for control functions.

When a channel monitoring a parameter indicates an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter will de-energize both channels of actuation logic of the associated Engineered Safety Features (ESF) equipment.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in Appendix A to 10 CFR 50 (Ref. 7). The fourth channel provides additional flexibility, by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing, while still maintaining a minimum two-out-of-three logic.

In order to take full advantage of the four channel design, adequate channel-to-channel independence must be demonstrated, approved by the NRC staff, and this approval documented by an NRC Safety Evaluation Report. Adequate channel-to-channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants that have demonstrated adequate channel-to-channel independence, as documented by the NRC Safety Evaluation Report (Ref. 3) may operate in a two-out-of-three logic configuration, with one

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

channel removed from service, for the time stated in Reference 3.

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of Institute of Electrical and Electronic Engineers (IEEE) 279-1971 (Ref. 4).

Bistables

Bistable trip units receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the matrix logic. They also provide local trip indication, and remote annunciation.

There are four channels of bistables, designated A through D, for each ESFAS function, one for each measurement channel. In cases where two ESF functions share the same input and trip setpoint (e.g. containment pressure input to CIAS and SIAS), the same bistable may be used to satisfy both functions. Similarly, bistables may be shared between the RPS and ESFAS (e.g. Pressurizer Pressure--Low input to the RPS and SIAS).

The trip setpoints and ALLOWABLE VALUES used in the bistables are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment effects, for those ESFAS channels which must function in harsh environments as defined by 10 CFR 50.49 (Ref. 2), ALLOWABLE VALUES specified in Table 3.3.2-1 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the plant protection selection of trip setpoint values (Ref. 6). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

ALLOWABLE VALUE to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. If the measured setpoint does not exceed the ALLOWABLE VALUE, the bistable is considered OPERABLE.

Setpoints in accordance with the ALLOWABLE VALUE will assure that Safety Limits (SLs) of LCO Section 2.0, "Safety Limits," are not violated during anticipated operational occurrences (AOOs), and the consequences of Design Basis Accidents (DBAs) will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA, and the equipment functions as designed.

Each channel can be tested on line to verify that the signal processing equipment and setpoint accuracy is within the specified allowance requirements of Reference 1. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated. SRs for the channels are specified in the Surveillance Requirements section.

The ALLOWABLE VALUES listed in Table 3.3.2-1 are based on the methodology described in Reference 6, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

<u>ESFAS Logic</u>

The two independent actuation subsystems compare the four sensor subsystem outputs. Figure B.3.3.2-1 illustrates the functional arrangement of one actuation subsystem. If a trip occurs in the same parameter in two or more sensor subsystem channels, the two-out-of-four logic in each actuation subsystem initiates one train of ESFAS. Either train controls sufficient redundant and independent equipment.

(continued)

(continued)

BACKGROUND (continued)

Each actuation subsystem channel is housed in two cabinets. One cabinet contains the logic circuitry for the actuation channel, while the other cabinet contains the power relay equipment. This power relay equipment includes the power relays (initiation relays) which actuate the ESFAS equipment in response to a signal from the actuation logic.

It is possible to change the two-out-of-four ESFAS logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the matrix logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the logic associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Trip channel bypassing can be simultaneously performed to any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

For plants that have demonstrated sufficient channel-to-channel independence two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures ESFAS actuation would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent actuations caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are operating bypasses (blocks) on the Pressurizer Pressure--Low input to the SIAS, and the Steam Generator (SG) Pressure--Low input to the MSIS, when these inputs are no longer required for protection. These bypasses are enabled manually when the enabling conditions are satisfied in three of the four sensor subsystem channels. The operating bypass circuitry employs four bistable channels in the sensor subsystems, sensing pressurizer pressure (for the SIAS), and SG pressure (for MSIS). These bistables provide contact output to the three-out-of-four logic in the two actuation subsystem channels. When the logic is satisfied, manual bypassing is permitted. There are two manual bypass

(continued)

(continued)

BACKGROUND (continued)

actuation controls for each function, one per train. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied.

Manual ESFAS initiation capability is provided to permit the operator to manually actuate an ESF System when necessary. Two push buttons are provided in the control room for each ESFAS function. Each push button actuates one train via the ESFAS logic.

The actuation logic is tested by inserting a local test signal. A coincidence logic trip will occur if there is the simultaneous presence of a sensor channel trip, either legitimate or due to testing. Most ESFAS functions employ several separate parallel two-out-of-four actuation logic modules, with each module actuating a subset of the ESFAS equipment associated with that function. Each of these subchannels can be tested individually, so that simultaneous actuation of an entire train can be avoided during testing.

Except in the case of actuation subchannels SIAS Nos. 5 and 10, CIAS No. 5, and MSIS No. 1, all actuation logic channels can be tested at power. The above-designated subchannels must be tested when shut down because they actuate the following equipment, which cannot be actuated at power:

- Reactor coolant pump (RCP) seal bleedoff isolation valves;
- Service water isolation valves;
- Volume control tank (VCT) discharge valves;
- Letdown stop valves;
- Component cooling water (CCW) to RCPs;
- CCW from RCPs;
- Main steam isolation valves;
- Feedwater isolation valves; and
- Instrument air containment isolation valves.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents can be detected by one or more ESFAS functions. One of the ESFAS functions is the primary actuation signal for that accident. An ESFAS function may be the primary actuation signal for more than one type of accident. An ESFAS function may also be a

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

secondary, or backup, actuation signal for one or more other accidents. Functions such as manual initiation not specifically credited in the accident analysis were qualitatively credited in the safety analysis or the NRC Staff-approved licensing basis for the plant. These functions may provide protection for conditions which do not require dynamic transient analysis to demonstrate function performance. These functions may also serve as backups to functions that were credited in the accident analysis described by Reference 5.

ESFAS protective functions are as follows:

1. Safety Injection Actuation Signal

The SIAS ensures acceptable consequences during loss-of-coolant accident (LOCA) events, including steam generator tube rupture (SGTR), and main steam line breaks (MSLBs) or feedwater line breaks (FWLBs) (inside containment). To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS) [, control room isolation,] and the emergency diesel generators.

2. Containment Spray Actuation Signal

The CSAS initiates containment spray, preventing containment over-pressurization during a LOCA or MSLB. To provide the required protection, both a high containment pressure signal and an SIAS have to actuate. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

The CIAS actuates the Containment Isolation System ensuring acceptable consequences during LOCA and MSLBs or FWLBs (inside containment). To provide protection, a high containment pressure signal will initiate CIAS at the same setpoint as a SIAS is generated.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

4. Main Steam Isolation Signal

The MSIS ensures acceptable consequences during an MSLB or FWLB by isolating both SGs if either generator indicates a low SG pressure. The MSIS, concurrent with or following a reactor trip, minimizes the rate of heat extraction and subsequent cooldown of the RCS during these events.

5. Recirculation Actuation Signal

At the end of the injection phase of a LOCA the Refueling Water Tank (RWT) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWT to containment sump must occur before the RWT empties to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWT to ensure the reactor remains shut down in the recirculation mode. A RWT Level--Low signal initiates the RAS.

6. Auxiliary Feedwater Actuation Signal

An AFAS initiates feedwater flow to both SGs if a low level is indicated in either SG unless the generator is ruptured.

The AFAS maintains an SG heat sink during the following events:

1. MSLB;
2. FWLB;
3. Inadvertent opening of an SG atmospheric dump valve; and
4. Loss of feedwater.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

A low SG water level signal will initiate auxiliary feed to the affected SG.

Secondary SG differential pressure (SG1 > SG2 or SG2 > SG1) inhibits auxiliary feed to a generator identified as being ruptured. This input to the AFAS logic prevents loss of the intact generator while preventing feeding a ruptured generator during MSLB and FWLBs. This prevents containment overpressurization during these events.

The ESFAS satisfies Criterion 3 of the NRC Interim Policy Statement.

LCO

The LCO requires all instrumentation performing an ESFAS function to be OPERABLE. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected functions. The specific criteria for determining channel OPERABILITY differ slightly between functions. These criteria are discussed on a function-by-function basis below.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same function bypassed. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the function to four channel operation (two-out-of-four logic), or placing the channel in trip (one-out-of-three logic). At plants where adequate channel-to-channel independence has been demonstrated, specific exceptions have been approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time.

Only the ALLOWABLE VALUES are specified for each ESFAS actuation trip function in the LCO. Nominal trip setpoints are specified in the plant-specific setpoint calculations. The nominal setpoints are selected to ensure the setpoints monitored by the CHANNEL FUNCTIONAL TESTS do not exceed the ALLOWABLE VALUE if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its ALLOWABLE VALUE, is acceptable provided that operation and testing is consistent with the assumptions of the plant-specific setpoint

(continued)

(continued)

LCO (continued)

calculations. Each ALLOWABLE VALUE specified is more conservative that the analytical limit assumed in transient and accident analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 6).

The trip functions specified in Table 3.3.2-1 are considered OPERABLE when:

1. All channel components necessary to provide an ESFAS actuation are functional and in service;

2. Channel measurement uncertainties are known via test, analysis, or design information to be within the assumptions of the setpoint calculations;

3. Required surveillance testing is current and has demonstrated performance within each surveillance test acceptance criteria; and

4. The associate operational bypass is not enabled except under the conditions set in the LCO Applicability for the function.

The Bases for the LCO on ESFAS functions are:

1. <u>Safety Injection Actuation Signal</u>

   1a. <u>Manual Actuation</u>

   This LCO requires two channels of SIAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

   Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

   The SIAS Manual Actuation channels only function to energize or de-energize, open or close, contacts. Therefore, these functions have no adjustable trip function with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

1b. Containment Pressure--High

This LCO requires four channels of SIAS Containment Pressure--High to be OPERABLE in MODES 1, 2, and 3.

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup), and not indicative of an off-normal condition. The setting is low enough to initiate the ESF functions when an off-normal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

1c.i Pressurizer Pressure--Low

This LCO requires four channels of SIAS Pressurizer Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

Pressurizer Pressure--Low trip channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, 3, and 4.

The ALLOWABLE VALUE for this trip is set low enough to prevent actuating the SIAS during normal plant operation and pressurizer pressure transients. The setting is high enough that with a LOCA or MSLB it will actuate to perform as expected, mitigating the consequences of the accidents.

The Pressurizer Pressure--Low trip may be blocked when pressurizer pressure is reduced during controlled plant shutdowns. This block is permitted below [1800] psia, and block permissive responses are annunicated in the control room. This allows for a controlled depressurization of

(continued)

(continued)

BASES (continued)

LCO (continued)

the RCS while maintaining administrative control of ESF protection. From a blocked condition, the block will be automatically removed as pressurizer pressure increases above 1800 psia as sensed by two of the four sensor subsystems, in accordance with the bypass philosophy of removing bypasses when the enabling conditions are no longer satisfied.

1c.ii <u>Bypass Permissive Removal for Pressurizer Pressure--Low</u>

This LCO requires four channels of the Bypass Permissive Removal for SIAS Pressurizer Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

The Bypass Removal for Pressurizer Pressure--Low channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The bypass permissive channels consist of four sensor subsystems and two actuation subsystems. This LCO applies to failures in the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered actuation logic failures, and are addressed in the logic LCO.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue.

[At this facility, the basis for the ALLOWABLE VALUE is as follows:]

1d. <u>Actuation Logic</u>

This LCO requires two channels of SIAS Actuation Logic for SIAS to be OPERABLE in MODES 1, 2, 3, and [4].

(continued)

(continued)

BASES (continued)

LCO
(continued)

Actuation logic consists of all circuitry housed within the actuation subsystems including the initiating relay contacts responsible for actuating the ESF equipment.

Actuation logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The SIAS Actuation Logic only functions to energize or de-energize, or to open or close, contacts.

Therefore, these functions have no adjustable trip function setpoints with which to associate an ALLOWABLE VALUE.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. For a complete actuation it is also necessary to have an automatic or manual SIAS. The SIAS opens the containment spray valves, whereas the CSAS actuates other required components. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure--High signal used in the SIAS is the same setpoint used in the CSAS. The transmitters used to initiate CSAS are independent of those used in the SIAS to prevent inadvertent containment spray due to failures in two sensor channels.

2a. Manual Actuation

This LCO requires two channels of CSAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CSAS Manual Actuation channels only function to energize/de-energize or open/close contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

2b. Containment Pressure--High

This LCO requires four channels of CSAS Containment Pressure--High to be OPERABLE in MODES 1, 2, and 3.

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY Requirements 1, 2, and 3.

The ALLOWABLE VALUE is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup), and not indicative of an off-normal condition. The setting is low enough to initiate the ESF functions when an off-normal condition is indicated. This allows the ESF Systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

The Containment Pressure--High setpoint is the same in the SIAS (Function 1), CSAS (Function 2), and CSIAS (Function 3). However different sensors and logic are used in each of these functions.

2c. Actuation Logic

This LCO requires two channels of CSAS Actuation Logic for CSAS to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation logic channels are OPERABLE when they satisfy OPERABILITY Requirements 1 and 3.

Actuation logic consists of all circuitry housed within the actuation subsystems including the initiating relay contacts responsible for actuating the ESF equipment.

The CSAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no

(continued)

(continued)

BASES (continued)

LCO (continued)

adjustable trip function with which to associate and ALLOWABLE VALUE.

3. Containment Isolation Actuation Signal

3a. Manual Actuation

This LCO requires two channels of CIAS Manual Actuation for CIAS to be OPERABLE in MODES 1, 2, 3, and 4.

Manual actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CIAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

3b. Containment Pressure--High

This LCO requires four channels of CIAS Containment Pressure--High to be OPERABLE in MODES 1, 2, and 3.

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup), and not indicative of an off-normal condition. The setting is low enough to initiate the ESF functions when an off-normal condition is indicated. This allows the ESF Systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

The Containment Pressure--High setpoint is the same in the SIAS (Function 1), CSAS (Function 2),

(continued)

(continued)

BASES (continued)

LCO (continued)

and CIAS (Function 3). However different sensors and logic are used in each of these functions.

3c. Containment Radiation--High

This LCO requires four channels of CIAS Containment Radiation--High to be OPERABLE in MODES 1, 2, and 3.

Containment Radiation--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE is high enough to avoid unnecessary actuation, but adequate to provide diverse actuation of the CIAS in the event of a LOCA.

3d. Actuation Logic

This LCO requires two channels of Actuation Logic for CIAS to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

Actuation logic consists of all circuitry housed within the actuation subsystems including the initiating relay contacts responsible for actuating the ESF equipment.

The CIAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable setpoints with which to associate an ALLOWABLE VALUE.

4. Main Steam Isolation Signal

4a. Manual Actuation

This LCO requires two channels [per SG] of the MSIS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

(continued)

(continued)

BASES (continued)

LCO (continued)

Manual actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The MSIS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

4b.1. Steam Generator Pressure--Low

This LCO requires four channels of MSIS SG Pressure--Low for each SG to be OPERABLE in MODES 1, 2, and 3.

SG Pressure--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, 3, and 4.

The ALLOWABLE VALUE is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide the required protection for excessive steam demand. An excessive steam demand causes the RCS to cool down, resulting in a positive reactivity addition to the core. An MSIS is required to prevent the excessive cooldown.

This function may be manually blocked when SG pressure is reduced during controlled plant cooldowns. The block is permitted below 785 psia and the block permissive responses are annunciated in the control room. This allows a controlled depressurization of the secondary system while maintaining administrative control of ESF protection. From a blocked condition the block will be removed automatically as SG pressure increases above 785 psia, as sensed by two of the four sensor subsystems, in accordance with the bypass philosophy of removing bypasses when the enabling conditions are no longer satisfied.

(continued)

(continued)

LCO
(continued)

4b.ii. Bypass Permissive Removal for SG Pressure--Low

This LCO requires four channels per SG of the Bypass Removal for MSIS SG Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

Bypass permissive channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2 and 3.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This LCO applies to failures in the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered actuation logic failures, and are addressed in the logic LCO.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue.

[For this facility, the basis for the ALLOWABLE VALUE is as follows:]

4c. Actuation Logic

This LCO requires two channels of MSIS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The MSIS Actuation Logic only functions to energize or de-energize, or to open or close, contacts. Therefore, these functions have no adjustable trip function with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

5. Recirculation Acutation Signal

5a. Manual Actuation

This LCO requires two channels of RAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The RAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts.

Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

5b. Refueling Water Tank Level--Low

This LCO requires four channels of RWT Level--Low to be OPERABLE in MODES 1, 2, and 3.

RWT Level--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The upper limit on ALLOWABLE VALUE for this trip is set low enough to ensure RAS does not initiate before sufficient water is transferred to the containment sump. Premature recirculation could impair the reactivity control function of safety injection by limiting the amount of boron injection. Premature recirculation could also damage or disable the recirculation system if recirculation begins before the sump has enough water to prevent air entrainment in the suction. The lower limit on the RWT Level--Low trip ALLOWABLE VALUE is high enough to transfer suction to the containment sump prior to emptying the RWT.

(continued)

(continued)

LCO
(continued)

5c. Actuation Logic

This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The RAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions do not have adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

6. Auxiliary Feedwater Actuation Signal

The AFAS logic actuates auxiliary feedwater (AFW) to an SG on low level in that generator unless it has been identified as being ruptured.

A low level in either generator, as sensed by a two-out-of-four coincidence of four wide range sensors for any generator, will generate an AFAS start signal, which starts both trains of AFW pumps, and feeds both SGs. The AFAS also monitors the secondary differential pressure in both SGs, and initiates an AFAS block signal to a ruptured generator if the pressure in that generator is lower than the other generator by the differential pressure setpoint.

6a. Manual Actuation

This LCO requires [four] channels per SG of AFAS Manual Actuation to be OPERABLE in MODES 1, 2, and 3.

Manual actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The AFAS Manual Actuation channels only function to energize or de-energize, open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

6b. SG A/B Level--Low

This LCO requires 4 channels, for each SG, of SG Level--Low to be OPERABLE in MODES 1, 2, and 3.

SG Level--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE assures adequate time exists to initiate AFW while the SGs can function as a heat sink.

6c. SG Differential Pressure--High (SG-A > SG-B) or (SG-B > SG-A).

This LCO requires four channels per SG of SG Differential Pressure--High to be OPERABLE in MODES 1, 2, and 3.

SG Differential Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is high enough to allow for small pressure differences and normal instrumentation errors between the SG channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured SG in the event of an MSLB or FWLB while permitting the feeding of the intact SG.

6d. Actuation Logic

This LCO requires two channels per SG of AFAS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

Actuation logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

(continued)

(continued)

LCO
(continued)

Actuation logic consists of all circuitry housed within the actuation subsystems including the initiating relay contacts responsible for actuating the ESF equipment.

The AFAS Actuation Logic only functio. to energize or de-energize, or open or c.ose, contacts. Therefore, these functions have no trip setpoints with which to associate an ALLOWABLE VALUE.

[For this facility, the following support systems are required to be OPERABLE to ensure ESFAS instrumentation OPERABILITY:]

[For this facility, those required support systems which upon their failure do not result in the ESFAS instrumentation being declared inoperable and their justification are as follows:]

[For this facility, the supported systems impacted by inoperability of the ESFAS instrumentation and the justification of whether or not each supported system is declared inoperable are as follows:]

APPLICABILITY

All ESFAS functions are required to be OPERABLE in MODES 1, 2, and 3. In MODES 1, 2 and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

1. Close the main steam isolation valves (MSIVs), to preclude a positive reactivity addition;
2. Actuate AFW to preclude the loss of the SGs as a heat sink (in the event the normal feedwater system is not available);
3. Actuate ESF Systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB; and

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

4. Actuate ESF Systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

In MODES 4, 5, and 6 automatic actuation of ESFAS functions is not required because adequate time is available for plant operators to evaluate plant conditions and respond by manually operating the ESF components if required. ESFAS manual actuation capability is required for functions other than AFAS in MODE 4 even though automatic actuation is not required. Because of the large number of components actuated on each ESFAS, actuation is simplified by the use of the manual actuation push buttons. Manual actuation of AFAS is not required in MODE 4 because AFW will already be in operation in this MODE.

The ESFAS actuation logic must be OPERABLE in the same MODES as the automatic and manual actuations. In MODE 4, only the portion of the ESFAS logic responsible for the required manual actuation must be OPERABLE.

In MODES 5 and 6, ESFAS-initiated systems are either reconfigured or disabled for shutdown cooling operation. Accidents in these MODES are slow to develop, and would be mitigated by manual operation of individual components.

A Note has been added to provide clarification that each function specified in Table 3.3.2-1 is treated as an independent entity for this LCO, with an independent Completion Time.

ACTIONS

A protection function channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined for each function in the LCO section of the Bases. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis.

Typically, the drift is small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is not consistent with the ALLOWABLE VALUE in Table 3.3.2-1, the channel must be declared inoperable immediately, and the appropriate Condition(s) from Table 3.3.2-1 entered.

In the event a channel's trip setpoint is found non-conservative with respect to the ALLOWABLE VALUE, or the transmitter, instrument loop, signal processing electronics, or ESFAS bistable is found inoperable, then all affected functions provided by that channel must be declared inoperable and the unit must enter the condition statement for the particular protection function affected.

When the number of inoperable channels in a trip function exceeds those specified in any related Condition associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered, if applicable in the current MODE of operation.

<u>Condition A</u>

Condition A is applicable to all ESFAS protection functions. Condition A addresses the situation where one or more channels for one or more functions are inoperable at the same time. The Required Action is to refer to Table 3.3.2-1 and immediately take the Required Actions for the protection functions affected.

<u>Condition B</u>

Condition B applies to the failure of a single channel of one or more input parameters in the following ESFAS functions:

1. SIAS
   Containment Pressure--High
   Pressurizer Pressure--Low

3. CIAS
   Containment Pressure--High
   Containment Radiation--High

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

4. MSIS
SG Pressure--Low

5. RAS
Refueling Water Tank Level--Low

6. AFAS
SG Level--Low
SG Differential Pressure--High

ESFAS coincidence logic is normally two-out-of-four. If one ESFAS channel is inoperable, startup or power operation is allowed to continue as long as action is taken to restore the design level of redundancy.

Required Action B.1 is the preferred action as it restores full functional capability of the ESFAS.

If one ESFAS channel is inoperable, startup or power operation is allowed to continue providing the inoperable channel is placed in bypass or trip within one hour (Required Action B.2.1). By specifying either option, the possibility of inadvertently bypassing a redundant channel is eliminated. The provision of four trip channels allows one channel to be bypassed (removed from service) during operations, placing the ESFAS in two-out-of-three coincidence logic.

The Completion Time of 1 hour allotted to restore bypass or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

For plants that have not demonstrated sufficient channel-to-channel independence, the failed channel is restored to OPERABLE status or is placed in trip within 48 hours (Required Action B.2.2.1 or B.2.2.2). Required Action B.2.2.1 restores the full capability of the function. Required Action B.2.2.1 places the function into a one-out-of-three configuration. In this configuration, common cause failure of the dependent channel cannot prevent ESFAS actuation. The 48-hour Completion Time is based upon

(continued)

(continued)

ACTIONS (continued)

operating experience which has demonstrated that a random failure of a second channel occurring during the 48-hour period is a low probability event.

Condition C

Condition C applies to the failure of two channels in any of the following ESFAS functions:

1. SIAS
   Containment Pressure--High
   Pressurizer Pressure--Low

3. CIAS
   Containment Pressure--High
   Containment Radiation--High

4. MSIS
   SG Pressure--Low

5. RAS
   RWT Level--Low

6. EFAS
   SG level--Low
   SG Differential Pressure--High

Required Action C.1 is the preferred option as it improves the functional reliability of the ESFAS.

With two inoperable channels, one channel should be placed in bypass, and the other channel should be placed in trip within the 1-hour Completion Time. With one channel of protective instrumentation bypassed, the ESFAS function is in two-out-of-three logic but with another channel failed, the ESFAS may be operating with a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the ESFAS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, ESFAS actuation will occur.

For plants that have not demonstrated sufficient channel-to-channel independence one of the failed channels should be restored to OPERABLE status within 48 hours, for reasons

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

similar to those stated under Condition B. After one channel is restored to OPERABLE, the provisions of Condition B still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action C.2.2 shall be placed in trip if more than 48 hours has elapsed since the initial channel failure.

<u>Condition D</u>

Condition D applies to the failure of one MSIS SG Pressure--Low or SIAS Pressurizer Pressure--Low bypass removal channel.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. Condition D applies to failures in one of the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches are considered actuation logic failures, and are addressed in Condition I.

In Condition D it is permissible to continue operation with one bypass permissive removal channel failed, providing the bypass is disabled (Required Action D.2). This can be accomplished by removing the bypass with the manual bypass key switch which disables the bypass in both trains. Since the bypass function must be manually enabled, the bypass permissive function will not by itself cause an undesired bypass insertion.

Alternatively, the bypass may be disabled by defeating the bypass permissive input in one of the four channels to the two-out-of-four bypass removal logic, placing the bypass removal feature in one-out-of-three logic. Thus any of the remaining three channels is capable of removing the bypass feature when the bypass enable conditions are no longer valid.

If the bypass removal feature in the inoperable channel cannot be defeated, actions to address the inoperability of the affected automatic trip channel must be taken. Required Action D.3.1, Required Action D.3.2.1, and Required Action D.3.2.2, are equivalent to the Required Actions for a

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

single automatic trip channel failure (Condition B). The 1-hour and 48-hour Completion Times have the same basis as discussed for Condition B.

Condition E

Condition E applies to two inoperable bypass removal channels. The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This Condition applies to failures in two of the four sensor subsystems. With two of the four sensor subsystems failed in a non-conservative direction (enabling the bypass function), the bypass removal feature is in two-out-of-two logic. Failures in the actuation subsystems, including the manual bypass key switches, are considered actuation logic failures, and are addressed in Condition I.

In Condition E it is permissible to continue operation with two bypass permissive channels failed, providing the bypasses are disabled in a similar manner as discussed for Condition D.

If the failed bypasses cannot be disabled, actions to address the inoperability of the affected automatic trip channels must be taken. Required Action E.3.1 and Required Action E.3.2 are equivalent to the Required Actions for a two automatic trip channel failures (Condition C). Also similar to Condition C, after one set of inoperable channels are restored the provisions of Condition D still apply to the remaining inoperable channel, with the Completion Time measured from the point of the initial bypass channel failure. The 1-hour and 48-hour Completion Times have the same basis as discussed for Condition C.

Condition F

Condition F applies to one CSAS Containment Pressure--High channel inoperable. CSAS logic is identical to that of the other ESFAS functions; however, the inadvertent actuation of a CSAS is undesirable, since it may damage equipment inside containment. For this reason, placing the inoperable channel in trip is not an option as it is in Conditions B and C.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Required Action F.1 is the preferred action as it restores full functional capability of the CSAS. If one CSAS channel is inoperable, operation is allowed to continue providing the inoperable channel is placed in bypass within 1 hour. The Completion Time of 1 hour allotted to bypass the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

For plants that have not demonstrated acceptable channel-to-channel independence, true four-channel independence cannot be assured, and two of the remaining three channels may be subject to common cause failures. Therefore, Required Action F.2.2 requires restoring the channel to OPERABLE status to restore the full functional capability of the CSAS Containment Pressure High function. The Completion Time of 48 hours is based upon operating experience that has demonstrated that random failure of a second channel is improbable during any given 48-hour period.

Condition G

Condition G applies to one AFAS Manual Actuation or AFAS Actuation Logic channel inoperable. It is identical to Condition I for the other ESFAS functions except the shutdown track imposed by Condition K.

The channel must be restored to OPERABLE status to restore redundancy of the AFAS function. The 1-hour Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

Condition H

If the Required Actions and associated Completion Times of Condition B, C, D, E, F, or G cannot be met the reactor should be brought to a MODE where the LCO does not apply to the affected function. Six hours to place the plant in MODE 3 and 12 hours in MODE 4 are reasonable times, based on operating experience, to reach the required MODES from full power in an orderly manner and without challenging plant systems.

(continued)

(continued)

ACTIONS (continued)

Condition I

Condition I applies to one manual actuation or actuation logic channel inoperable for those ESFAS functions which must be OPERABLE in MODES 1 through 4 (all functions except AFAS). The shutdown track imposed by Condition J requires entry into MODE 5, where the LCO does not apply to the affected functions.

The channel must be restored to OPERABLE status to restore redundancy of the affected functions. The 1-hour Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

Condition J

Condition J is entered when the required actions and associated Completion Times of Condition I are not met. The plant must be brought to a MODE where the LCO does not apply to the affected functions. Six hours to bring the plant to MODE 3 and 30 additional hours to reach MODE 5 are reasonable times, based on operating experience, to reach these MODES from full power in an orderly manner and without challenging plant systems.

Condition K

Condition K is applicable to each one of the ESFAS functions presented in Table 3.3.2-1.

Required Action K.1 verifies that the Required Actions have been initiated for those supported systems declared inoperable because of the inoperability of the support channel(s) within a Completion time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination.

Required Action K.1 ensures that those identified Required Actions associated with supported systems impacted by the inoperability of channel(s) associated with each ESFAS function have been initiated. This can be accomplished by entering the supported systems LCOs or independently as a group of Required Actions needed to be initiated every time

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition K is entered. [For this facility, the identified supported systems Required Actions associated with each ESFAS Function are as follows:]

Required Action K.2 verifies that all required support or supported features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 should be immediately entered. However, if the support or supported feature LCO takes into consideration the loss-of-function situation then LCO 3.0.3 may not need to be entered.

SURVEILLANCE REQUIREMENTS

The SRs for any particular ESFAS function are found in the SRs column of Table 3.3.2-1, for that function. Most functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing.

In order for a facility to take credit for topical reports as the basis for justifying Surveillance Frequencies, topical reports should be supported by an NRC Staff Safety Evaluation Report that establishes the acceptability of each topical report for that facility.

SR 3.3.2.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. CHANNEL CHECK will detect gross channel failure, thus it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION. The high radiation instrumentation should be compared to similar plant instruments located throughout the plant. If the radiation monitor employs keep-alive sources or check

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

sources operable from the control room, the CHANNEL CHECK should also note the detector's response to these sources.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside their limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off-scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off-scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Surveillance Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited to 12 hours. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent checks of channel operability during normal operational use of displays associated with the LCO required channels.

SR 3.3.2.2 and SR 3.3.2.3

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed.

The CHANNEL FUNCTIONAL TEST consists of an overlapping test sequence similar to that employed in the RPS which tests the individual sensor subsystems using an analog test input to each bistable.

Bistable Tests. "As found" and "as left" values for bistable trip setpoints are recorded. The bistable setpoints must be found to trip within the ALLOWABLE VALUES specified in the LCO. The difference between the current "as found" and the previous test "as left" values must be

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

consistent with the drift allowance used in the setpoint analysis. Whenever these tolerances are not met, a recalibration can be performed to establish OPERABILITY of the channel. However, repeated consecutive failures would be indicative of a failure that cannot be corrected by recalibration alone.

<u>Actuation Logic Tests</u>. Actuation subsystem testing includes injecting one trip signal into each two-out-of-four logic subsystem in each ESFAS function, and using a bistable trip input to satisfy the trip logic. Initiation relays associated with the affected channel will then actuate the individual ESFAS components. Since each ESFAS function employs subchannels of actuation logic, it is possible to actuate individual components without actuating an entire ESFAS function.

Note 1 to SR 3.3.2.3 requires that actuation logic tests include operation of initiation relays. Note 2 allows exemption of certain relays from testing at power to allow for the fact that operating certain relays during power operation could cause plant transients or equipment damage. those initiation relays which cannot be tested at power must be tested in accordance with Note 2 in SR 3.3.2.3. These include: SIAS No. 6, SIAS No. 10, CIAS No. 5, and MSIS No. 1.

These relays actuate the following components, which cannot be tested at power:

- RCP seal bleedoff isolation valves;
- Service water isolation valves;
- VCT discharge valves;
- Letdown stop valves;
- CCW to and from the RCPs;
- MSIVs and feedwater isolation valves; and
- Instrument air containment isolation valves.

The reasons that each of the above cannot be fully tested at power are stated in Reference 1.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components.

(continued)

(continued)

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

A test signal is then superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS channel trip channel bypassed.

SR 3.3.2.4

Surveillance Requirement 3.3.2.4 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.2.2 except 3.3.2.4 is performed within 92 days prior to startup and is only applicable to bypass functions. These include the Pressurizer Pressure--Low Bypass and the MSIS SG Pressure--Low Bypass.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass permissives is critical during plant heatups because the bypasses may be in place prior to entering MODE 3, but must be removed at the appropriate points during plant startup to enable the ESFAS function. Consequently, just prior to startup is the appropriate time to verify Bypass Removal function OPERABILITY. Once the bypasses are removed the bypasses must not fail in such a way that the associated ESFAS function is inappropriately bypassed. This feature is verified by the appropriate ESFAS function CHANNEL FUNCTIONAL TEST.

The allowance to conduct this test within 92 days of startup is based upon the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

SR 3.3.2.5

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to the measured parameter with the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive tests, to ensure that the instrument channel remains operational with the setpoint within the assumptions of the plant-specific setpoint analysis. Transmitter "as found" and "as left" values are recorded and used to verify

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

drift assumptions. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint errors are within the assumptions of the plant-specific setpoint analysis. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis.

Recalibration restores OPERABILITY of an otherwise functional component found to have errors larger than assumed by the setpoint analysis. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure which cannot be corrected by recalibration.

Field transmitters may be calibrated in place, removed and calibrated in a laboratory, or replaced with an equivalent, laboratory-calibrated, unit.

The Surveillance Frequency is based on the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.2.6

A CHANNEL FUNCTIONAL TEST is performed on the manual ESFAS actuation circuitry, de energizing relays, and providing manual actuation of the function.

This test verifies that the trip push buttons are capable of opening contacts in the actuation logic as designed, de-energizing the initiation relays, and providing manual actuation of the function. The 18-month Frequency was developed considering it was prudent that these Surveillances only be performed during a plant outage. This is due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 18-month Frequency.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.7

This Surveillance ensures that the train actuation response times are verified on a STAGGERED TEST BASIS. The response time values are provided in the FSAR, and are the maximum values assumed in the safety analyses.

Individual component response times are not modeled in the analyses. The analysis models the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor, to the point at which the equipment in both trains reaches the required functional state, e.g., pumps at rated discharge pressure, valves in full open or closed position. [For this facility, ENGINEERED SAFETY FEATURE RESPONSE TIME testing acceptance criteria are contained in the following document:]

The test may be performed in one measurement or overlapping segments, with verification that all components are measured.

ENGINEERED SAFETY FEATURE RESPONSE TIME tests are conducted on a 18-month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n x 18 months, where, is the number of channels in the function. Testing of the final actuation devices, which make up the bulk of the response time, is included in the testing of each channel. Therefore, staggered testing results in response time verification of these devices every 18 months. The 18-month STAGGERED TEST BASIS Frequency is based upon plant operating experience which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Response times cannot be determined at power since equipment operation is required.

REFERENCES

1. [Unit Name] FSAR, Chapter [7.3], ["Instrumentation and Control"].

2. Title 10, Code of Federal Regulations, Part 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."

(continued)

(continued)

BASES (continued)

REFERENCES (continued)

3. [Unit Name], [NRC Staff Safety Evaluation Report, (Date)].

4. Institute of Electrical and Electronic Engineers, IEEE-279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

5. [Unit Name] FSAR, Chapter [14], "Accident Analysis."

6. [Unit Name], "[Plant Protection System Selection of Trip Setpoint Values.]"

7. Title 10, Code of Federal Regulations, Appendix A, "General Design Criteria for Nuclear Power Plants."

8. CEN 327 "RPS/ESFAS Extended Test Interval Evaluation," June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.2 Engineered Safety Features Actuation Systems (ESFAS) Instrumentation (Digital)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and Reactor Coolant System (RCS) pressure boundary to mitigate accidents.

The ESFAS contains devices and circuitry which generate the following signals when monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS);
2. Containment Spray Actuation Signal (CSAS);
3. Containment Isolation Actuation Signal (CIAS);
4. Containment Cooling Actuation Signal (CCAS);
5. Main Steam Isolation Signal (MSIS);
6. Recirculation Actuation Signal (RAS); and
7. Emergency Feedwater Actuation System (EFAS).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS instrumentation systems is segmented into three interconnected modules. These modules are:

- Measurement Channels
- Bistables; and
- ESFAS Logic:
  - Matrix Logic;

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

- Initiation Logic (Trip Paths); and
- Actuation Logic.

The role of each of these modules in the ESFAS is discussed below.

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the generation of trip signals. These channels are designated A through D. Measurement channels provide input to ESFAS bistables within the same ESFAS channel. In addition, some measurement channels are used as inputs to Reactor Protection System (RPS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS or ESFAS are not used for control functions.

When a channel monitoring a parameter indicates an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter will de-energize Matrix Logic, which in turn de-energizes the Initiation Logic. This causes both channels of Actuation Logic to de-energize. Each channel of Actuation Logic controls one train of the associated engineered safety features (ESF) equipment.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in Appendix A to 10 CFR 50 (Ref. 7). The fourth channel provides additional flexibility, by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing, while still maintaining a minimum two-out-of-three logic.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

In order to take full advantage of the four-channel design, adequate channel-to-channel independence must be demonstrated, approved by the NRC staff, and this approval documented by an NRC Safety Evaluation Report. Adequate channel-to-channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants that have demonstrated adequate channel-to-channel independence, as documented by the NRC Safety Evaluation Report (Ref. 3) may operate in a two-out-of-three logic configuration, with one channel removed from service, for the time stated in Reference 2.

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of Institute of Electrical and Electronic Engineers (IEEE) 279-1971 (Ref. 4).

<u>Bistables</u>

Bistable trip units, mounted in the Plant Protective System (PPS) cabinet, receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Matrix Logic. They also provide local trip indication, and remote annunciation.

There are four channels of bistables, designated A through D, for each ESFAS function, one for each measurement channel. In cases where two ESF functions share the same input and trip setpoint (e. g. containment pressure input to CIAS and SIAS), the same bistable may be used to satisfy both functions. Similarly, bistables may be shared between the RPS and ESFAS (e. g. Pressurizer Pressure—Low input to the RPS and SIAS). Bistable output relays de-energize when a trip occurs, in turn de-energizing bistable relays mounted in the PPS relay card racks.

The contacts from these bistable relays are arranged into six coincidence matrices, comprising the Matrix Logic. If bistables monitoring the same parameter in at least two channels trip, the Matrix Logic will generate an ESF actuation (two-out-of-four logic).

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

The trip setpoints and ALLOWABLE VALUES used in the bistables are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment effects, for those ESFAS channels which must function in harsh environments as defined by 10 CFR 50.49 (Ref. 2), ALLOWABLE VALUES specified in Table 3.3.2-1 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 6). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the ALLOWABLE VALUE to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. If the measured setpoint does not exceed the ALLOWABLE VALUE, the bistable is considered OPERABLE.

Setpoints in accordance with the ALLOWABLE VALUE will assure that Safety Limits of LCO Section 2.0, "Safety Limits" are not violated during anticipated operational occurrences (AOOs), and the consequences of Design Basis Accidents (DBAs) will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA, and the equipment functions as designed.

Each channel can be tested on line to verify that the signal processing equipment and setpoint accuracy is within the specified allowance requirements of Reference 1. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated. SRs for the channels are specified in the Surveillance Requirements section.

The ALLOWABLE VALUES listed in Table 3.3.2-1 are based upon the methodology described in Reference 6, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint. All field sensors and

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

ESFAS Logic

The ESFAS Logic, consisting of Matrix, Initiation and Actuation Logic, employs a scheme that provides an ESF actuation of both trains when bistables in any two of the four channels sensing the same input parameter trip. This is called a two-out-of-four trip logic. This logic is shown in Figure B 3.3.2-1.

Matrix Logic refers to the matrix power supplies, bistable relay contacts, and interconnecting wiring up to, but not including the matrix relays.

Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and the initiation relays.

Actuation Logic consists of all circuitry housed within the auxiliary relay cabinets (ARCs) used to actuate the ESF function, and interconnecting wiring to the initiation relay contacts mounted in the PPS cabinet.

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices, to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected, consisting of a trip in the same function in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one relay contact from each matrix relay in each of the four trip paths. Each trip path controls two initiation relays. Each of the two initiation relays in each trip path controls contacts in the Actuation Logic for one train of ESF.

(continued)

(continued)

BACKGROUND (continued)

When a coincidence occurs in two ESFAS channels, all four matrix relays in the affected matrix will de-energize. This, in turn will de-energize all eight initiation relays, four used in each Actuation Logic.

Each of the four Initiation Logic channels opens contacts affecting the Actuation Logic in both ARCs if any of the six coincidence matrices de-energize their associated matrix relays. They thus perform a logical or function. Each Initiation Logic channel has its own power supply, and is independent of the other three channels. Although each of the four Initiation Logic channels within an ESFAS function uses separate power supplies, the Initiation Logic for the different ESFAS functions shares power supplies. Thus failure of a power supply may force entry into the Condition specified for each of the affected ESFAS functions.

Each of the two channels of Actuation Logic, mounted in the ESFAS ARCs, is responsible for actuating one train of ESF equipment. Each ESF function has separate Actuation Logic in each ARC.

The contacts from the Initiation Logic are configured in a selective two-out-of-four logic in the Actuation Logic, similar to the configuration employed by the RPS in the reactor trip circuit breakers (RTCBs). This logic controls ARC-mounted subgroup relays, which are normally energized. Contacts from these relays, when de-energized, actuate specific ESF equipment.

It is possible for two Initiation Logic channels affecting the same trip leg to de-energize in multiple ESFAS functions if a matrix power supply or vital instrument bus fails. This will result in opening the two contacts in each ARC Actuation Logic, leaving the Actuation Logic for both trains in one-out-of-two logic.

If one set of Initiation Logic contacts has been opened in response to a single Initiation Logic channel failure, the affected set of contacts may be closed for up to 1 hour for surveillance testing on the OPERABLE Initiation Logic channels. In this case the redundant set of Initiation Logic contacts will provide protection if a trip should be required. It is unlikely that a trip will be required

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

during the surveillance testing, coincident with a failure of the remaining series initiation relay contacts.

If a single matrix power supply or vital bus failure has de-energized two Initiation Logic channels, the same trip leg in both ARCs will open, placing the Actuation Logic in one-out-of-two logic in both trains. Operation may continue in this condition subject to the requirements of Condition D providing the initiation relay contacts in the Actuation Logic trip leg for both trains open as required.

With one Actuation Logic channel inoperable, automatic actuation of one train of ESF may be inhibited. The remaining train provides adequate protection in the event of DBAs, but the single-failure criterion may be violated. For this reason operation in this condition is restricted.

Failures of individual bistables and their relays are considered measurement channel failures. This section describes failures of the Matrix Logic not addressed in the above, such as the failure of matrix relay power supplies, or the failure of the trip channel bypass contact in the bypass condition. Loss of a single vital bus will de-energize one of the two power supplies in each of three matrices. This will result in two initiation circuits de-energizing, reducing the ESFAS Actuation Logic to a one-out-of-two logic in both trains. For the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure is to be treated as a single matrix channel failure, providing the affected matrix relays de-energize as designed. Although each of the six matrices within an ESFAS function uses separate power supplies, the matrices for the different ESFAS functions share power supplies. Thus failure of a matrix power supply may force entry into the Condition specified for each of the affected ESFAS functions.

(continued)

(continued)

BASES (continued)

This figure for illustration only. Do not use for operation.

Figure B 3.3.2-1

Simplified Functional Diagram of the
ESFAS Logic

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

It is possible to change the two-out-of-four ESFAS logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Trip channel bypassing can be simultaneously performed to any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. An interlock prevents simultaneous trip channel bypassing of the same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

For plants that have demonstrated sufficient channel-to-channel independence, two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures ESFAS actuation would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent actuations caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select ESFAS actuation trips. These bypasses are enabled manually, in all four channels, when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Operating bypasses normally are implemented in the bistable, so that normal trip indication is also disabled. The Pressurizer Pressure--Low input to the SIAS shares an operating bypass with the Pressurizer Pressure--Low reactor trip.

Manual ESFAS initiation capability is provided to permit the operator to manually actuate an ESF System when necessary.

Two sets of two push buttons (located in the control room) for each ESF function are provided, and each set actuates both trains. Each manual actuation push button opens one trip path, de-energizing one set of two initiation relays,

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

one affecting each train of ESF. Initiation relay contacts are arranged in a selective two-out-of-four configuration in the Actuation Logic. By arranging the push buttons in two sets of two, such that both push buttons in a set must be depressed, it is possible to assure that manual actuation will not be prevented in the event of a single random failure. Each set of two push buttons is designated a single channel in this LCO.

APPLICABLE SAFETY ANALYSES

Each of the analyzed accidents can be detected by one or more ESFAS functions. One of the ESFAS functions is the primary actuation signal for that accident. An ESFAS function may be the primary actuation signal for more than one type of accident. An ESFAS function may also be a secondary, or backup, actuation signal for one or more other accidents. Functions such as manual initiation not specifically credited in the accident analysis were qualitatively credited in the safety analysis or the NRC Staff-approved licensing basis for the plant. These functions may provide protection for conditions which do not require dynamic transient analysis to demonstrate function performance. These functions may also serve as backups to functions that were credited in the accident analysis described by Reference 5.

ESFAS protective functions are as follows:

1. Safety Injection Actuation Signal

SIAS ensures acceptable consequences during large-break loss-of-coolant accidents (LOCAs), small-break LOCAs, control element assembly ejection accidents, and main steam line breaks (MSLBs) inside containment. To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCSs), [control room isolation,] and emergency diesel generators.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Spray Actuation Signal

CSAS actuates containment spray, preventing containment over-pressurization during large-break LOCAs, small-break LOCAs, and MSLBs or feedwater line breaks (FWLBs) inside containment. CSAS is initiated by high-high containment pressure and an SIAS. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

CIAS ensures acceptable mitigating actions during large- and small-break LOCAs, and MSLBs or FWLBs either inside or outside containment. CIAS is initiated by low pressurizer pressure or high containment pressure.

4. Containment Cooling Actuation Signal

CCAS mitigates containment overpressurization when required by either a manual or automatic SIAS function. This function is not employed by all plants.

5. Main Steam Isolation Signal

MSIS ensures acceptable consequences during an MSLB or FWLB (between the SG and the main feedwater check valve), either inside or outside containment. MSIS isolates both SGs if either generator indicates a low pressure condition or if a high containment pressure condition exists. This prevents an excessive rate of heat extraction and subsequent cooldown of the RCS during these events.

6. Recirculation Actuation Signal

At the end of the injection phase of a LOCA the refueling water storage tank (RWST) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWST to containment sump must occur before the RWST empties

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWST to ensure the reactor remains shut down in the recirculation mode. A RWST Level--Low signal initiates the RAS.

7. <u>Emergency Feedwater Actuation System</u>

EFAS consists of two SG-specific signals (EFAS 1 and EFAS 2). EFAS 1 initiates emergency feed to SG 1 and EFAS 2 initiates emergency feed to SG 2.

EFAS maintains an SG heat sink during a steam generator tube rupture event and an MSLB or FWLB event either inside or outside containment.

Low SG water level initiates emergency feed to the affected SG, providing the generator is not identified (by the circuitry) as faulted (a steam or feedwater line break).

EFAS logic includes SG-specific inputs from the SG Pressure--Low bistable comparator (also used in MSIS), and the SG Differential Pressure--High (SG1 > SG2 or SG2 > SG1, bistable comparators), to determine if a rupture in either generator has occurred.

Rupture is assumed if the affected generator has a low pressure condition, unless that generator is significantly higher in pressure than the other generator.

This latter feature allows feeding the intact SG even if both are below the MSIS setpoint, while preventing the ruptured generator from being fed. Not feeding a ruptured generator prevents containment over-pressurization during the analyzed events.

The ESFAS satisfies Criterion 3 of the NRC Interim Policy Statement.

(continued)

BASES (continued)

LCO

The LCO requires all instrumentation performing an ESFAS function to be OPERABLE. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected functions. The specific criteria for determining channel OPERABILITY differs slightly between functions.

For those designs approved by the NRC Staff to permit one of the two-out-of-four channels bypassed for an extended period of time, the plant may operate for the time allowed in Reference 3, with one channel in each function bypassed, effectively placing the plant in a two-out-of-three logic configuration in those functions. In other cases, plants are restricted to 48 hours in a trip channel bypass condition before restoring the function to four channel operation (two-out-of-four logic), or placing the channel in trip (two-out-of-three logic).

Only ALLOWABLE VALUES are specified for each ESFAS actuation trip function in the LCO. Nominal trip setpoints are specified in the plant-specific setpoint calculations. The nominal setpoints are selected to ensure the setpoints monitored by the CHANNEL FUNCTIONAL TESTS do not exceed the ALLOWABLE VALUE if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its ALLOWABLE VALUE, is acceptable provided that the operation and testing is consistent with the assumptions of the plant-specific setpoint calculations. Each ALLOWABLE VALUE specified is more conservative than the analytical limit assumed in transient and accident analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 6).

The trip functions specified in Table 3.3.2.-1 are considered OPERABLE when:

1. All channel components necessary to provide an ESFAS actuation are functional and in service;

2. Channel measurement uncertainties are known via test, analysis, or design information to be within the assumptions of the setpoint calculations;

(continued)

(continued)

BASES (continued)

LCO (continued)

3. Required surveillance testing is current and has demonstrated performance within each surveillance test acceptance criteria; and

4. The associate operational bypass is not enabled except under the conditions set in the LCO Applicability for the function.

These criteria are discussed on a function-by-function basis below.

The bases for the LCOs on ESFAS functions are:

1. Safety Injection Actuation Signal

a. Manual Actuation

This LCO requires two channels of SIAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The SIAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

b. Containment Pressure--High

This LCO requires four channels of SIAS Containment Pressure--High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure--High signal is shared between the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 5).

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is set high enough to allow for small pressure increases in

(continued)

(continued)

BASES (continued)

LCO (continued)

containment expected during normal operation (i.e., plant heatup), and not indicative of an off-normal condition. The setting is low enough to initiate the ESF functions when an off-normal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

[illegible].i Pressurizer Pressure--Low

This LCO requires four channels of SIAS Pressurizer Pressure--Low to be OPERABLE in MODES 1 and 2.

Pressurizer Pressure--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, 3, and 4.

The ALLOWABLE VALUE for this trip is set low enough to prevent actuating the ESF functions (SIAS and CIAS) during normal plant operation and pressurizer pressure transients. The setting is high enough that with the specified accidents the ESF systems will actuate to perform as expected, mitigating the consequences of the accidents.

The Pressurizer Pressure--Low trip setpoint, which provides SIAS, CIAS, and RPS trip, may be manually decreased to a floor value of 300 psia to allow for a controlled cooldown and depressurization of the RCS without causing a reactor trip, CIAS, or SIAS. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value (400 psia) to ensure a reactor trip, CIAS, and SIAS will occur if required during RCS cooldown and depressurization.

From this reduced setting, the trip setpoint will increase automatically as pressurizer pressure increases, tracking actual RCS pressure until the trip setpoint is reached.

When the trip setpoint has been lowered below the bypass permissive setpoint of 400 psia, the

(continued)

(continued)

BASES (continued)

LCO (continued)

Pressurizer Pressure--Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When RCS pressure rises above the bypass removal setpoint, the bypass is removed.

c.ii Bypass Removal

This LCO requires four channels of Bypass Removal for SIAS Pressurizer Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

Each of the four channels enables and disables the bypass capability for a single channel. Therefore all four bypass removal channels must be OPERABLE to ensure that none of the four automatic trip channels is inadvertently bypassed.

Bypass removal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Because the trip setpoint has a floor value of 300 psia, a channel trip will result if pressure is decreased below this setpoint without bypassing.

The bypass removal ALLOWABLE VALUE was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated for by required shutdown margin.

d. Matrix Logic

This LCO requires six channels of SIAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

Matrix Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

(continued)

(continued)

BASES (continued)

LCO (continued)

The SIAS Matrix Logic only functions to energize or de-energize, or open or close, contacts.

Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

e. Initiation Logic

This LCO requires four channels of SIAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The SIAS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

f. Actuation Logic

This LCO requires two channels of SIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The SIAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. For an automatic actuation it is necessary to have a Containment Pressure--High High signal, coincident with an SIAS. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure--High signal used in the SIAS will initiate

(continued)

(continued)

BASES (continued)

LCO (continued)

before the Containment Pressure--High High. This ensures that a CSAS will not initiate unless required.

a. Manual Actuation

This LCO requires two channels of CSAS Manual Actuation to be OPERABLE in MODES 1, 2, and 3.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CSAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

b. Containment Pressure--High High

This LCO requires four channels of CSAS Containment Pressure--High High to be OPERABLE in MODES 1, 2, and 3.

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is set high enough to allow for first-response ESF Systems (Containment Cooling Systems) to attempt to mitigate the consequences of an accident before resorting to spraying borated water onto containment equipment. The setting is low enough to initiate CSAS in time to prevent containment pressure from exceeding design.

c. Automatic SIAS (Function 1)

This LCO requires four channels of Automatic SIAS input to CSAS to be OPERABLE in MODES 1, 2, and 3.

The Automatic SIAS occurs on Pressurizer Pressure--Low or Containment Pressure--High, and is explained above.

(continued)

(continued)

BASES (continued)

LCO (continued)

d. Matrix Logic

This LCO requires six channels of CSAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

Matrix Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CSAS Matrix Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

e. Initiation Logic

This LCO requires four channels of CSAS Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CSAS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

f. Actuation Logic

This LCO requires two channels of CSAS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CSAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

3. Containment Isolation Actuation Signal

For plants where the SIAS and CIAS are actuated on Pressurizer Pressure--Low or Containment Pressure--High, the SIAS and CIAS share the same input channels, bistables, and matrices and matrix relays. The remainder of the initiation channels, the manual channels, and the Actuation Logic are separate. Since their applicability is also the same, they have identical actions.

a. Manual Actuation

This LCO requires two channels of CIAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CIAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

b. Containment Pressure--High

This LCO requires four channels of CIAS Containment Pressure--High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure--High signal is shared between the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 5).

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup), and not indicative of an off-normal condition. The setting is low enough to initiate the ESF functions when an off-normal

(continued)

(continued)

LCO (continued)

condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

c.i Pressurizer Pressure--Low

This LCO requires four channels of CIAS Pressurizer Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

Pressurizer Pressure--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, 3, and 4.

The ALLOWABLE VALUE for this trip is set low enough to prevent actuating the ESF functions (SIAS and CIAS) during normal plant operation and pressurizer pressure transients. The setting is high enough that with the specified accidents the ESF systems will actuate to perform as expected, mitigating the consequences of the accidents.

The Pressurizer Pressure--Low trip setpoint, which provides a CIAS, SIAS, and RPS trip, may be manually decreased to a floor ALLOWABLE VALUE of 300 psia to allow for a controlled cooldown and depressurization of the RCS without causing a reactor trip, CIAS or SIAS. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value (400 psi) to ensure a reactor trip, CIAS, and SIAS will occur if required during RCS cooldown and depressurization.

From this reduced setting, the trip setpoint will increase automatically as pressurizer pressure increases, tracking actual RCS pressure until the trip setpoint is reached.

When the trip setpoint has been lowered below the bypass removal setpoint of 400 psia, the Pressurizer Pressure--Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in

(continued)

(continued)

BASES (continued)

LCO (continued)

preparation for shutdown cooling. When RCS pressure rises above the bypass removal, the bypass is removed.

c.ii Bypass Removal

This LCO requires four channels of Bypass Removal for CIAS Pressurizer Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

Each of the four channels enables and disables the bypass capability for a single channel. Therefore all four bypass removal channels must be OPERABLE to ensure that none of the four channels are inadvertently bypassed.

Bypass Removal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Because the trip setpoint has a floor value of 300 psia, a channel trip will result if pressure is decreased below this setpoint without bypassing.

The bypass removal ALLOWABLE VALUE was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated by required shutdown margin.

d. Matrix Logic

This LCO requires six channels of CIAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

Matrix Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CIAS Matrix Logic only function to energize or de-energize, or open or close, contacts.

Therefore, these functions have no adjustable

(continued)

(continued)

BASES (continued)

LCO (continued)

trip setpoints with which to associate an ALLOWABLE VALUE.

e. Initiation Logic

This LCO requires four channels of CIAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CIAS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

f. Actuation Logic

This LCO requires two channels of CIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CIAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

4. Containment Cooling Actuation Signal

For plants employing a separate CCAS signal, the CCAS function can be automatically or manually actuated on an SIAS. It can also be manually actuated using two channels of CCAS push buttons, configured similarly to all other ESFAS manual actuations. CCAS therefore shares the SIAS sensor channels, bistables, coincidence matrices, and matrix relays. It has separate manual channels and Actuation Logic.

(continued)

(continued)

BASES (continued)

LCO (continued)

a. Manual CCAS Actuation

This LCO requires two channels of CCAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 2.

The CCAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

b. Manual SIAS Actuation

This LCO requires two channels of SIAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The SIAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

c. Automatic SIAS (Function 1)

This LCO requires four channels of automatic SIAS (function 1) input to CCAS to be OPERABLE in MODES 1, 2, and 3.

The Automatic SIAS which occurs on Pressurizer Pressure--Low or Containment Pressure--High is explained above.

d. Initiation Logic

This LCO requires four channels of CSAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

(continued)

(continued)

BASES (continued)

LCO (continued)

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CCAS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

b. Actuation Logic

This LCO requires two channels of CCAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The CCAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

5. <u>Main Steam Isolation Signal</u>

a. Manual Actuation

This LCO requires two channels of MSIS Manual Actuation to be OPERABLE in MODES 1, 2, and 3.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The MSIS Manual Actuation channels only function to energize or de-energize, or open or close, contacts.

Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

b. SG Pressure--Low

This LCO requires four channels per SG of MSIS SG Pressure--Low to be OPERABLE in MODES 1, 2, and 3.

SG Pressure--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide an MSIS (Function 5) during an excessive steam demand event. An excessive steam demand event causes the RCS to cool down resulting in a positive reactivity addition to the core.

MSIS limits this cooldown by isolating both steam generators if the pressure in either drops below the trip setpoint. A RPS trip on SG Pressure--Low is initiated simultaneously, using the same bistable. The SG Pressure--Low bistable output is also used in the EFAS Logic (Function 7), to aid in determining if an SG is intact.

The SG Pressure--Low trip setpoint may be manually decreased as SG pressure is reduced. This prevents an RPS trip or MSIS actuation during controlled plant cooldown. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value of 200 psia to ensure a reactor trip and MSIS will occur when required.

c. Containment Pressure--High

This LCO requires four channels of Containment Pressure--High to be OPERABLE in MODES 1, 2, and 3.

(continued)

(continued)

BASES (continued)

LCO (continued)

The Containment Pressure--High signal is shared between the SIAS (function 1), CIAS (function 3), and MSIS (function 5).

Containment Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup), and not indicative of an off-normal condition. The setting is low enough to initiate the ESF functions when an off-normal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

d. Matrix Logic

This LCO requires six channels of MSIS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

Matrix Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The MSIS Matrix Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

e. Initiation Logic

This LCO requires four channels of MSIS Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The MSIS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

(continued)

(continued)

BASES (continued)

LCO (continued)

f. Actuation Logic

This LCO requires two channels of MSIS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The MSIS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

6. <u>Recirculation Actuation Signal</u>

a. Manual Actuation

This LCO requires two channels of RAS Manual Actuation to be OPERABLE in MODES 1, 2, 3, and 4.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The RAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

b. RWST Level--Low

This LCO requires four channels of RAS RWST Level--Low to be OPERABLE in MODES 1, 2, and 3.

RWST Level--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The upper limit on the ALLOWABLE VALUE for this trip is set low enough to ensure RAS does not initiate before sufficient water is transferred to the containment sump. Premature recirculation could impair the reactivity control function of safety injection by limiting the amount of boron

(continued)

(continued)

LCO (continued)

injection. Premature recirculation could also damage or disable the recirculation system if recirculation begins before the sump has enough water to prevent air entrainment in the suction. The lower limit on the RWST Level--Low trip ALLOWABLE VALUE is high enough to transfer suction to the containment sump prior to emptying the RWST.

c. Matrix Logic

This LCO requires six channels of RAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

Matrix Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The RAS Matrix Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

d. Initiation Logic

This LCO requires four channels of RAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The RAS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

e. Actuation Logic

This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

(continued)

(continued)

BASES (continued)

LCO (continued)

The RAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

7. Emergency Feedwater Actuation System (EFAS-1 and EFAS-2)

EFAS-1 is initiated by either a low SG level coincident with no low pressure trip present on SG 1, or by a low SG level coincident with a differential pressure between the two generators with the higher pressure in SG 1. EFAS-2 is similarly configured to feed SG 2.

The SG secondary differential pressure is used, in conjunction with an SG Pressure--Low input from each SG, as an input of the EFAS logic where it is used to determine if a generator is intact. The EFAS logic inhibits feeding an SG if a SG Pressure--Low condition exists in that generator, and the pressure in that SG is less than the pressure in the other SG by the Steam Generator Differential Pressure (SGΔP)--High setpoint.

The SGΔP logic thus enables the feeding of an SG in the event that a plant cooldown causes an SG Pressure--Low condition, while inhibiting feeding the other (lower pressure) SG, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the SG channels during normal operation.

The following LCO description applies to both EFAS signals.

a. Manual Actuation

This LCO requires two channels of Manual Actuation to be OPERABLE for each EFAS in MODES 1, 2, and 3.

Manual Actuation channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

(continued)

(continued)

BASES (continued)

LCO (continued)

The EFAS Manual Actuation channels only function to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

b. SG Level--Low

This LCO requires four channels of SG Level--Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

SG Level--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The SG Level--Low EFAS input is derived from the SG Level--Low RPS bistable output. EFAS is thus initiated simultaneously with a reactor trip. The setpoint ensures at least a 20-minute inventory of water remains in the affected SG at reactor trip. Thus, EFAS is initiated well before SG inventory is challenged.

c. SG Differential Pressure--High (SG-1 > SG-2) or (SG-2 > SG-1)

This LCO requires four channels of SG Differential Pressure--High to be OPERABLE for each EFAS in MODES 1, 2, and 3.

SG Differential Pressure--High signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2, and 3.

The ALLOWABLE VALUE for this trip is high enough to allow for small pressure differences and normal instrumentation errors between the SG channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured SG in the event of an MSLB or FWLB while permitting the feeding of the intact SG.

(continued)

(continued)

BASES (continued)

LCO (continued)

d. SG Pressure--Low

This LCO requires four channels of SG Pressure--Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The SG Pressure--Low input is derived from the SG Pressure--Low RPS bistable output. This output is also used as an MSIS input.

SG Pressure--Low signal channels are OPERABLE when they satisfy OPERABILITY requirements 1, 2 and 3.

The ALLOWABLE VALUE for this trip is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide an MSIS (Function 5) during an excessive steam demand event. An excessive steam demand is one indicator of a potentially ruptured SG, thus this EFAS input in conjunction with the SGΔP function prevents the feeding of a potentially ruptured SG.

The SG Pressure--Low trip setpoint may be manually decreased as SG pressure is reduced. This prevents an RPS trip or MSIS actuation during controlled plant cooldown. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value of 200 psi to ensure that a reactor trip and MSIS will occur when required.

e. Matrix Logic

This LCO requires six channels of Matrix Logic to be OPERABLE for each EFAS in MODES 1, 2, and 3.

Matrix Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The EFAS Matrix Logic only functions to energize or de-energize, or open or close, contacts.

(continued)

(continued)

BASES (continued)

LCO (continued)

Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

f. Initiation Logic

This LCO requires four channels of Initiation Logic to be OPERABLE for each EFAS in MODES 1, 2, and 3.

Initiation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The EFAS Initiation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoint with which to associate an ALLOWABLE VALUE.

g. Actuation Logic

This LCO requires one channel of Actuation Logic to be OPERABLE for each EFAS in MODES 1, 2, and 3.

Actuation Logic channels are OPERABLE when they satisfy OPERABILITY requirements 1 and 3.

The EFAS Actuation Logic only functions to energize or de-energize, or open or close, contacts. Therefore, these functions have no adjustable trip setpoints with which to associate an ALLOWABLE VALUE.

[For this facility, the following support systems are required to be OPERABLE to ensure ESFAS Instrumentation System OPERABILITY:]

[For this facility, those required support systems which upon their failure, do not declare the ESFAS Instrumentation System inoperable and their justification are as follows:]

[For this facility, the supported systems impacted by the inoperability of the ESFAS instrumentation and the justification for each declared inoperable are as follows:]

(continued)

BASES (continued)

APPLICABILITY

In MODES 1, 2 and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF system responses to:

1. Close the main steam isolation valves to preclude a positive reactivity addition;

2. Actuate emergency feedwater to preclude the loss of the SGs as a heat sink (in the event the normal feedwater system is not available);

3. Actuate ESF Systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB; and

4. Actuate ESF Systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

In MODES 4, 5, and 6 automatic actuation of these functions is not required because adequate time is available to evaluate plant conditions and respond by manually operating the ESF components if required. ESFAS Manual Actuation capability is required in MODE 4 for SIAS, CIAS, CCAS, and RAS even though automatic actuation is not required. Because of the large number of components actuated by these functions, ESFAS actuation is simplified by the use of the Manual Actuation push buttons.

[At this facility manual, system-level, actuation of CSAS, MSIS, and EFAS is not required in MODE 4 for the following reasons:]

The ESFAS logic must be OPERABLE in the same MODES as the automatic and manual actuations. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Actuation must be OPERABLE.

In MODES 5 and 6, the systems initiated by ESFAS are either reconfigured or disabled for shutdown cooling operation. Accidents in these MODES are slow to develop, and would be mitigated by manual operation of individual components.

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

Several trips have operating bypasses, discussed in the preceding LCO section. The interlocks that allow these bypasses shall be OPERABLE whenever the RPS function they support is OPERABLE.

A Note has been added to provide clarification that each function specified in Table 3.3.2-1 is treated as an independent entity for this LCO, with an independent Completion Time.

ACTIONS

A protection function channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined for each function in the LCO section of the Bases. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis. Typically the drift is found to be small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the trip setpoint is less conservative than the ALLOWABLE VALUE in Table 3.3.2-1, the channel must be declared inoperable immediately, and the appropriate Conditions from Table 3.3.2-1 must be entered immediately.

In the event a channel's trip setpoint is found non-conservative with respect to the ALLOWABLE VALUE, or the transmitter, instrument loop, signal processing electronics, or ESFAS bistable is found inoperable, then all affected functions provided by that channel must be declared inoperable and the LCO Condition entered for the particular protection function affected.

When the number of inoperable channels in a trip function exceeds those specified in one or other related Conditions associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately, if applicable in the current MODE of operation.

(continued)

(continued)

ACTIONS (continued)

<u>Condition A</u>

Condition A is applicable to all ESFAS protection functions. Condition A addresses the situation where one or more channels for one or more functions are inoperable at the same time. The Required Action is to refer to Table 3.3.2-1 immediately and to take the Required Actions for the protection functions affected.

<u>Condition B</u>

Condition B applies to the failure of a single channel of one or more input parameters in the following ESFAS functions:

1. Safety Injection Actuation Signal
   - Containment Pressure--High
   - Pressurizer Pressure--Low

2. Containment Spray Actuation Signal
   - Containment Pressure--High High
   - Automatic SIAS

3. Containment Isolation Actuation Signal
   - Containment Pressure--High
   - Pressurizer Pressure--Low

4. Containment Cooling Actuation Signal
   - Automatic SIAS

5. Main Steamline Isolation Signal
   - SG Pressure--Low
   - Containment Pressure--High

6. Recirculation Actuation Signal
   - RWST Level--Low

7. Emergency Feedwater Actuation System
   - SG Level--Low
   - SG Differential Pressure--High
   - SG Pressure--Low

ESFAS coincidence logic is normally two-out-of-four.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Required Action B.1 is the preferred action as it restores full functional capability of the ESFAS.

If one RPS channel is inoperable, startup or power operation is allowed to continue providing the inoperable channel is placed in bypass or trip within 1 hour (Required Action B.2.1).

The 1-hour Completion Time allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

For plants that have not demonstrated sufficient channel-to-channel independence, the failed channel is restored to OPERABLE status or is placed in trip within 48 hours (Required Action B.2.2.1 or B.2.2.2). Required Action B.2.2.1 restores the full capability of the function. Required Action B.2.2.2 places the function into a one-out-of-three configuration. In this configuration, common-cause failure of dependent channels cannot prevent trip. The 48-hour Completion Time is based on operating experience which has demonstrated that a random failure of a second channel occurring during the 48-hour period is a low-probability event.

Condition C

Condition C applies to the failure of two channels of one or more input parameters in the following ESFAS functions:

1. Safety Injection Actuation Signal
   Containment Pressure--High
   Pressurizer Pressure--Low

2. Containment Spray Actuation Signal
   Containment Pressure--High High
   Automatic SIAS

3. Containment Isolation Actuation Signal
   Containment Pressure--High
   Pressurizer Pressure--Low

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

4. Containment Cooling Actuation Signal
   Automatic SIAS

5. Main Steamline Actuation Signal
   SG Pressure--Low
   Containment Pressure--High

6. Recirculation Actuation Signal
   RWST Level--Low

7. Emergency Feedwater Actuation System
   SG Level--Low
   SG Differential Pressure--High
   SG Pressure--Low.

Required Action C.1 is the preferred action as it improves the functional reliability of the ESFAS.

With two inoperable channels, power operation may continue provided one inoperable channel is placed in bypass, and the other channel is placed in trip within 1 hour. With one channel of protective instrumentation bypassed, the ESFAS function is in two-out-of-three logic in the bypassed input parameter, but with another channel failed, the ESFAS may be operating with a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the ESFAS function in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, ESFAS actuation will occur.

For plants that have not demonstrated sufficient channel-to-channel independence, the bypassed channel should be restored to OPERABLE status within 48 hours, for reasons similar to those stated under Condition B. After one channel is restored to OPERABLE, the provisions of Condition B still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action C.2.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

<u>Condition D</u>

Condition D applies if one Matrix Logic channel is inoperable. Since matrix power supplies in a given matrix (e.g. AB, BC, etc.) are common to all ESFAS functions, a single power-supply failure may affect more than one matrix.

Loss of a single vital instrument bus will de-energize one of the two matrix power supplies in up to three matrices. This is considered a single matrix failure, providing the matrix relays associated with the failed power supplies de-energize as required. [For this facility, the consequences for the matrix relays not de-energizing as required are as follows:]

The channel must be restored to OPERABLE status within 48 hours. This provides the operator with time to take appropriate actions and still assure that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second Matrix Logic channel is low during any given 48-hour period. If the channel cannot be restored to OPERABLE status within 48 hours, Condition J is entered.

<u>Condition E</u>

Condition E applies to one Manual Actuation or Initiation Logic Channel inoperable for CSAS, MSIS, or EFAS. It is identical to Condition K for the other ESFAS functions except for the shutdown track invoked.

The channel must be restored to OPERABLE status within 1 hour. The Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the remaining OPERABLE channels.

Failure of a single Initiation Logic channel may open one contact affecting both Actuation Logic channels. For the purposes of this specification, the Actuation Logic is not inoperable. This prevents the need to enter LCO 3.0.3 in the event of an Initiation Logic channel failure. The Actions differ from those involving one RPS manual channel inoperable, because in the case of the RPS, opening RTCBs can be easily performed and verified. Opening an initiation

(continued)

(continued)

ACTIONS (continued)

relay contact is more difficult to verify, and subsequent shorting of the contact is always possible.

Condition F

Condition F applies to the failure of both Initiation Logic channels affecting the same trip leg for CSAS, MSIS, or EFAS. It is identical to Condition L for the other ESFAS functions except for the shutdown track invoked.

In this case, the Actuation Logic channels are not inoperable, since they are in one-out-of-two logic, and capable of performing as required. This prevents the need to enter LCO 3.0.3 in the event of a matrix or vital bus power failure.

Both Initiation Logic channels in the same trip leg will de-energize if a matrix power supply or vital instrument bus is lost. This will open the Actuation Logic contacts, satisfying the Required Action to open at least one set of contacts in the affected trip leg. Indefinite operation in this condition is prohibited because of the difficulty of assuring the contacts remain open under all conditions. Thus, the channel must be restored to OPERABLE status within 48 hours. This provides the operator with time to take appropriate actions and still assure that the risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that the probability of a random failure of a second channel is low during any given 48-hour period. If the channel cannot be restored to OPERABLE status with 48 hours, Condition J is entered.

Of greater concern is the failure of the initiation circuit in a non-trip condition, e.g. due to two initiation relay failures. With one failed, there is still the redundant contact in the trip leg of each Actuation Logic. With both failed in a non-trip condition, the ESFAS function is lost. To prevent this, immediate opening of at least one contact in the affected trip leg is required. If the required contact has not opened, as indicated by annunciation or trip leg current lamps, manual actuation of the affected trip leg

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

contacts may be attempted. Caution must be exercised, since depressing the wrong ESFAS push buttons may result in an ESFAS actuation.

Condition G

Condition G applies to CSAS, MSIS, or EFAS Actuation Logic. It is identical to Condition M for the other ESFAS functions except for the shutdown track invoked.

The channel must be restored to OPERABLE status within 1 hour. The Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

Failure of a single Initiation Logic channel, matrix channel power supply, or vital instrument bus may open one or both contacts in the same trip leg in both Actuation Logic channels. For the purposes of this specification, the Actuation Logic is not inoperable. This prevents the need to enter LCO 3.0.3 in the event of a vital bus, matrix, or initiation channel failure.

Required Action G.1 is modified by a Note to indicate that one channel of Actuation Logic may be bypassed for up to 1 hour for surveillance testing provided the other channel is OPERABLE.

[For this facility, justification for this Note is as follows:].

Condition H

Condition H applies to one Pressurizer Pressure--Low automatic bypass removal channel inoperable. This function is shared with the RPS Pressurizer Pressure--Low bypass removal.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. Condition H applies to failures in one of the four sensor subsystems, including sensors, bistables, and associated equipment.

(continued)

(continued)

ACTIONS (continued)

Failure in the actuation subsystems, including the manual bypass key switches, is considered Actuation Logic failure, and is addressed in Conditions G and M.

In Condition H it is permissible to continue operation with one bypass permissive removal channel failed, providing the bypass is disabled. This can be accomplished by removing the bypass with the manual bypass keyswitch which disables the bypass in both trains. Since the bypass function must be manually enabled, the bypass permissive function will not by itself cause an undesired bypass insertion. Alternatively, the bypass may be disabled by defeating the bypass permissive input in one of the four channels to the two-out-of-four bypass removal logic, placing the bypass removal feature in one-out-of-three logic. Thus any of the remaining three channels is capable of removing the bypass feature when the bypass enable conditions are no longer valid.

If the bypass removal feature in the inoperable channel cannot be defeated, action to address the inoperability of the affected automatic trip channel must be taken. Required Action H 3.1, Required Action H.3.2.1, and Required Action H.3.2.2, are equivalent to the Required Actions for a single automatic trip channel failure (Condition B). The 1-hour and 48-hour Completion Times have the same basis as discussed for Condition B.

Condition I

Condition I applies to two inoperable bypass removal channels. The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This Condition applies to failures in two of the four sensor subsystems. With two of the four sensor subsystems failed in a non-conservative direction (enabling the bypass function), the bypass removal feature is in two-out-of-two logic. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures, and are addressed in Conditions G and M.

In Condition I it is permissible to continue operation with two bypass permissive channels failed, providing the bypasses are disabled in a similar manner as discussed for Condition H.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

If the failed bypasses cannot be disabled, actions to address the inoperability of the affected automatic trip channels must be taken. Required Action I 3.1 and Required Action I 3.2, are equivalent to the Required Actions for two automatic trip channel failures (Condition C). Also similar to Condition C, after one set of inoperable channels is restored the provisions of Condition H apply to the remaining inoperable channel, with the Completion Time measured from the point of the initial bypass channel failure. The 1-hour and 48-hour Completion Times have the same basis as discussed for Condition C.

Condition J

If the Required Actions and associated Completion Times of Conditions B, C, D, E, F, G, H, or I cannot be met, the plant must be brought to a MODE in which the Required Actions do not apply. The 6 hours allowed to bring the plant to MODE 3 and 6 additional hours to reach MODE 4 are reasonable, based on operating experience, to reach the required MODES from full power in an orderly manner and without challenging plant systems.

Condition K

Condition K is identical to Condition E except for the shutdown track invoked. It applies to one Initiation Logic or manual actuation channel inoperable for SIAS, CIAS, CCAS, and RAS functions which must be OPERABLE in MODES 1 through 4. The shutdown track imposed by Condition N requires entry into MODE 5, in which the LCO does not apply.

Condition L

Condition L is identical to Condition F except for the shutdown track invoked. It applies to two Initiation Logic channels inoperable for ESFAS functions which must be OPERABLE in MODES 1 through 4 ([SIAS, CIAS, CCAS, and RAS]). The shutdown track imposed by Condition N requires entry into MODE 5, in which the LCO does not apply.

Condition M

Condition M is identical to Condition G, except for the shutdown track invoked. It applies to one Actuation Logic

(continued)

(continued)

ACTIONS (continued)

channel inoperable for SIAS, CIAS, CCAS, and RAS functions which must be OPERABLE in MODES 1 through 4. The shutdown track imposed by Condition N requires entry into MODE 5, in which the LCO does not apply.

Condition N

If the Required Actions and associated Completion Times of Conditions K, L, or M are not met, the plant must be brought to a MODE in which the Required Actions do not apply. The 6 hours allowed to bring the plant to MODE 3 and 36 additional hours to reach MODE 5 is reasonable, based on operating experience, to reach the required MODES from full power in an orderly manner and without challenging plant systems.

Condition O

Condition O is applicable to each one of the ESFAS functions presented in Table 3.3.2-1.

Required Action O.1 verifies that the Required Actions have been initiated for those supported systems declared inoperable because of the inoperability of the support channel(s) within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination.

Required Action O.1 ensures that those identified Required Actions associated with supported systems impacted by the inoperability of channel(s) associated with each ESFAS function have been initiated. This can be accomplished by entering the supported systems LCOs or independently as a group of Required Actions needed to be initiated every time Condition O is entered. [For this facility, the identified supported systems Required Actions associated with each ESFAS function are as follows:]

Required Action O.2 verifies that all required support or supported features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 should be immediately entered. However, if the

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

support or supported feature LCOs take into consideration the loss-of-function situation then LCO 3.0.3 may not need to be entered.

SURVEILLANCE REQUIREMENTS

The SRs for any particular ESFAS function are found in the SR column of Table 3.3.2-1, for that function. Most functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response-time testing.

In order for a facility to take credit for topical reports for the basis for justifying Surveillance Frequencies, topical reports should be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that facility.

SR 3.3.2.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or something even more serious. CHANNEL CHECK will detect gross channel failure, thus it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off-scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off-scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale.

(continued)

(continued)

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance interval, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited to 12 hours. Since the probability of two random failures in redundant channels in any 12-hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

<u>SR 3.3.2.2 and SR 3.3.2.3</u>

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed.

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SR 3.3.2.2, SR 3.3.2.3, and SR 3.3.2.4 tests the entire ESFAS from the bistable input through the actuation of the individual subgroup relays. These overlapping tests are described in Reference 1. SR 3.3.2.2 and SR 3.3.2.3 are normally performed together and in conjunction with RPS testing. SR 3.3.2.4 is performed on a semiannual basis, and verifies that the subgroup relays are capable of actuating their respective ESF components when de-energized.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components. SR 3.3.2.2 and SR 3.3.2.3 include:

<u>Bistable Tests</u>. "As found" and "as left" values for bistable trip setpoints are recorded. The bistable setpoints must be found to trip within the ALLOWABLE VALUES specified in the LCO. The difference between the current "as found" and the previous "as left" values must be consistent with the drift allowance used in the setpoint analysis. Whenever these tolerances are not met, a recalibration can be performed to establish OPERABILITY of the channel. However, repeated consecutive failures would be indicative of a failure that cannot be corrected by recalibration alone.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

A test signal is then superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS channel trip channel bypassed.

Matrix Logic Tests. This test is performed one matrix at a time. It verifies that a coincidence in the two input channels for each function removes power to the matrix relays. During testing, power is applied to the matrix relay test coils, and prevents the matrix relay contacts from assuming their energized state. This test will detect any short circuits around the bistable contacts in the coincidence logic, such as may be caused by faulty bistable relay or trip channel bypass contacts.

Trip Path (Initiation Logic) Tests. These tests are similar to the Matrix Logic tests, except that test power is withheld from one matrix relay at a time, allowing the initiation circuit to de-energize, opening one contact in each Actuation Logic channel.

The initiation circuit lockout relay must be reset (except for EFAS, which lacks initiation circuit lockout relays) prior to testing the other three initiation circuits, or a reactor trip may result.

Automatic Actuation Logic operation is verified during Initiation Logic testing by verifying that current is interrupted in each trip leg in the selective two-out- of-four actuation circuit logic whenever the initiation relay is de-energized. A Note is added to indicate that testing of Actuation Logic shall include verification of the proper operation of each initiation relay.

The Surveillance Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

SR 3.3.2.4

Individual ESFAS subgroup relays must also be tested, one at a time, to verify the individual ESFAS components will actuate when required. Proper operation of the individual subgroup relays is verified by de-energizing these relays one at a time using an ARC-mounted test circuit. Proper

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

operation of each component actuated by the individual relays is thus verified without the need to actuate the entire ESFAS function.

The [184-day] surveillance interval is based on operating experience and ensures individual relay problems can be detected within this time frame. Considering the large number of similar relays in the ARC, and the similarity in their use, a large test sample can be assembled to verify the validity of this interval. [For this facility, the actual justification based on the test sample is as follows:]

Some components cannot be tested at power since their actuation might lead to plant trip or equipment damage. Reference [illegible] lists these relays exempt from testing at power, with an explanation of the reason for each exception. Relays not tested at power must be tested in accordance with Note 2 in SR 3.3.2.4.

SR 3.3.2.5

SR 3.3.2.5 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.2.2 except SR 3.3.2.5 is performed within 92 days prior to startup and is only applicable to bypass functions. Since the Pressurizer Pressure--Low bypass is identical for both the RPS and ESFAS, this is the same surveillance performed for the RPS in SR 3.3.1.14.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass permissives is critical during plant heatups because the bypasses may be in place prior to entering MODE 3, but must be removed at the appropriate points during plant startup to enable the ESFAS function. Consequently, just prior to startup is the appropriate time to verify bypass function operability. Once the bypasses are removed the bypasses must not fail in such a way that the associated ESFAS function is inappropriately bypassed. This feature is verified by SR 3.3.2.2.

The allowance to conduct this test within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 8).

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.6

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to the measured parameter with the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive tests, to ensure that the instrument channel remains operational with the setpoint within the assumptions of the plant-specific setpoint analysis. Transmitter "as found" and "as left" values are recorded and used to verify drift assumptions. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint errors are within the assumptions of the plant-specific setpoint analysis. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis.

Recalibration restores operability of an otherwise functional component found to have errors larger than assumed by the setpoint analysis. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure which cannot be corrected by recalibration.

Field transmitters may be calibrated in place, removed and calibrated in a laboratory, or replaced with an equivalent laboratory-calibrated unit.

The Surveillance Frequency is based upon the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.2.7

A CHANNEL FUNCTIONAL TEST is performed on the manual ESFAS actuation circuitry, de-energizing relays and providing manual actuation of the function.

This test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed. The 18-month Frequency was developed considering it was prudent that these Surveillances only be performed during a plant

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

outage. This was due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 18-month Frequency.

SR 3.3.2.8

This Surveillance ensures that the train actuation response times are verified on a STAGGERED TEST BASIS. The response time values are provided in the FSAR, and are the maximum values assumed in the safety analyses.

Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor, to the point at which the equipment in both trains reaches the required functional state, e.g., pumps at rated discharge pressure, valves in full open or closed position. [For this facility, response time testing acceptance criteria are contained in the following document:]

The test may be performed in one measurement on overlapping segments, with verification that all components are measured.

The 18-month Frequency was developed because many Surveillances can only be performed during a plant outage. Response-time tests are conducted on a 18-month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n x 18 months, where n is the number of channels in the function. Testing of the final actuation devices, which make up the bulk of the response time, is included in the testing of each channel. Therefore, staggered testing results in response time verification of these devices every 18 months. The 18-month Frequency is based upon plant operating experience which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Response times cannot be determined at power since equipment operation is required.

(continued)

BASES (continued)

REFERENCES

1. [Unit Name] FSAR, Section [7.3], "[Instrumentation and Control]."

2. Code of Federal Regulations, Title 10, Part 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."

3. [Unit Name] [NRC Staff Safety Evaluation Report, (Date)].

4. Institute of Electrical and Electronic Engineers, IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

5. [Unit Name] FSAR, Section [15], "[Accident Analysis]."

6. [Unit Name] "[Plant Protection System Selection of Trip Setpoint Values]."

7. Title 10, Code of Federal Regulations, Appendix A, "General Design Criteria for Nuclear Power Plants."

8. CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," May 1986, including Supplement 1, March 1989.

B 3.3 INSTRUMENTATION

B 3.3.3 <u>Emergency Diesel Generator (EDG) Loss of Voltage Start (LOVS)</u> (Analog and Digital)

BASES

BACKGROUND

The EDGs provide a source of emergency power when offsite power is either unavailable or insufficiently stable to allow safe plant operation. Undervoltage protection will generate a LOVS in the event a loss-of-voltage or degraded-voltage condition occurs. There are two LOVS functions for each 4.16kV vital bus.

Four undervoltage relays with inverse time characteristics are provided on each 4.16kV Class 1E instrument bus for the purpose of detecting a sustained undervoltage condition or a loss of bus voltage. The relays are combined in a two-out-of-four logic to generate a LOVS if the voltage is below 75% for a short time or below 90% for a long time. The LOVS-initiated actions are described in Reference 1.

<u>Trip Setpoints and ALLOWABLE VALUE</u>

The trip setpoints and ALLOWABLE VALUES are based on the analytical limits presented in Reference 2. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, ALLOWABLE VALUES specified in SR 3.3.3 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in Reference 3. The actual nominal trip setpoint is normally still more conservative than that required by the plant-specific setpoint calculations. If the measured setpoint does not exceed the documented surveillance test acceptance criteria, the undervoltage relay is considered OPERABLE.

Setpoints in accordance with the ALLOWABLE VALUE will assure that Safety Limits (SLs) are not violated during anticipated operational occurrences (AOOs) and that the consequences of

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident, and the equipment functions as designed.

The undervoltage protection scheme has been designed to protect the plant from spurious trips caused by the offsite power source. This is made possible by the [inverse voltage time] characteristics of the relays used. A complete loss of offsite power will result in approximately a [1]-second delay in LOVS actuation. The EDG starts and is available to accept loads within a [10]-second time interval of Engineered Safety Feature Actuation System (ESFAS) or LOVS. Emergency power is established within the maximum time delay assumed for each event analyzed in the accident analysis (Ref. [illegible]).

Since there are four protective channels in a two-out-of-four trip logic for each division of the 4.16kV power supply, no single failure will cause or prevent protective system actuation. This arrangement meets IEEE Standard 279-1971 criteria (Ref. [illegible]).

APPLICABLE SAFETY ANALYSES

The EDG LOVS is required for engineered safety feature (ESF) systems to function in any accident with a loss of offsite power. Its design basis is that of the ESFAS.

Accident analyses credit the loading of the EDG based on a loss of offsite power during a loss-of-coolant accident (LOCA). The actual EDG start has historically been associated with the ESFAS actuation. The diesel loading has been included in the delay time associated with each safety system component requiring EDG-supplied power following a loss of offsite power. The analysis assumes a nonmechanistic EDG loading, which does not explicitly account for each individual component of the loss of power detection and subsequent actions. [At this facility, the total actuation time for the limiting systems is as follows:] This delay time includes contributions from the EDG start, EDG loading, and Safety Injection System component actuation. The response of the EDG to a loss of power must be demonstrated to fall within this analysis response time when including the contributions of all portions of the delay.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

The required channels of LOVS, in conjunction with the ESF systems powered from the EDGs, provide plant protection in the event of any of the analyzed accidents discussed in Reference 2, in which a loss of offsite power is assumed. LOVs channels are required to meet the redundancy and testability requirements of GDC 21 in 10 CFR 50, Appendix A (Ref. 5).

The delay times assumed in the safety analysis for the ESF equipment include the [10]-second EDG start delay and the appropriate sequencing delay, if applicable. The response of the EDG to a loss of power must be demonstrated to fall within this analysis response time. The response times for ESFAS-actuated equipment in LCO 3.3.2 include the appropriate EDG loading and sequencing delay.

The EDG LOVS channels satisfy Criterion 3 of the NRC Interim Policy Statement.

LCO

The LCO for the LOVS requires that four channels per bus of each LOVS instrumentation function be OPERABLE in MODES 1, 2, 3, and 4. The LOVS supports safety systems associated with the ESFAS. In MODES 5 and 6, the four channels must be OPERABLE whenever the associated EDG is required to be OPERABLE to ensure that the automatic start of the EDG is available when needed.

The LOVS trip functions are considered OPERABLE when:

1. All channel components necessary to provide a LOVS actuation are functional and in service;

2. Channel measurement uncertainties are known (via test, analysis, or design information) to be within the assumptions of the setpoint calculations; and

3. Required Surveillance testing is current and has demonstrated performance within each Surveillance test acceptance criteria.

Actions allow maintenance (trip channel) bypass of individual channels, but the bypass activates interlocks that prevent operation with a second channel in the same

(continued)

(continued)

BASES (continued)

LCO (continued)

function bypassed. Plants are restricted to 48 hours in a trip channel bypass condition before either restoring the function to four-channel operation (two-out-of-four logic), or placing the channel in trip (one-out-of-three logic). At plants where adequate channel-to-channel independence has been demonstrated, specific exceptions have been approved by the NRC staff to permit one of the two-out-of-four channels to be bypassed for an extended period of time.

Loss of LOVS function could result in the delay of safety system initiation when required. This could lead to the violation of the SLs during certain AOOs, or unacceptable consequences during accidents. During the loss of offsite power, which is an AOO, the EDG powers the motor-driven auxiliary feedwater pumps. Failure of these pumps to start would leave only the one turbine-driven pump, as well as an increased potential for a loss of decay heat removal through the secondary system.

Only ALLOWABLE VALUES are specified for each function in the LCO. Nominal trip setpoints are specified in the plant-specific setpoint calculations. The nominal setpoints are selected to ensure that the setpoint measured by CHANNEL FUNCTIONAL TESTS does not exceed the ALLOWABLE VALUE if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within the ALLOWABLE VALUE, is acceptable provided that operation and testing is consistent with the assumptions of the plant-specific setpoint calculation. Each ALLOWABLE VALUE specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the plant protection system selection of trip setpoint values (Ref. 3).

[For this facility, the relay configuration is as follows:]

[For this facility, the trip meets single-failure criterion for single-phasing events as follows:]

[For this facility, the time-delay setpoint is controlled as follows:]

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, the basis for ALLOWABLE VALUES is as follows:]

[For this facility, the following support systems are required OPERABLE to ensure EDG LOVS instrumentation OPERABILITY:]

[For this facility, those required support systems which, upon their failure, do not result in the EDG LOVS instrumentation being declared inoperable and their justification are as follows:]

[For this facility, the supported systems impacted by the inoperability of the EDG LOVS instrumentation and the justification of whether or not each supported system is declared inoperable are as follows:]

APPLICABILITY

The EDG LOVS actuation function is required in MODES 1, 2, 3, and 4 because ESF functions are designed to provide protection in these modes. Actuation in MODE 5 or 6 is required whenever the required EDG must be OPERABLE, so that it can perform its function on a loss of power or degraded power to the vital bus.

A Note has been added to provide clarification that for this LCO, each function is treated as an independent entity with an independent Completion Time.

ACTIONS

A LOVS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined in the LCO section of the Bases. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the instrument is set up for adjustment to bring it within specification. If the trip setpoint is less conservative than the ALLOWABLE VALUE, the channel must

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

be declared inoperable immediately, and the appropriate Conditions must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the ALLOWABLE VALUE, or the channel is found inoperable, then all affected functions provided by that channel must be declared inoperable and the LCO Condition entered. Since the required channels are specified on a per EDG basis, the Conditions may be entered separately for each EDG.

When the number of inoperable channels in a trip function exceeds those specified in one or other related Conditions associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately, if applicable in the current MODE of operation.

Condition A

Condition A applies if one channel is inoperable for one or more functions per EDG bus.

Restoring the channel to OPERABILITY (Required Action A.1) is the preferred action because it restores full functional capability of the LOVS. If the channel cannot be restored to OPERABLE status, the affected channel should either be bypassed or tripped within 1 hour (Required Action A.2.1).

Placing this channel in either condition ensures that logic is in a known configuration. In trip, the LOVS logic is one out of three. In bypass, the LOVS logic is two out of three, and interlocks prevent bypass of a second channel for the affected function. The 1-hour Completion Time is sufficient to perform these Required Actions.

Once Required Action A.2.1 has been complied with, Required Action A.2.2.1 allows 48 hours to repair the inoperable channel for those plants that have not demonstrated sufficient channel-to-channel independence on this function. If the channel cannot be restored to OPERABLE status, it must be tripped in accordance with Required Action A.2.2.2. The time allowed to repair or trip the channel is reasonable to repair the affected channel, while ensuring that the risk involved in operating with the inoperable channel is

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

acceptable. The 48-hour Completion Time is based upon operating experience, which has demonstrated that a random failure of a second channel is a rare event during any given 48-hour period.

Condition B

Restoring at least one channel to OPERABLE status is the preferred action (Require Action B.1). If the channel cannot be restored to OPERABLE status within 1 hour, the affected EDG(s) and other associated supported systems should be declared inoperable (Required Action B.2) unless one affected channel is bypassed and the other is tripped, in accordance with Required Action B.3.1. This places the function in one-out-of-two logic. The 1-hour Completion Time is sufficient to perform the Required Actions.

Once Required Action B.3.1 has been complied with, Required Action B.3.2 allows 48 hours to repair the bypassed inoperable channel for those plants that have not demonstrated sufficient channel-to-channel independence on this function.

After one channel is restored to OPERABLE, the provisions of Condition A still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action B.3.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.

Condition C

Condition C applies if the Required Actions and associated Completion Times are not met, or if more than two of the channels are inoperable for one or more functions per EDG bus.

Required Action C.1 declares immediately the associated EDG(s) inoperable and LCO 3.8.1, "AC Sources Operating," or LCO 3.8.2, "AC Sources Shutdown," is immediately entered. Also, other supported systems, affected by LOVs channel inoperability are declared inoperable and the corresponding LCOs entered. [For this facility, the supported systems impacted by LOVs channel inoperability are as follows:]

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition D

Condition D is applicable to each of the EDG LOVs functions.

Required Action D.1 verifies that the Required Actions have been initiated for those supported systems declared inoperable because of the inoperability of the support channel(s) within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination.

Required Action D.1 ensures that those identified Required Actions associated with supported systems impacted by the inoperability of channel(s) associated with each EDG LOVs function have been initiated. This can be accomplished by entering the supported systems LCOs. [Alternatively, the appropriate Required Actions for the supported systems may be listed in the Required Actions for Condition D of this LCO.]

[For this facility, the identified supported systems Required Actions associated with each EDG LOVS function are as follows:]

Required Action D.2 verifies that all required support or supported features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 should be immediately entered. However, if the support or supported feature LCO takes into consideration the loss-of-function situation then LCO 3.0.3 may not need to be entered.

SURVEILLANCE REQUIREMENTS

The following SRs apply to each EDG LOVS function.

SR 3.3.3.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the indicated output of the potential transformers that feed the LOVS undervoltage

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

relays. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two channels could be an indication of excessive drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If the channels are within the match criteria, it is an indication that the channels are OPERABLE.

The surveillance interval, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited to 12 hours. Since the probability of two random failures in redundant channels in any 12-hour period is extremely low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

SR 3.3.3.2

A CHANNEL FUNCTIONAL TEST is performed every 31 days to ensure that the entire channel will perform its intended function when needed.

The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given function in any 31-day interval is a rare event.

[For this facility, a CHANNEL FUNCTIONAL TEST constitutes the following:]

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.3

SR 3.3.3.3 is the performance of a CHANNEL CALIBRATION every 18 months. The CHANNEL CALIBRATION verifies the accuracy of each component within the instrument channel. This includes calibration of the undervoltage relays and demonstrates that the equipment falls within the specified operating characteristics defined by the manufacturer. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint errors are within the assumptions of the plant-specific setpoint analysis. Recalibration restores OPERABILITY of an otherwise functional component that does not meet these criteria. Repeated failures of the same channel over a relatively small number of test intervals, however, must be considered as potentially indicative of a deterministic failure that cannot be corrected by recalibration. Completion of this test results in the channel being properly adjusted and expected to remain within the "as found" tolerance assumed by the setpoint analysis until the next scheduled surveillance. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis in Reference 3. The setpoints, as well as the response to a loss-of-voltage and degraded-voltage test, shall include a single-point verification that the trip occurs within the required delay time as shown in Reference 1. The Surveillance Frequency is based upon the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

REFERENCES

1. [Unit Name] FSAR, Section [8.3], "[Onsite Power Systems]."

2. [Unit Name] FSAR, Section [15], "[Accident Analysis]."

3. [Unit Name] "[Plant Protection System Selection of Trip Setpoint Values.]"

4. IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

5. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

B 3.3 INSTRUMENTATION

B 3.3.4 Miscellaneous Actuation Instrumentation (MAI) (Analog)

BASES

BACKGROUND

This LCO encompasses those plant-specific instrumentation channels which perform actuation functions required for plant protection, but are not otherwise included in LCO 3.3.2, "Engineered Safety Feature Actuation System (ESFAS)" or LCO 3.3.3, "Emergency Diesel Generator Loss of Voltage Start." Specifically included are those non-Nuclear Steam Supply System functions which, because of differences in purpose, design, and operating requirements, are not included in LCO 3.3.2 and LCO 3.3.3. Details of this LCO are for illustration only. Individual plants shall include those functions and LCO requirements applicable to them. The MAI in this LCO includes:

1. Containment Purge Isolation Signal (CPIS);

2. Control Room Isolation Signal (CRIS);

3. Chemical and Volume Control System (CVCS) Isolation Signal; and

4. Shield Building Filtration Actuation Signal (SBFAS).

These systems are addressed in References 2 and 3. A brief description of each follows:

1. Containment Purge Isolation Signal

The CPIS provides protection from radioactive contamination in the containment in the event a fuel assembly should be severely damaged during handling.

The CPIS will detect any abnormal amounts of radioactive material in the containment and will initiate purge valve closure to limit the release of radioactivity to the environment. The containment purge supply and exhaust valves are closed on a CPIS, when a high radiation in containment is detected.

The CPIS includes two independent, redundant actuation subsystems. Where two isolation control valves are

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

provided for a single containment penetration, each valve is controlled by a separate actuation subsystem. Where one valve is available, a single actuation subsystem initiates valve closure. One train also isolates the containment air exhaust fan, whereas the other train isolates the containment air supply fan. A list of actuated valves and an additional description of the CPIS is presented in Reference 1. Both trains of CPIS are actuated on a two-out-of-four coincidence from the same four containment radiation sensor subsystems. Containment purge isolation also occurs on a Containment Isolation Actuation Signal (CIAS). This function is addressed by LCO 3.3.2, "ESFAS Instrumentation."

2. Control Room Isolation Signal

The CRIS terminates the supply of outside air to the control room and initiates actuation of the Emergency Filtration System to minimize operator radiation exposure. The CRIS includes two independent, redundant actuation trains. Each train employs the same two sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. These sensors are not considered redundant because they detect different types of activity. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment. Actuating either train will perform the intended function. Control room isolation also occurs on a SIAS.

3. Chemical and Volume Control System Isolation Signal

The CVCS isolation signal provides protection from radioactive contamination as well as personnel and equipment protection in the event of a letdown line rupture outside containment.

Each of the two actuation subsystems isolate a separate letdown isolation valve in response to a high pressure condition [4.3] psig in either the west penetration room or letdown heat exchanger room. Two pressure detectors in each of these rooms feed the

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

four sensor subsystems. On a two-out-of-four coincidence, both actuation subsystems will actuate.

4. Shield Building Filtration Actuation Signal

[For this facility, the function of the SBFAS is as follows:]

Trip Setpoints and ALLOWABLE VALUES

The trip setpoints are the nominal values at which the bistables are set. Any bistable is considered to be properly adjusted when the "as left" value is within the band for channel calibration accuracy, i.e. ± (Rack Calibration + Comparator Setting Accuracy).

Trip setpoints used in the bistables are based on the analytical limits stated in Reference 3. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift, ALLOWABLE VALUES specified in Table 3.3.4-1 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 4). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the ALLOWABLE VALUE to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the Surveillance interval. If the measured setpoint does not exceed the ALLOWABLE VALUE, the bistable is considered OPERABLE.

The ALLOWABLE VALUES listed in Table 3.3.4-1 are based upon the methodology described in Reference 4, which incorporates all of the known uncertainties applicable for each channel. Setpoints in accordance with the ALLOWABLE VALUE will assure that Safety Limits are not violated during anticipated operational occurrences (AOOs), and the consequences of Design Basis Accidents will be acceptable, providing the

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

plant is operated from within the LCOs at the onset of the AOO or accident, and the equipment functions as designed.

The ALLOWABLE VALUES listed in Table 3.3.4-1 are based upon the methodology described in Reference 4, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

Each channel can be tested on line to verify that the signal processing equipment and setpoint accuracy is within the specified allowance requirements of Reference 2. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated.

APPLICABLE SAFETY ANALYSES

1. <u>Containment Purge Isolation Signal</u>

   The CPIS is required to isolate the containment purge valves in the event of the fuel handling accident in containment, as described in Reference 3.

2. <u>Control Room Isolation Signal</u>

   The CRIS, in conjunction with the Control Room Emergency Air Cleanup System (CREACS) maintains the control room atmosphere within conditions suitable for prolonged occupancy throughout the duration of any one of the accidents discussed in Reference 3. The radiation exposure of control room personnel, through the duration of any one of the postulated accidents, does not exceed the limits set by GDC 19 of Appendix A to 10 CFR 50. Since the two radiation monitoring channels are not truly redundant, failure of a single radiation monitoring channel can inhibit CRIS for certain events. [At this facility, the CRIS does not need to respond in these cases for the following reasons:]

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

3. Chemical and Volume Control System Isolation Signal

The CVCS Isolation Signal is redundant to the SIAS for letdown line breaks outside containment. In addition, an excess flow check valve is located in containment just downstream of the regenerative heat exchanger, which isolates letdown when flow exceeds 200 gpm. [At this facility, the provision of two sensors in each room in a two-out-of-four logic configuration satisfies the single failure criterion as follows:]

4. Shield Building Filtration Actuation Signal

[At this facility, the safety analyses applicable to SBFAS is as follows:]

The MAI satisfies the requirements of Criterion 3 of the NRC Interim Policy Statement.

LCO

MAI channels are OPERABLE when the applicable criteria below are met:

1. All channel components necessary to provide an initiation signal are functional and in service. For sampling systems, OPERABILITY requires correct valve lineups, sample pump operation, and filter motor operation as well as detector OPERABILITY, if these supporting features are necessary for trip to occur under the conditions assumed by the safety analysis or setpoint analysis;
2. Channel measurement uncertainties are known via test, analysis, or design information to be within the assumptions of the setpoint calculations; and
3. Required Surveillance testing is current and has demonstrated performance within each Surveillance test's acceptance criteria.

Only the ALLOWABLE VALUES are specified for each trip function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its ALLOWABLE VALUE, is acceptable provided that the difference

(continued)

(continued)

LCO (continued)

between the nominal trip setpoint and the ALLOWABLE VALUE is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses. Each ALLOWABLE VALUE specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 4).

The bases for the LCO on these functions are:

1. <u>Containment Purge Isolation Signal</u>

   a. Manual Actuation

   The LCO on Manual Actuation backs up the automatic trips and ensures operators have the capability to rapidly initiate the CPIS function if any parameter is trending towards its setpoint. Both available channels must be OPERABLE to ensure that a single failure will not disable the function.

   Manual Actuation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

   b. Containment Radiation--High

   The LCO on the radiation channels requires that all four be OPERABLE.

   Containment Radiation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1, 2, and 3.

   [For this facility, the basis for the Containment Radiation--High ALLOWABLE VALUE is as follows:]

   c. Actuation Logic

   Both trains of Actuation Logic must be OPERABLE to assure that no single random failure can prevent automatic actuation. If one fails, it must be restored to OPERABLE status.

(continued)

BASES (continued)

LCO (continued)

Actuation Logic channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

2. Control Room Isolation Signal

a. Manual Actuation

The LCO on Manual Actuation backs up the automatic trips and ensures operators have the capability to rapidly initiate the CRIS function if any parameter is trending towards its setpoint. Both available channels must be OPERABLE to ensure that a single failure will not disable the function.

Manual Actuation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

b. Airborne Radiation

Both channels of Airborne Radiation channel are required to be OPERABLE to ensure the control room isolates on either high iodine and high particulate or gaseous concentration.

Airborne Radiation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1, 2, and 3.

[For this facility, the basis for the Airborne Radiation ALLOWABLE VALUE is as follows:]

c. Actuation Logic

Both trains of Actuation Logic must be OPERABLE to assure that no single random failure can prevent automatic actuation. If one fails, it must be restored to OPERABLE status.

Actuation Logic channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

(continued)

(continued)

BASES (continued)

LCO (continued)

3. Chemical and Volume Control System Isolation Signal

[At this facility, the bases for CVCS LCO requirements are as follows:]

4. Shield Building Filtration Actuation Signal

[At this facility, the bases for SBFAS LCO requirements are as follows:]

[For this facility, the following support systems are required to be OPERABLE to ensure MAI OPERABILITY:]

[For this facility, those required support systems which, upon their failure, do not result in the MAI being declared inoperable and their justification are as follows.]

[For this facility, the supported systems impacted by the inoperability of the MAI and the justification of whether or not each supported system is declared inoperable are as follows:]

APPLICABILITY

1. Containment Purge Isolation Signal

In MODE 5 or 6, the SIAS isolation of containment purge valves is not required to be OPERABLE. However, during CORE ALTERATIONS or when moving irradiated fuel there is the possibility of a fuel handling accident requiring the CPIS on high radiation in containment. Accordingly, the CPIS must be OPERABLE in MODES 5 and 6.

In MODES 1 through 4, the containment purge valves are closed by CIAS.

2. Control Room Isolation Signal

The CRIS functions must be OPERABLE in MODES 1, 2, 3, and 4 and in all MODES during CORE ALTERATIONS and movement of irradiated fuel or loads over irradiated fuel to ensure a habitable environment for the control room operators.

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

3. Chemical and Volume Control System Isolation Signal

[At this facility, the bases for CVCS isolation applicability requirements are as follows:]

4. Shield Building Filtration Actuation Signal

[At this facility, the bases for SBFAS applicability requirements are as follows:]

A Note has been added to provide clarification that for this LCO each function specified in Table 3.3.4-1 is treated as an independent entity with an independent Completion Time.

ACTIONS

A protection function channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined for each function in the LCO section of the Bases. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis. Typically the drift is not large, and would result in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not consistent with the ALLOWABLE VALUE in Table 3.3.4-1, the channel must be declared inoperable immediately, and the appropriate Conditions from Table 3.3.4-1 must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the ALLOWABLE VALUE, or the sampling equipment transmitter, instrument loop, signal processing electronics, or bistable is found inoperable, then all affected functions provided by that channel should be declared inoperable and the LCO Condition entered for the particular protection function affected.

When the number of inoperable channels in a trip function exceed those specified in one or other related conditions

(continued)

(continued)

ACTIONS (continued)

associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be immediately entered if applicable in the current MODE of operation.

<u>Condition A</u>

Condition A is applicable to all MAI functions. Condition A addresses the situation where one or more channels for one or more functions are inoperable at the same time. The Required Action is to refer to Table 3.3.4-1 and to take the Required Actions for the protection functions affected.

<u>Condition B</u>

Condition B applies to the failure of one or more Containment Radiation--High CPIS Manual Actuation or CPIS Actuation Logic channels. The Required Actions are to immediately restore the affected channels to OPERABLE status; or place and maintain all containment purge and exhaust valves in closed positions; or suspend CORE ALTERATIONS and suspend movement of fuel assemblies within containment. Required Action B.1 is the preferred action as it restores the full functional capability of the CPIS. Required Action B.2 accomplishes the CPIS function. Required Action B.3.1 and Required Action B.3.2 place the plant in a condition where CPIS OPERABILITY is not required. The Completion Time accounts for the fact that Condition B addresses, in the limit, complete loss of the CPIS function under conditions in which a fuel handling accident is possible and CPIS provides the only automatic mitigation of radiation release.

<u>Conditions C and D</u>

Conditions C and D are applicable to manual and automatic actuation of the CREACS by CRIS.

Condition C applies to the failure of one or more channels in MODES 1, 2, 3, or 4. Since the two CRIS radiation inputs measure different parameters, one radiation monitoring channel failure can disable the system's ability to respond to certain types of releases. Therefore, failure of one or more input channels constitutes a loss of the CRIS function

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

for certain events. Consequently, entry into this condition requires action to either restore the failed channel(s) (Required Action C.1) or manually perform the CRIS safety function (Required Action C.2). The Completion Time of 1 hour is sufficient to complete the Required Actions and accounts for the fact that CPIS supplements control room isolation by other functions (e.g. SIAS) in MODES 1, 2, 3, and 4. If the channel cannot be restored to OPERABLE status, the plant must be placed in MODE 3 in the following 6 hours and MODE 5 in the next 30 hours. The Completion Times of 6 and 30 hours for reaching MODES 3 and 5 from MODE 1 are reasonable based on operating experience and normal cooldown rates and do not challenge plant safety systems or operators. Condition D applies to the failure of one or more channels during CORE ALTERATIONS and when moving irradiated fuel or loads over irradiated fuel.

The Required Actions are immediately taken to restore one CRIS channel to OPERABLE status; or place one OPERABLE CREACS train in emergency filtration mode; or CORE ALTERATIONS, positive reactivity additions, movement of irradiated fuel, and movement of loads over irradiated fuel are suspended. The Completion Time recognizes the fact that the radiation signals are the only functions available to initiate control room isolation in the event of a fuel handling accident. Note that in MODE 1, 2, 3, or 4, both Conditions C and D may apply at same time, such as during fuel movement in the fuel building.

Conditions C and D have been modified by a Note which specifies that CREACS be placed manually in the emergency filtration mode, if the auto-swapover to emergency filtration is inoperable. [At this facility, the basis for this Note is as follows:]

Condition E

Condition E applies to the failure of one SBFAS Manual Actuation channel, or one Actuation Logic associated with CVCS isolation signal or SBFAS. Required Action E.1 requires restoration of the inoperable channel to restore redundancy of the affected function. The Completion Time of 1 hour is commensurate with the importance of avoiding vulnerability of a single failure in the only remaining OPERABLE channel.

(continued)

(continued)

ACTIONS (continued)

Condition F

Condition F applies if one of the four CVCS sensor channels is inoperable. The Required Actions are identical to those of ESFAS functions employing four redundant sensors in LCO 3.3.2. The channel must be placed in bypass or trip if it cannot be repaired within 1 hour (Required Action F.2.1). By specifying either option, the possibility of inadvertently bypassing a redundant channel is eliminated. The provision of four trip channels allows one channel to be bypassed (removed from service) during operations, placing the ESFAS in two-out-of-three coincidence logic. Placing the channel in bypass is preferred, since the CVCS isolation function will be in two-out-of-three logic. This will avoid possible inadvertent CVCS isolation if an additional channel fails. The 1-hour Completion Time to bypass or trip the channel is sufficient time to perform the Required Actions.

Once Required Action to trip or bypass the channel has been complied with, Required Action F.2.2.1 and Required Action F.2.2.2 provide for restoring channel to OPERABLE status or placing channel in trip within 48 hours. Required Action F.2.2.1 restores the full capability of the function. Required Action F.2.2.1 places the function into a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent MAI actuation. The Completion Time provides the operator with time to take appropriate actions and still assure that any risk involved in operating with a failed channel is acceptable. Operating experience has demonstrated that a failure of a second channel is improbable during any given 48-hour period.

Condition G

Condition G applies if two of the four CVCS West Penetration Room/Letdown Heat Exchanger Room Pressure--High channels are inoperable. The Required Actions are identical to those for other ESFAS functions employing four redundant sensors in LCO 3.3.2.

Restoring at least one channel to OPERABLE status is the preferred Required Action. If this cannot be accomplished, one channel should be placed in bypass and the other channel

(continued)

(continued)

ACTIONS (continued)

in trip. The allowed Completion Time of 1 hour is sufficient time to perform the Required Actions.

Once Required Action to trip or bypass the channel has been complied with, Required Action H.2.2 provides for restoring the one channel to OPERABLE status within 48 hours. The justification of the 48-hour Completion Time is the same as for Condition F.

After one channel is restored to OPERABLE, the provisions of Condition F still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action G.2.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.

<u>Condition H</u>

Condition H specifies the shutdown track to be followed if the Required Actions and associated Completion Times of Conditions E, F, or G are not met. The plant must be placed in a MODE in which the LCO does not apply. This is done by placing the plant in at least MODE 3 within 6 hours and in MODE 5 within 36 hours. The Completion Times are reasonable based on operating experience, to reach the required MODE from full power operation in an orderly manner and without challenging plant systems.

<u>Condition I</u>

Condition I is applicable to each one of the MAI functions presented in Table 3.3.4-1.

Required Action I.1 verifies that the Required Actions have been initiated for those supported systems declared inoperable because of the inoperability of the support channel(s) within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination.

Required Action I.2 ensures that those identified Required Actions associated with supported systems impacted by the inoperability of channel(s) associated with each MAI function have been initiated by entering the supported

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

systems' LCOs. [Alternatively, the appropriate Required Actions for the supported systems may be listed in the Required Actions for Condition I of this LCO.]

[For this facility, the identified supported systems Required Actions associated with each MAI function are as follows:]

Required Action I.2 verifies that all required support or supported features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 is immediately entered. However, if the support or supported feature LCO takes into consideration the loss-of-function situation, then LCO 3.0.3 may not need to be entered.

SURVEILLANCE REQUIREMENTS

The SRs for any particular MAI function are found in the SRs column of Table 3.3.4-1 for that function.

SR 3.3.4.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION. The high radiation instrumentation should be compared to similar plant instruments located throughout the plant. If the radiation monitor employs keep-alive sources or check sources operable from the control room, the CHANNEL CHECK should also note

(continued)

(continued)

SURVEILLANCE REQUIREMENTS (continued)

the detector's response to these sources.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment have drifted outside its limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off-scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale. [At this facility, the following administrative controls and design features (e.g., downscale alarms) immediately alert operations to loss of function in the nonredundant channels:]. [At this facility, verification of sample system alignment and operation for gaseous, particulate, and iodine monitors is required as follows:]

The Surveillance interval, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited to 12 hours. Since the probability of two random failures in redundant channels in any 12-hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

<u>SR 3.3.4.2</u>

A CHANNEL FUNCTIONAL TEST is performed every 31 days to ensure the entire channel will perform its intended function when needed. The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift which demonstrates that failure of more than one channel of a given function in any 31-day interval is a rare event.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

A CHANNEL FUNCTIONAL TEST verifies the function of the trip, interlock, and alarm functions of the channel. The test inserts a simulated or actual signal as close to the sensor as practicable and verifies required trip, interlocks, and alarms function when the input is beyond the trip point. Where the design has made provisions for including sensors in the CHANNEL FUNCTIONAL TEST, the test signal shall be inserted at that point. "As found" and "as left" values for bistable trip setpoints are recorded. Bistable setpoints are to be found within the ALLOWABLE VALUES specified in the LCO. The difference between the current "as found" and the previous "as left" setpoints must be within the drift allowance used in the setpoint analysis. Recalibration of the bistable setpoint restores the OPERABILITY of an otherwise functional component that does not meet these criteria. However, repeated failures of the same channel over a small number of test intervals should be evaluated as potentially indicating a deterministic failure which cannot be corrected by recalibration. This Surveillance can be performed on the individual sensor channels without actuating the train by using test bypass switches.

SR 3.3.4.3

Proper operation of the individual subgroup relays is verified by de-energizing these relays during the CHANNEL FUNCTIONAL TEST of the actuation logic every 31 days. This will actuate the function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. Note 1 indicates this test includes verification of operation for each initiation relay. [At this facility, the verification is conducted as follows:]

Note 2 indicates that relays that cannot be tested at power are exempt from the Surveillance Requirement while at power. These relays must, however, be tested during each entry into MODE 5 for longer than 24 hours unless they have been tested within the previous 6 months. [At this facility, the basis for this exemption is as follows:] [At this facility, the following relays are exempt:]

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY which demonstrates that failure of more than one channel of a given function in any 31-day interval is a rare event.

SR 3.3.4.4

The SBFAS can be initiated either on a SIAS or manually. This Surveillance is a restatement of SIAS SR 3.3.2.3 on the SIAS function. Performing SR 3.3.2.3 satisfies this Surveillance. The Frequency is the same as that for the SR 3.3.2.3.

SR 3.3.4.5

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to measured parameter with the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive tests, to ensure that the instrument channel remains operational with the setpoint within the assumptions of the plant-specific setpoint analysis. Detector "as found" and "as left" values are recorded and used to verify drift assumptions. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoints errors are within the assumptions of the plant-specific setpoint analysis. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis.

Recalibration restores OPERABILITY of an otherwise functional component found to have errors larger than assumed by the setpoint analysis. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure which cannot be corrected by recalibration.

Radiation detectors may be removed and calibrated in a laboratory, or replaced with an equivalent, laboratory calibrated, unit.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance Frequency is based upon the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

[For this facility, radiation detectors are calibrated as follows:]

SR 3.3.4.6

Every 18 months, a CHANNEL FUNCTIONAL TEST is performed on the manual MAI actuation circuitry.

This test verifies that the trip pushbuttons are capable of opening contacts in the Actuation Logic as designed de-energizing the initiation relays and providing manual actuation of the function. The 18-month Frequency was developed considering it was prudent that these Surveillances only be performed during a plant outage. This was due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 18-month Frequency.

SR 3.3.4.7

This Surveillance ensures that the train actuation response times are verified on a STAGGERED TEST BASIS. The response time values are provided in the FSAR, and are the maximum values assumed in the safety analyses.

Individual component response times are not modeled in the analyses. The analysis model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor, to the point at which the equipment in both trains reaches the required functional state, e.g., pumps at rated discharge pressure, valves in full open or closed position. [For this facility, response time testing acceptance criteria are contained in the following document:]

The test may be performed in one measurement or overlapping segments, with verification that all components are measured.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

Response time tests are conducted on an 18-month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n times 18 months, where n is the number of channels in the function. Testing of the final actuation devices, which make up the bulk of the response time, is included in the testing of each channel. Therefore, staggered testing results in response time verification of these devices every 18 months. The 18-month STAGGERED TEST BASIS Frequency is based upon plant operating experience which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Response times cannot be determined at power since equipment operation is required.

REFERENCES

1. [Unit Name] FSAR, Section [6.2], "Containment Systems."
2. [Unit Name] FSAR, Section [7.3], "Engineered Safety Features Systems."
3. [Unit Name] FSAR, Section [15], "Accident Analysis."
4. [Unit Name], "[Plant Protection System Selection of Trip Setpoint Values.]"

B 3.3 INSTRUMENTATION

B 3.3.4 Miscellaneous Actuation Instrumentation (MAI) (Digital)

BASES

BACKGROUND

This LCO encompasses those plant-specific instrumentation channels which perform some actuation functions required for plant protection, but are not otherwise included in LCO 3.3.2, "Engineered Safety Feature Actuation System (ESFAS)," or LCO 3.3.3, "Emergency Diesel Generator (EDG) Loss of Voltage Start (LOVS)." Specifically included are those non-Nuclear Steam Supply System functions which because of differences in purpose, design, and operating requirements, are not included in LCO 3.3.2 and LCO 3.3.3. Details of this LCO are for illustration only. Individual plants shall include those functions and LCO requirements applicable to them. The MAI in this LCO includes:

1. Containment Purge Isolation Signal (CPIS);

2. Control Room Isolation Signal (CRIS); and

3. Fuel Handling Isolation Signal (FHIS).

These systems are addressed in References 1 and 2. A brief description of each follows:

1. Containment Purge Isolation Signal

   The CPIS provides protection from radioactive contamination in the containment in the event a fuel assembly should be damaged during handling or operation.

   The CPIS will detect any abnormal amounts of radioactive material in the containment and will initiate purge valve closure to limit the release of radioactivity to the environment. Both the mini-purge and large volume purge supply and exhaust valves are closed on a CPIS, when a high radiation level in containment is detected.

(continued)

(continued)

BACKGROUND (continued)

The CPIS includes two independent, redundant logic subsystems, including actuation trains. Each train employs four sensors, each one detecting one of the following:

- gaseous,
- airborne particulate,
- iodine, or
- gamma (area).

Since these sensors each measure a different parameter, they are not considered redundant to each other.

If any one of these sensors exceeds the bistable trip setpoint, the CPIS train will be actuated (one-out-of-four logic).

Each train actuates a separate series valve in the containment purge supply and return lines. Either train controls sufficient equipment to perform the isolation function. These valves are also isolated on a Safety Injection Actuation Signal (SIAS) and Containment Isolation Actuation Signal (CIAS).

2. <u>Control Room Isolation Signal</u>

The CRIS terminates the supply of outside air to the control room and initiates actuation of the emergency filtration system to minimize operator radiation exposure. The CRIS includes two independent, redundant logic subsystems, including actuation trains. Each train employs the same two sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. Since the two sensors detect different types of activity, they are not considered redundant to each other. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment.

(continued)

(continued)

BACKGROUND (continued)

Actuating either train will perform the intended function. Control room isolation also occurs on a SIAS.

3. <u>Fuel Handling Isolation Signal</u>

The FHIS provides protection from radioactive contamination in the spent fuel pool area, in the event that a spent fuel element should be severely damaged during handling. The FHIS will detect radioactivity from fission products in the fuel, and will initiate appropriate actions so the release to the environment is limited. More detail is presented in Reference 3. The FHIS includes two independent, redundant logic subsystems, including actuation trains. Each train employs the same two sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. Since the two sensors detect different types of activity, they are not considered redundant to each other. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment.

<u>Trip Setpoints and ALLOWABLE VALUES</u>

The trip setpoints are the nominal values at which the bistables are set. Any bistable is considered to be properly adjusted when the "as left" value is within the band for channel calibration accuracy (i.e., ± Rack Calibration + Comparator Setting Accuracy).

Trip setpoints used in the bistables are based on the analytical limits (Ref. 4). The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, and instrument drift ALLOWABLE VALUES specified in Table 3.3.4-1 are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in "Plant Protection System Selection of Trip Setpoint Values" (Ref. 5). The actual

(continued)

(continued)

BACKGROUND (continued)

nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the ALLOWABLE VALUE to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. If the measured setpoint does not exceed the ALLOWABLE VALUE, the bistable is considered OPERABLE.

Setpoints in accordance with the ALLOWABLE VALUE will assure that safety limits are not violated during anticipated operational occurrences (AOOs), and the consequences of Design Basis Accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or accident, and the equipment functions as designed.

The ALLOWABLE VALUES listed in Table 3.3.4-1 are based upon the methodology described in Reference 5, which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each trip setpoint. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

Each channel can be tested on line to verify that the signal processing equipment and setpoint accuracy is within the specified allowance requirements of Reference 2. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated.

APPLICABLE SAFETY ANALYSES

1. <u>Containment Purge Isolation Signal</u>

The CPIS is a backup to the CIAS systems in MODES 1, 2, 3, and 4 and will close the containment purge valves in the event of high radiation levels resulting from a primary leak in the containment.

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

The CPIS is also required to close the containment purge valves in the event of the fuel handling accident in containment, as described in Reference 4. This accident is a limiting case representing a class of accidents that might involve radiation release in containment without CIAS actuation. The CPIS ensures the consequences of a dropped fuel assembly in the containment are not as severe as a dropped assembly in the fuel handling building. This ensures that the offsite consequences of radiation accidents in containment are within 10 CFR 100 limits.

2. Control Room Isolation Signal

The CRIS, in conjunction with SIAS, and the Control Room Emergency Air Cleanup System (CREACS), maintains the control room atmosphere within conditions suitable for prolonged occupancy throughout the duration of any one of the accidents discussed in Reference 4. The radiation exposure of control room personnel, through the duration of any one of the postulated accidents, does not exceed the limits set by GDC 19 of 10 CFR 50, Appendix A.

3. Fuel Handling Isolation Signal

The FHIS is required to isolate the normal Fuel Building Air Cleanup System (FBACS) and automatically initiate the recirculation and filtration systems in the event of the fuel handling accident in the fuel handling building or a loss-of-coolant accident, as described in Reference 4. The FHIS helps assure acceptable consequences for the dropping of a spent fuel bundle breaching up to 60 fuel pins.

The MAI satisfies Criterion 3 of the NRC Interim Policy Statement.

LCO

MAI channels are OPERABLE when the applicable criteria below are met:

1. All channel components necessary to provide an initiation signal are functional and in service. For

(continued)

(continued)

LCO (continued)

sampling systems, OPERABILITY requires correct valve lineups, sample pump operation, and filter motor operation as well as detector OPERABILITY if these supporting features are necessary for trip to occur under the conditions assumed by the safety analysis or setpoint analysis;

2. Channel measurement uncertainties are known via test, analysis, or design information to be within the assumptions of the setpoint calculations; and

3. Required surveillance testing is current and has demonstrated performance within each surveillance test's acceptance criteria.

Only the ALLOWABLE VALUES are specified for each trip function in the LCO. Operation with a trip setpoint less conservative than the nominal trip setpoint, but within its ALLOWABLE VALUE, is acceptable provided that the difference between the nominal trip setpoint and the ALLOWABLE VALUE is equal to or greater than the drift allowance assumed for each trip in the transient and accident analyses. Each ALLOWABLE VALUE specified is more conservative than the analytical limit assumed in the transient and accident analysis in order to account for instrument uncertainties appropriate to the trip function. These uncertainties are defined in the "Plant Specific Setpoint Methodology" (Ref. 5).

The bases for the LCO on these functions are:

1. <u>Containment Purge Isolation Signal</u>

1.a. <u>Manual Actuation</u>

The LCO on manual actuation ensures that the CPIS function can easily be initiated if desired. Both available channels are required to ensure a single failure will not disable the manual initiation capability.

Manual actuation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

(continued)

BASES (continued)

LCO (continued)

1.b.,1.c. Airborne Radiation and Containment Area Radiation

The LCO on the four airborne radiation channels requires that each channel be OPERABLE for each actuation logic channel, since they are not redundant to each other. [At this facility, the purge isolation function meets the single failure criterion as follows:]

The trip setpoint of twice background is selected to allow detection of small deviations from normal. The absolute value of trip setpoint in MODES 5 and 6 differs from the setpoint in MODES 1 through 4 so that a fuel handling accident can be detected in the lower background radiation expected in these MODES.

Airborne radiation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1, 2, and 3.

1.d. Actuation Logic

Two channels of actuation Logic are required to be OPERABLE to ensure that no single logic failure disables actuation in both trains.

Actuation logic channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

2. Control Room Isolation Signal

2.a. Manual Actuation

The LCO on Manual actuation ensures that the CRIS function can easily be initiated if desired. Both available channels are required to ensure a single failure will not disable the manual initiation capability.

Manual actuation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

(continued)

(continued)

LCO (continued)

2.b. Airborne Radiation

The LCO on the two airborne radiation channels requires that each channel be OPERABLE for each actuation logic channel, since they are not redundant to each other. [At this facility the control room isolation function meets the single failure criterion as follows:]

[At this facility, the basis for the CRIS radiation monitor ALLOWABLE VALUES are as follows:]

Airborne radiation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1, 2, and 3.

2.c. Actuation Logic

Two channels of actuation logic are required to be OPERABLE to ensure that no single logic failure disables actuation in both trains.

CRIS actuation logic channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

3. Fuel Handling Isolation Signal

3.a. Manual Actuation

The LCO on manual actuation ensures that the FHIS function can easily be initiated if desired. Both available channels are required to ensure a single failure will not disable the manual initiation capability.

Manual actuation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1 and 3.

3.b. Airborne Radiation

The LCO on the two airborne radiation channels requires that each channel be OPERABLE for each actuation logic channel, since they are not

(continued)

(continued)

BASES (continued)

LCO (continued)

redundant to each other. [At this facility, the FHIS function meets the single failure criterion as follows:]

[At this facility, the basis for the FHIS radiation monitor ALLOWABLE VALUES is as follows:]

Airborne radiation channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1, 2, and 3.

3.c. Actuation Logic

Two channels of Actuation Logic are required to be OPERABLE to ensure that no single logic failure disables actuation in both trains.

FHIS actuation logic channels are OPERABLE when they satisfy MAI OPERABILITY Criteria 1, 2, and 3.

[For this facility, the following support systems are required to be OPERABLE to ensure MAI OPERABILITY:]

[For this facility, those required support systems which, upon their failure, do not result in the MAI being declared inoperable and their justification are as follows:]

[For this facility, the supported systems impacted by the inoperability of the MAI and the justification of whether or not each supported system is declared inoperable are as follows:]

APPLICABILITY

1. Containment Purge Isolation Signal

In MODES 1, 2, 3, and 4, the mini-purge valves may be open. In these MODES, it is necessary to assure the valves will shut in the event of a primary leak in containment.

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

In MODE 5 or 6 during CORE ALTERATIONS or movement of irradiated fuel, there is the possibility of a fuel handling accident requiring CPIS on high radiation in containment.

2. Control Room Isolation Signal

The CRIS functions must be OPERABLE in MODES 1, 2, 3, and 4 and in all MODES during CORE ALTERATIONS and movement of irradiated fuel or loads over irradiated fuel to ensure a habitable environment for the control room operators.

3. Fuel Handling Isolation Signal

The FHIS is required to be OPERABLE in MODES 1, 2, 3, and 4 and when irradiated fuel is in the storage pool. [For this facility, the basis for this requirement is as follows:]

A Note has been added to provide clarification that for this LCO each function specified in Table 3.3.4-1 is treated as an independent entity with an independent Completion Time.

ACTIONS

A protection channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined for each function in the LCO section of the Bases. The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant-specific setpoint analysis. Typically the drift is not large, and would result in a delay of actuation rather than a total loss of function. This determination is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not consistent with the ALLOWABLE VALUE in Table 3.3.4-1, the channel must be declared inoperable immediately, and the appropriate Conditions from Table 3.3.4-1 must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the ALLOWABLE VALUE, or the

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

transmitter, instrument loop, signal processing electronics, or bistable is found inoperable, then all affected functions provided by that channel are required to be declared inoperable and the LCO Condition entered for the particular protective function affected.

When the number of inoperable channels in a trip function exceeds that specified in one or other related Conditions associated with the same trip function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 is immediately entered if applicable in the current MODE of operation.

Condition A

Condition A is applicable to all MAI functions. Condition A addresses the situation where one or more channels for one or more functions are inoperable at the same time. The Required Action is to refer to Table 3.3.4-1 and to take the Required Actions for the protection functions affected.

Condition B

Condition B applies to the failure of one or more of the following channels associated with CPIS during CORE ALTERATIONS and when moving irradiated fuel in containment in MODE 5 or 6:

1.a. Manual Actuation (2 channels)

1.b.i. Airborne Radiation - Gaseous (1 channel)

1.b.ii. Airborne Radiation - Particulate (1 channel)

1.b.iii. Airborne Radiation - Iodine (1 channel)

1.c. Containment Area Radiation (Gamma) (1 channel)

1.d. Actuation Logic (2 channels)

The Required Actions are to immediately restore the affected channels to OPERABLE status, or to place and maintain containment purge and exhaust valves in closed positions, or to suspend CORE ALTERATIONS and to suspend movement of fuel assemblies within containment.

(continued)

(continued)

ACTIONS (continued)

Required Action B.1 is the preferred action as it restores the full functional capability of the function. Required Action B.2 accomplishes the CPIS function. Required Action B.3.1 and Required Action B.3.2 place the plant in a configuration where CPIS OPERABILITY is not required. The Completion Time accounts for the fact that Condition B, in the limit, addresses complete loss of the CPIS function under conditions where a fuel handling accident in containment is possible and CPIS provides the only automatic mitigation of radiation release.

Condition C

Condition C applies to the failure of one or more of the following channels associated with CPIS in MODE 1, 2, 3, or 4:

1.a. Manual Actuation (2 channels)

1.b.i. Airborne Radiation - Gaseous (1 channel)

1.b.ii. Airborne Radiation - Particulate (1 channel)

1.b.iii. Airborne Radiation - Iodine (1 channel)

1.c. Containment Area Radiation (Gamma) (1 channel)

1.d. Actuation Logic (2 channels)

The Required Actions are to restore the affected channels to OPERABLE status or place and maintain containment purge and exhaust valves in closed positions within 1 hour. Required Action C.1 is the preferred action as it restores the full functional capability of the function. Required Action C.2 accomplishes the CPIS function. Required Action C.3.1 and Required Action C.3.2 place the plant in a configuration where CPIS OPERABILITY is not required. The Completion Time of 1 hour is reasonable for repairing the channel and takes into account the time required to isolate the affected penetrations and the relative importance of maintaining containment OPERABILITY during MODE 1, 2, 3, or 4. Furthermore, it credits the fact that CIAS initiates purge valve isolation for events occurring in MODE 1, 2, 3, or 4.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

If the affected channels cannot be restored to OPERABLE status or the affected penetrations cannot be isolated, the plant is placed in MODE 3 in the following 6 hours and in MODE 5 in the next 30 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

Condition D

Condition D applies to the failure of one or more of the following channels associated with CPIS in MODES 1, 2, 3, or 4:

1.b.i. Airborne Radiation - Gaseous

1.b.ii. Airborne Radiation - Particulate

During these MODES, the possibility exists where radiation leakage may occur in the containment which could require closure of all purge and exhaust valves. The Required Action is to perform the Required Actions of LCO 3.4.15, "RCS Leakage Detection Instrumentation." [At this facility, the basis for Required Action D.1 is as follows:]

Conditions E and F

Conditions E and F applies to the manual and automatic initiation of CRIS to actuate the Control Room Emergency Air Cleanup System (CREACS).

Condition E applies to the failure of one of the following channels associated with CRIS in MODE 1, 2, 3, or 4:

2.a. Manual Actuation (2 channels)

2.b.i. Airborne Radiation - Particulate (1 channel), Iodine (1 channel)

2.b.ii. Airborne Radiation - Gaseous (1 channel)

2.c. Actuation Logic (2 channels)

(continued)

(continued)

ACTIONS (continued)

Since two CRIS radiation inputs measure different parameters, one radiation monitor failure can disable the system's ability to respond to certain types of releases. Therefore, failure of one or more input channels constitutes a loss of the CRIS function. Consequently, entry into this Condition requires action to either restore the failed channel(s) (Required Action E.1), or manually perform the CRIS function (Required Action E.2). The Completion Time of 1 hour is sufficient to perform the Required Actions and accounts for the fact that CRIS supplements control room isolation by other functions (e.g., SIAS) in MODES 1, 2, 3, and 4.

If the affected channels cannot be restored to OPERABLE status or one OPERABLE CREACS train cannot be placed in the emergency filtration mode, the plant is placed in MODE 3 within the following 6 hours and in MODE 5 within the next 30 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

Condition F applies to the failure of one or more of the channels mentioned above for Condition E associated with the CRIS during CORE ALTERATIONS, or when moving irradiated fuel or loads over irradiated fuel. The Completion Time accounts for the fact that the radiation monitor signals are the only functions available to initiate control room isolation in the event of a fuel handling accident. Note that in MODES 1, 2, 3, and 4 both Conditions E and F may apply at some times, such as during fuel movement in the fuel handling building.

The Required Actions are to restore the affected channels to OPERABLE status, or place one OPERABLE CREACS train in emergency filtration mode, or suspend CORE ALTERATIONS and suspend positive reactivity additions and suspend movement of irradiated fuel and loads over irradiated fuel. These Required Actions are required to be completed immediately.

Conditions E and F are modified by a Note, which specifies that CREACS be placed manually in the emergency filtration mode, if auto-swapover to emergency filtration is inoperable. [At this facility, the basis for this Note is as follows:]

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Conditions G and H

Conditions G and H apply to the manual and automatic initiation of FHIS to actuate the FBACS.

Condition G applies to the failure of one of the following channels associated with FHIS in MODE 1, 2, 3, or 4:

3.a. Manual Actuation (2 channels)

3.b.i. Airborne Radiation - Gaseous (1 channel)

3.b.ii. Airborne Radiation - Particulate (1 channel), Iodine (1 channel)

3.c. Actuation Logic (2 channels)

The Required Actions are to restore the affected channels to OPERABLE status or place one OPERABLE FBACS train in operation within 1 hour. The Completion Time of 1 hour is sufficient to perform the Required Actions. The Completion Time accounts for the fact that the FHIS radiation monitors are the only signals available to automatically initiate the FBACS to mitigate radioactive releases in the fuel building and credits the relatively lower likelihood of such events when irradiated fuel is not being moved.

If the affected channels cannot be restored to OPERABLE status or one OPERABLE FBACS train cannot be placed in operation, the plant is placed in MODE 3 within the following 6 hours and in MODE 5 within the next 30 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODE from full power in an orderly manner and without challenging plant systems.

Condition H applies to the failure of one or more of the same channels mentioned above for Condition G associated with FBACS during movement of irradiated fuel in the fuel building.

The Required Actions are to restore the affected channels to OPERABLE status, or place one OPERABLE FBACS train in

(continued)

(continued)

ACTIONS (continued)

operation, or suspend movement of irradiated fuel in the fuel building. These Required Actions are required to be completed immediately. The Completion Time accounts for the higher likelihood of releases in the fuel building during fuel handling. Note that in MODES 1, 2, 3, and 4, both Conditions G and H may apply in certain circumstances.

Condition I

Condition I is applicable to each one of the MAI functions presented in Table 3.3.4-1.

Required Action I.1 verifies that the Required Actions have been initiated for those supported systems declared inoperable because of the inoperability of the support channel(s) within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination.

Required Action I.1 ensures that those identified Required Actions associated with supported systems impacted by the inoperability of channel(s) associated with each MAI function have been initiated by entering the supported systems' LCOs. [Alternatively, the appropriate Required Actions for the supported systems may be listed in the Required Actions for Condition I of this LCO.]

[For this facility, the identified supported systems' Required Actions associated with each MAI function are as follows:]

Required Action I.2 verifies that all required support or supported features associated with the other redundant channel(s) are OPERABLE within a Completion Time of 1 hour. The specified Completion Time is sufficient for plant operations personnel to make this determination. If verification determines loss of functional capability, LCO 3.0.3 is immediately entered. However, if the support or supported feature LCO takes into consideration the loss of function situation, then LCO 3.0.3 may not need to be entered.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

The SRs for any particular MAI function are found in the SRs column of Table 3.3.4-1 for that function. Most MAI functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing.

SR 3.3.4.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION. The high radiation instrumentation should be compared to similar plant instruments located throughout the plant. If the radiation monitor employs keep-alive sources or check sources operable from the control room, the CHANNEL CHECK should also note the detector's response to these sources.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Surveillance interval, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, performance of the CHANNEL CHECK guarantees that undetected overt channel failure is limited

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

to 12 hours. Since the probability of two random failures in redundant channels in any 12-hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of the displays associated with the LCO required channels.

[At this facility, the following administrative controls and design features (e.g., downscale alarms) immediately alert operators to loss of function in nonredundant channels:]

[For this facility, the CHANNEL CHECK verification of sample system alignment and operation for gaseous, particulate, iodine, and gamma monitors is as follows:]

SR 3.3.4.2

SR 3.3.4.2 is the performance of a CHANNEL CHECK on the particulate and iodine channels used in the CPIS. It differs only in the Surveillance interval, which is weekly. These channels use a filter to trap the particulate and iodine activity prior to the air sample being pumped to the gaseous activity chamber. This technique results in an integration of total particulate and iodine activity until the filter assemblies are replaced. The low levels of activity expected make more frequent monitoring unnecessary.

[At this facility, the following administrative controls and design features (e.g., downscale alarms) immediately alert operators to loss of function:]

SR 3.3.4.3

A CHANNEL FUNCTIONAL TEST is performed every 31 days to ensure the entire channel will perform its intended function when needed. The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given function in any 31-day interval is a rare event.

A CHANNEL FUNCTIONAL TEST verifies the function of the trip, interlock, and alarm functions of the channel. The test inserts a simulated or actual signal as close to the

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

sensor as practicable and verifies required trip, interlocks, and alarms function when the input is beyond the trip point. Where the design has made provisions for including sensors in the CHANNEL FUNCTIONAL TEST, the test signal shall be inserted at that point. "As found" and "as left" values for bistable trip setpoints are recorded. Bistable setpoints are to be found within the ALLOWABLE VALUES specified in the LCO. The difference between the current "as found" and the previous "as left" setpoints must be within the drift allowance used in the setpoint analysis. Recalibration of the bistable setpoint restores the OPERABILITY of an otherwise functional component that does not meet these criteria. However, repeated failures of the same channel over a small number of test intervals should be evaluated as potentially indicating a deterministic failure which cannot be corrected by recalibration. By using test bypass switches, this surveillance can be performed on the individual sensor channels without actuating the train.

SR 3.3.4.4

Proper operation of the individual subgroup relays is verified by actuating these relays during the CHANNEL FUNCTIONAL TEST of the actuation logic every 31 days. This will actuate the function, operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given function during any 31-day interval is a rare event.

A Note to the SR indicates that this test includes verification of operation for each initiation relay. [At this facility, the verification is conducted as follows:]

SR 3.3.4.5

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to the measured parameter with the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive tests, to ensure that the instrument channel

(continued)

(continued)

SURVEILLANCE REQUIREMENTS (continued)

remains operational with the setpoint within the assumptions of the plant-specific setpoint analysis. Detector "as found" and "as left" values are recorded and used to verify drift assumptions. For OPERABLE channels, CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint errors are within the assumptions of the plant-specific setpoint analysis. Measurement and setpoint error determination and readjustment must be performed consistent with the assumptions of the plant-specific setpoint analysis.

Recalibration restores OPERABILITY of an otherwise functional component found to have errors larger than assumed by the setpoint analysis. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure which cannot be corrected by recalibration.

Radiation detectors may be removed and calibrated in a laboratory, or replaced with an equivalent, laboratory calibrated, unit.

The Surveillance Frequency is based upon the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift in the setpoint analysis.

[For this facility, radiation detectors are calibrated as follows:]

SR 3.3.4.6

Every 18 months, or approximately every refueling, a CHANNEL FUNCTIONAL TEST is performed on the manual actuation circuitry.

This test verifies that the trip push buttons are capable of opening contacts in the actuation logic as designed, actuating the initiation relays, and providing manual actuation of the function. The 18-month Frequency was developed considering it is prudent that these Surveillances would only be performed during a plant outage. This is due to the plant conditions needed to perform the Surveillance and the potential for unplanned plant

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

transients if the Surveillance is performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed on the 18-month Frequency.

SR 3.3.4.7

This Surveillance ensures that the train actuation response times are verified on a STAGGERED TEST BASIS. The response time values are provided in the FSAR and are the maximum values assumed in the safety analyses.

Individual component response times are not modeled in the analyses. The analyses model the overall or total elapsed time, from the point at which the parameter exceeds the trip setpoint value at the sensor, to the point at which the equipment in both trains reaches the required functional state (e.g., pumps at rated discharge pressure, valves in full open or closed position). [For this facility, response time testing acceptance criteria are contained in the following documents.]

The test may be performed in one measurement or overlapping segments, with verification that all components are measured.

Response time tests are conducted on an 18-month STAGGERED TEST BASIS. This results in the interval between successive tests of a given channel of n times 18 months, where n is the number of channels in the function. Testing of the final actuation devices, which make up the bulk of the response time, is included in the testing of each channel. Therefore, staggered testing results in response time verification of these devices every 18 months. The 18-month STAGGERED TEST BASIS Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Response times cannot be determined at power, since equipment operation is required.

(continued)

BASES (continued)

REFERENCES

1. [Unit Name] FSAR, Section [6.2], "[Containment Systems]."
2. [Unit Name] FSAR, Section [7.3], "[Engineered Safety Features Systems]."
3. [Unit Name] FSAR, Section [9], "[Auxiliary Systems]."
4. [Unit Name] FSAR, Section [15], "[Accident Analysis]."
5. [Unit Name] "Plant Protection System Selection of Trip Setpoint Values."

B 3.3 INSTRUMENTATION

B 3.3.5 Post-Accident Monitoring (PAM) Instrumentation (Analog and Digital)

BASES

BACKGROUND

Indications of plant variables are required by the control room operating personnel during accident situations to:

1. Provide information required to permit the operator to take preplanned manual actions to accomplish safe plant shutdown;

2. Determine whether the Reactor Protection System (RPS), Engineered Safety Feature Actuation Systems, manually initiated safety systems, and other systems important to safety are performing their intended functions (i.e., reactivity control, core cooling, maintaining Reactor Coolant System (RCS) integrity, and maintaining containment OPERABILITY);

3. Provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release (i.e., fuel cladding, reactor coolant pressure boundary, and containment) and to determine if a gross breach of a barrier has occurred; and

4. Provide information regarding the release of radioactive materials to allow for early indication of the need to initiate action necessary to protect the public and for an estimate of the magnitude of any impending threat.

At the start of an accident, it may be difficult for the operator to determine immediately what accident has occurred or is occurring and therefore to determine the appropriate response. For this reason, reactor trip and certain other safety actions (e.g., emergency core cooling actuation, containment isolation, or depressurization) have been designed to be performed automatically during the initial stages of an accident. Instrumentation is also provided to indicate information about plant variables required to enable the operation of manually initiated safety systems and other appropriate operator actions involving systems important to safety.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Independent of the above tasks, it is important that operators be informed if the barriers to the release of radioactive materials are being challenged. Therefore, PAM instrument ranges are selected so that the instrument will always be on scale. Instruments that are not part of the PAM System may provide limited backup capability, but they may not have the necessary range to track the course of the accident; consequently, multiple instruments with overlapping ranges may be necessary. It is essential that degraded conditions and their magnitude be identified so the operators can take actions that are available to mitigate the consequences. It is not intended that operators be encouraged to prematurely circumvent systems important to safety, but that they be adequately informed in order that unplanned actions can be taken when necessary.

Examples of serious events that could threaten safety if conditions degrade are loss-of-coolant accidents (LOCAs), overpressure transients, anticipated operational occurrences that become accidents such as anticipated transients without scram, and reactivity excursions that result in releases of radioactive materials. Such events require that the operators understand, within a short time period, the ability of the barriers to limit radioactivity release (i.e., that they understand the potential for breach of a barrier or whether an actual breach of a barrier has occurred because of an accident in progress).

It is essential that the required instrumentation be capable of surviving the accident environment in which it is located for the length of time its function is required. It is, therefore, either designed to withstand the accident environment or to be protected by a local protected environment.

Variables for accident monitoring are selected to provide the essential information needed by the operator to determine if the plant safety functions are being performed. The availability of such instrumentation is important so that responses to corrective actions can be observed and the need for, and magnitude of, further actions can be determined.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

These essential instruments are identified by plant-specific documents (Ref. 1) addressing the recommendations of Regulatory Guide 1.97 (Ref. 2) as required by Supplement 1 to NUREG 0737 (Ref. 3). The instrument channels required to be OPERABLE by this LCO equate to two classes of parameters identified during plant-specific implementation of Regulatory Guide 1.97 as Type A variables and Category 1 variables.

Type A variables are included in this LCO because they provide the primary information required to permit the control room operator to take specific manually controlled actions for which no automatic control is provided and that are required for safety systems to accomplish their safety functions for Design Basis Accidents (DBAs). Primary information is information that is essential for the direct accomplishment of the specified safety functions; it does not include those variables that are associated with contingency actions that may also be identified in written procedures. Because the list of Type A variables widely differs between plants, Table 3.3.5-1 contains no examples of Type A variables, except for those that may also be Category 1.

Category 1 variables are the key variables deemed risk significant because they are needed to:

1. Determine whether other systems important to safety are performing their intended functions;

2. Provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release; and

3. Provide information regarding the release of radioactive materials to allow for early indication of the need to initiate action necessary to protect the public and for an estimate of the magnitude of any impending threat.

These key variables are identified by plant-specific Regulatory Guide 1.97 analyses (Ref. 1). These analyses identified the plant-specific Type A variables and provided justification for deviating from the NRC proposed list of Category 1 variables.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Table 3.3.5-1 provides a list of variables typical of those identified by plant-specific Regulatory Guide 1.97 analyses. [Table 3.3.5-1 in plant-specific Technical Specifications (TS) should list all Type A and Category 1 variables identified by the plant specific Regulatory Guide 1.97 analysis, as amended by the NRC's Safety Evaluation Report (SER).]

Type A and Category 1 variables are required to meet Regulatory Guide 1.97 Category 1 (Ref. 2) design and qualification requirements for seismic and environmental qualification, single failure criterion, utilization of emergency standby power, immediately accessible display, continuous readout, and recording of display.

Listed below are discussions of the specified instrument functions listed in Table 3.3.5-1. These discussions are intended as examples of what should be provided for each function when the plant specific list is prepared.

1. <u>[Wide Range] Neutron Flux</u>

   [Wide range] neutron flux indication is provided to verify reactor shutdown. [At this facility, the Wide Range Neutron Flux PAM channels consist of the following:]

2, 3. <u>Reactor Coolant System (RCS) Hot and Cold Leg Temperature</u>

   Reactor Coolant System (RCS) Hot and Cold Leg Temperatures are Category 1 variables provided for verification of core cooling and long-term surveillance.

   Reactor outlet temperature inputs to the PAM are provided by two fast-response resistance elements and associated transmitters in each loop. The channels provide indication over a range of 32°F to 700°F.

4. <u>RCS Pressure (Wide Range)</u>

   RCS wide range pressure is a Category 1 variable provided for verification of core cooling and RCS integrity long-term surveillance.

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

Wide range RCS loop pressure is measured by pressure transmitters with a span of 0-3000 psig. The pressure transmitters are located outside the containment. Redundant monitoring capability is provided by two trains of instrumentation. Control room indications are provided through the inadequate core cooling (ICC) plasma display. The ICC plasma display is the primary indication used by the operator during an accident. Therefore, the accident monitoring specification deals specifically with this portion of the instrument channel.

In some plants, RCS pressure is a Type A variable because the operator uses this indication to monitor the cooldown of the RCS following a steam generator tube rupture or small-break LOCA. Operator actions to maintain a controlled cooldown, such as adjusting steam generator pressure or level, would use this indication. Furthermore, RCS pressure is one factor that may be used in decisions to terminate reactor coolant pump operation.

5. Reactor Vessel Water Level

Reactor Vessel Water Level is provided for verification and long-term surveillance of core cooling.

The reactor vessel level monitoring system provides a direct measurement of the collapsed liquid level above the fuel alignment plate. The collapsed level represents the amount of liquid mass which is in the reactor vessel above the core. Measurement of the collapsed water level is selected because it is a direct indication of the water inventory. The collapsed level is obtained over the same temperature and pressure range as the saturation measurements, thereby encompassing all operating and accident conditions where it must function. Also, it functions during the recovery interval. Therefore it is designed to survive the high steam temperature which may occur during the preceding core recovery interval.

The level range extends from the top of the vessel down to the top of the fuel alignment plate The

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

response time is short enough to track the level during small-break LOCA events. The resolution is sufficient to show the initial level drop, the key locations near the hot leg elevation, and the lowest levels just above the alignment plate. This provides the operator with adequate indication to track the progression of the accident and to detect the consequences of its mitigating actions or the functionality of automatic equipment.

6. <u>Containment Sump Water Level (Wide Range)</u>

Containment sump water level is provided for verification and long-term surveillance of RCS integrity. [For this facility, Containment sump water level instrumentation consists of the following:]

7. <u>Containment Pressure (Wide Range)</u>

Containment pressure is provided for verification of RCS and containment OPERABILITY. [For this facility, containment pressure instrumentation consists of the following:]

8. <u>Containment Isolation Valve Position</u>

Containment Isolation Valve Position is provided for verification of containment OPERABILITY. [For this facility, Containment Isolation Valve Position consists of the following:]

9. <u>Containment Area Radiation (High Range)</u>

Containment area radiation is provided to monitor for the potential of significant radiation releases and to provide release assessment for use by operators in determining the need to invoke site emergency plans. [For this facility, containment area radiation instrumentation consists of the following:]

10. <u>Containment Hydrogen Concentration</u>

Containment Hydrogen concentration is provided to detect high hydrogen concentration conditions which represent a potential for containment breach. This

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

variable is also important in verifying the adequacy of mitigating actions.

[For this facility, containment hydrogen instrumentation consists of the following:]

11. Pressurizer Level

Pressurizer Level is used to determine whether to terminate safety injection, if still in progress, or to reinitiate safety injection if it has been stopped. Knowledge of pressurizer water level is also used to verify the plant conditions necessary to establish natural circulation in the RCS and to verify that the plant is maintained in a safe shutdown condition. [For this facility, pressurizer level instrumentation consists of the following:]

12. Steam Generator Water Level

Steam Generator Water Level is provided to monitor operation of decay heat removal via the steam generators. The Category 1 indication of steam generator level is the extended startup range level instrumentation. The extended startup range level covers a span of 6 to 394 inches above the lower tubesheet. The measured differential pressure is displayed in inches of water at 68°F. Temperature compensation of this indication is performed manually by the operator. Redundant monitoring capability is provided by two trains of instrumentation. The uncompensated level signal is input to the plant computer, a control room indicator, and the [auxiliary feedwater (AFW)] control system.

At some plants, operator action is based on the control room indication of steam generator water level. The RCS response during a design basis small-break LOCA is dependent on the break size. For a certain range of break sizes, the boiler-condenser mode of heat transfer is necessary to remove decay heat. At these plants, extended startup range level is a Type A variable because the operator must manually raise and control steam generator level to establish boiler-condenser heat transfer. Operator

(continued)

(continued)

BACKGROUND (continued)

action is initiated on a loss of subcooled margin. Feedwater flow is increased until the indicated extended startup range level reaches the boiler-condenser setpoint.

13. <u>Condensate Storage Tank Level</u>

Condensate Storage Tank (CST) Level is provided to ensure water supply for [AFW]. The CST provides the assured safety grade water supply for the [AFW] system. The CST consists of two identical tanks connected by a common outlet header. Inventory is monitored by a 0 to 144 inch level indication for each tank. CST level is displayed on a control room indicator, strip chart recorder, and plant computer. In addition, a control room annunciator alarms on low level.

At some plants, CST level is considered a Type A variable because the control room meter and annunciator are considered the primary indication used by the operator. The DBAs which require [AFW] are the loss of electric power, steam line break (SLB), and small-break LOCA. The CST is the initial source of water for the [AFW] System. However, as the CST is depleted, manual operator action is necessary to replenish the CST or align suction to the [AFW] pumps from the hotwell.

14, 15, 16, 17. <u>Core Exit Temperature</u>

Core exit temperature is provided for verification and long-term surveillance of core cooling.

An evaluation was made of the minimum number of valid core exit thermocouples necessary for inadequate core cooling detection. The evaluation determined the reduced complement of core exit thermocouples necessary to detect initial core recovery and trend the ensuing core heatup. The evaluations account for core nonuniformities including incore effects of the radial decay power distribution and excore effects of condensate runback in the hot legs and nonuniform inlet temperatures. Based on these evaluations,

(continued)

(continued)

BASES (continued)

BACKGROUND (continued)

adequate or inadequate core cooling detection is assured with two valid core exit thermocouples per quadrant.

The design of the incore instrumentation system includes a Type K (chromel-alumel) thermocouple within each of the 56 incore instrument detector assemblies. The junction of each thermocouple is located a few inches above the fuel assembly inside a structure which supports and shields the incore instrument detector assembly string from flow forces in the outlet plenum region. These core exit thermocouples monitor the temperature of the reactor coolant as it exits the fuel assemblies.

The core exit thermocouples have a usable temperature range from 32°F to up to 2300°F although accuracy is reduced at temperatures above 1800°F.

18. Auxiliary Feedwater [AFW] Flow

[AFW] Flow is provided to monitor operation of decay heat removal via the steam generators.

The [AFW] Flow to each steam generator is determined from a differential pressure measurement calibrated to a span of 0-1200 gpm. Redundant monitoring capability is provided by two independent trains of instrumentation for each steam generator. Each differential pressure transmitter provides an input to a control room indicator and the plant computer. Since the primary indication used by the operator during an accident is the control room indicator, the accident monitoring specification deals specifically with this portion of the instrument channel.

At some plants [AFW] Flow is a Type A variable because operator action is required to throttle flow during an SLB accident in order to prevent the [AFW] pumps from operating in runout conditions. [AFW] Flow is also used by the operator to verify that the [AFW] System is delivering the correct flow to each steam generator. However, the primary indication used by the operator to ensure an adequate inventory is steam generator level.

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES

The PAM instrumentation ensures the OPERABILITY of Regulatory Guide 1.97 Type A and Category 1 variables so that the control room operating staff can:

1. Perform the diagnosis required to support preplanned actions for the primary success path of Design Basis Accidents (DBAs);

2. Take the specified, preplanned, manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions;

3. Determine whether systems important to safety are performing their intended functions;

4. Determine the potential for causing a gross breach of the barriers to radioactivity release;

5. Determine if a gross breach of a barrier has occurred; and

6. Initiate action necessary to protect the public and for an estimate of the magnitude of any impending threat.

These functions support the requirements of GDCs 13 and 19 of Appendix A to 10 CFR 50 (Ref. 4). The plant-specific Regulatory Guide 1.97 analysis documents the process that identified Type A and Category 1 variables.

PAM instrumentation that satisfies the definition of Type A in Regulatory Guide 1.97 meets Criterion 3 of the NRC Interim Policy Statement. Category 1 PAM instrumentation is retained in the Specification because it is intended to assist operators in minimizing the consequences of accidents. Therefore, Category 1 variables are important in reducing public risk.

LCO

The PAM instrumentation LCO provides the requirement of Type A and Category 1 monitors which provide information required by control room operators to:

(continued)

(continued)

BASES (continued)

LCO (continued)

- Permit the operator to take preplanned manual actions to accomplish safe plant shutdown;
- Determine whether systems important to safety are performing their intended functions;
- Provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release and to determine if a gross breach of a barrier has occurred; and
- Provide information regarding the release of radioactive materials to allow for early indication of the need to initiate action necessary to protect the public and for an estimate of the magnitude of any impending threat.

Two channels are required to be OPERABLE for most functions. Two OPERABLE channels ensure no single failure within either of the PAM instrumentation, its auxiliary supporting features, or its power sources, concurrent with the failures that are a condition of or result from a specific accident, prevents the operators from being presented the information necessary for them to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident.

Furthermore, provision of two channels allows channel checks during the post accident phase to confirm the validity of displayed information. More than two channels may be required at some plants if the Regulatory Guide 1.97 analysis determined that failure of one accident monitoring channel results in information ambiguity (that is, the redundant displays disagree) that could lead operators to defeat or fail to accomplish a required safety function. This might also be accomplished by providing an independent channel to monitor a different variable that bears a known relationship to the multiple channels (addition of a diverse channel).

In Table 3.3.5-1 the exceptions to the two channel requirement are Core Exit Temperatures, loop/steam generator related variables, and Containment Isolation Valve Position.

(continued)

(continued)

BASES (continued)

LCO (continued)

Two OPERABLE channels of core exit thermocouples are required for each channel in each quadrant to provide indication of radial distribution of the coolant temperature rise across representative regions of the core. Power distribution symmetry was considered in determining the specific number and locations provided for diagnosis of local core problems. Therefore, two randomly selected thermocouples may not be sufficient to meet the two thermocouples per channel requirement in any quadrant. The two thermocouples in each channel must meet the additional requirement that one be located near the center of the core and the other near the core perimeter, such that the pair of core exit thermocouples indicate the radial temperature gradient across their core quadrant. Plant-specific evaluations in response to Item II.F.2 of NUREG 0737 should have identified the thermocouple pairings that satisfy these requirements. Two sets of two thermocouples in each quadrant ensure a single failure will not disable the ability to determine the radial temperature gradient.

For loop and steam generator related variables, the required information is individual loop temperature and individual steam generator level. In these cases two channels are required OPERABLE for each loop of steam generator to redundantly provide the necessary information.

In the case of Containment Isolation Valve Position, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of passive valve or system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

A PAM channel is OPERABLE when:

1. All channel components necessary to provide the required indication are functional;

(continued)

(continued)

BASES (continued)

LCO (continued)

2. Channel measurement uncertainties are known via test, analysis, or design information to be sufficiently small such that measurement and indication errors will not mislead operators into actions that would challenge plant safety; and

3. Required Surveillance testing is current and has demonstrated performance within each surveillance test's acceptance criteria.

LCO Table 3.3.5-1 is for illustration purposes only. Plant-specific TS tables will list all Type A and Category 1 variables identified by the plant's Regulatory Guide 1.97 analysis, as amended by NRC's plant-specific Safety Evaluation Report.

[For this facility, the following support systems are required to be OPERABLE to ensure PAM instrumentation OPERABILITY:]

[For this facility, those required support systems which upon their failure do not result in declaring the PAM instrumentation inoperable and their justification are as follows:]

APPLICABILITY

The PAM instrumentation LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and preplanned actions required to mitigate DBEs. The applicable DBAs are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, plant conditions are such that the likelihood of an event occurring which would require PAM instrumentation is low; therefore, the PAM instrumentation is not required to be OPERABLE in these MODES.

A Note indicates that the provisions of LCO 3.0.4 are not applicable to the functions contained in the LCO. A second Note provides clarification that each function specified in the Table 3.3.5-1 is treated as an independent entity for this LCO with an independent Completion Time.

(continued)

BASES (continued)

ACTIONS

A channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined for each function in the LCO section of the Bases.

Condition A

When one required channel in one or more functions is inoperable, each inoperable channel must be restored to OPERABLE status within 30 days. In some channels it may be possible to have one PAM channel inoperable, but still have all required channels OPERABLE. For example, some plants have four equivalent channels available to perform certain PAM functions. In these cases, the failure of one or two of the channels leaves at least two channels OPERABLE to meet the LCO requirements. Therefore, for this example, Condition A need not be entered unless three channels fail. The 30-day Completion Time is based on operating experience and takes into account the remaining OPERABLE channels and the low probability of an event requiring PAM instrumentation during this interval.

Condition B

With two required channels inoperable in one or more functions, at least one channel in each function should be restored to OPERABLE status within 7 days. The Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrument operation and the availability of alternate means to obtain the required information. Continuous operation with two required channels inoperable is not acceptable because the alternate indications may not fully meet all performance of qualification requirements applied to the PAM instrumentation. Therefore, requiring restoration of at least one inoperable channel limits the risk that the PAM function will be in degraded condition should an accident occur.

Condition C

Required Action C.1 directs the operator to follow the directions given in Table 3.3.5-1 for entering either Conditions D or E immediately.

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

Condition D

For the majority of functions in Table 3.3.5-1, if the Required Actions and associated Completion Times of Condition A or B are not met, then the plant must be placed in a MODE in which the LCO requirements are not applicable. This is done by placing the plant in MODE 3 within 6 hours and MODE 4 within 12 hours. The Completion Times are reasonable, based on operating experience, to reach the required MODES from full power operation in an orderly manner and without challenging plant systems.

Condition E

At this facility, alternate means of monitoring [reactor vessel water level and containment area radiation] have been developed and tested. These alternate means may be temporarily installed if the normal PAM channel(s) cannot be restored to OPERABLE status within the allotted time. If these alternate means are invoked, the Required Action is not to shut the plant down but rather to follow the directions of LCO 5.9.2, "Special Reports," in the Administrative Controls section of the TS. The report provided to the NRC should discuss the alternate means invoked, describe the degree to which the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels.

[At this facility, the alternate monitoring provisions consist of the following:]

SURVEILLANCE REQUIREMENTS

The following SRs apply to each PAM instrumentation function in Table 3.3.5-1.

SR 3.3.5.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. A CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION. The high radiation instrumentation should be compared to similar plant instruments located throughout the plant. If the radiation monitor employs keep-alive sources or check sources operable from the control room, the CHANNEL CHECK should also note the detector's response to these sources.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment have drifted outside their limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off-scale during time when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off-scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given function in any 31-day interval is a rare event. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel during normal operational use of the displays associated with this LCO's required channels.

SR 3.3.5.2

A CHANNEL CALIBRATION is performed every 18 months, or approximately every refueling. CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies the channel responds to the measured parameter with the necessary range and accuracy. For OPERABLE channels, CHANNEL CALIBRATION shall find that

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

measurement errors are within the assumptions of the plant-specific setpoint analysis and are sufficiently small such that measurement and indication errors will not mislead operators into actions that would challenge plant safety.

Transmitter "as found" and "as left" values are recorded and used to verify drift assumptions. Field transmitters may be calibrated in place, removed and calibrated in a laboratory, or replaced with an equivalent, laboratory calibrated, unit.

Resistance temperature detector (RTD) and thermocouple (T/C) channels may be calibrated in place using cross calibration techniques, or in a test bath after removal from piping. For cross calibration, at least one sensor should be replaced with a newly calibrated sensor during each refueling cycle to ensure accurate sensor cross calibration. This replacement sensor should be the same model as the remaining RTDs or T/Cs. Using a newly calibrated sensor as a reference assures sensor signal drift continues to remain random rather than systematic, and is within the limits specified. The replacement interval may be extended to alternate refueling if it is demonstrated that over the extended interval, the sensor drift is random rather than systematic. This determination may use results of statistical analysis of operating data and calibration data from similar plants using the same model of RTD or T/C in the same environmental conditions.

Recalibration restores operability of an otherwise functional component that does not meet these criteria. However, repeated failures of the same channel over a relatively small number of test intervals must be considered as potentially indicating a deterministic failure which cannot be corrected by recalibration.

For the containment area radiation instrumentation, a CHANNEL CALIBRATION may consist of an electronic calibration of the channel, not including the detector, for range decades above 10 R/hr, and one-point calibration check of the detector below 10 R/hr with a gamma source.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)	The Surveillance Frequency is based upon the assumption of an 18-month calibration interval in the determination of the magnitude of equipment drift.
REFERENCES	1. [Plant-specific document (e.g., FSAR, NRC Regulatory Guide 1.97 SER letter).] 2. U.S. NRC Regulatory Guide 1.97, "Instrumentation for Light-Water Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." 3. U.S. NRC NUREG 0737, Supplement 1, "Clarification of TMI Action Plan Requirements." 4. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

B 3.3 INSTRUMENTATION

B 3.3.6 Remote Shutdown System (Analog and Digital)

BASES

BACKGROUND

The Remote Shutdown System provides the control room operator with sufficient instrumentation and controls to place and maintain the facility in a safe shutdown condition from a location other than the control room. This capability is necessary to protect against the possibility that the control room becomes inaccessible or a fire destroying all equipment in one facility fire area disables critical control room instruments or controls. A safe shutdown condition is defined as MODE 3. With the facility in MODE 3, the [Auxiliary Feedwater (AFW) System] and the steam generator (SG) safety valves or the SG atmospheric dump valves can be used to remove core decay heat and meet all safety requirements. The long-term supply of water for the [AFW System] and the ability to borate the Reactor Coolant System (RCS) from outside the control room allows extended operation in MODE 3.

In the event that the control room becomes inaccessible, or a fire disables critical control or display functions in the control room, the operators can establish control at the remote shutdown panel, and place and maintain the facility in MODE 3. Not all controls and the necessary transfer switches are located at the remote shutdown panel. Some controls and transfer switches will be operated locally at the switchgear, motor control panels, or other local stations. The facility automatically reaches MODE 3 following a facility shutdown and can be maintained safely in MODE 3 for an extended period of time.

The OPERABILITY of the Remote Shutdown System control and instrumentation functions ensure that there is sufficient information available on selected plant parameters to place and maintain the plant in MODE 3 should the control room become inaccessible or critical control room displays or controls become unavailable.

APPLICABLE SAFETY ANALYSES

The Remote Shutdown System is required to provide equipment at appropriate locations outside the control room with a

(continued)

(continued)

APPLICABLE SAFETY ANALYSES (continued)

capability to promptly shut down and maintain the plant in a safe Condition in MODE 3.

Furthermore, in the event of a fire in any one plant fire area, the Remote Shutdown System is designed to ensure one train of systems necessary to achieve and maintain MODE 3 Conditions from either the control room or emergency control station(s). The criteria governing the design of the Remote Shutdown System are 10 CFR 50, Appendix A, GDC 19 and Appendix R.

Specific system requirements are presented in Reference 1 and the NRC staff approved plant-specific fire protection topical report.

The Remote Shutdown System is considered an important contributor to the reduction in risk of plant accidents and as such it has been retained in the Technical Specifications as indicated in the NRC Interim Policy Statement.

LCO

The Remote Shutdown System LCO provides the requirements for the OPERABILITY of the instrumentation and controls necessary to place and maintain the plant in MODE 3 from a location other than the control room. The instrumentation and controls typically required are listed in Table B 3.3.6-1, following this specification. For Remote Shutdown System channels that support only the functions required by 10 CFR 50, Appendix R, one division is required to be OPERABLE.

For channels that fulfill GDC 19 requirements for the number of OPERABLE channels required, depends upon the plant's licensing basis as described in the NRC plant-specific Safety Evaluation Report (SER). Generally, two divisions are required OPERABLE. However, only one channel is required if the plant has justified such a design, and the NRC's SER accepted the justification. The controls, instrumentation, and transfer switches are those required for:

a. Core Reactivity Control (initial and long term);

b. RCS Pressure Control;

(continued)

(continued)

LCO (continued)

c. Decay Heat Removal via the [AFW System] and the safety valves or SG atmospheric dump valves;

d. RCS Inventory Control via charging flow; and

e. Safety support systems for the above functions, as well as service water, component cooling water, and onsite power, including the diesel generators.

A division of a Remote Shutdown System is OPERABLE if all instrument and control channels needed to support the remote shutdown functions are OPERABLE in that Division. In some cases, Table B 3.3.6-1 may indicate that the required information or control capability is available from several alternate sources. In these cases, the division is OPERABLE as long as one channel of any of the alternate information or control sources for each function is OPERABLE.

Remote Shutdown System instrumentation channels are OPERABLE when:

a. All channel components necessary to provide the required indication are functional;

b. Channel measurement uncertainties are known via test, analysis, or design information to be sufficiently small such that measurement and indication errors will not mislead operators into actions that would challenge plant safety limits or prevent prompt entry into MODE 3; and

c. Required surveillance testing is current and has demonstrated performance within each surveillance test's acceptance criteria.

Remote Shutdown System controls are OPERABLE when:

a. All channel components, including transfer switches necessary to provide remote shutdown control are functional; and

(continued)

(continued)

BASES (continued)

LCO (continued)

b. Required surveillance testing is current and has demonstrated performance within each surveillance test's acceptance criteria.

The Remote Shutdown System equipment covered by this LCO does not need to be in operation to be considered OPERABLE. This LCO is intended to ensure that the equipment will be OPERABLE if plant Conditions require that the Remote Shutdown System be placed in operation.

For this facility, a Remote Shutdown System Division is considered OPERABLE when all the plant-specific instrumentation, controls, transfer switches and support systems listed in Table B 3.3.6-1 are OPERABLE.

[For this facility, the following support systems are required to be OPERABLE to ensure Remote Shutdown System OPERABILITY:]

[For this facility, those required support systems which, upon their failure, do not declare the Remote Shutdown System inoperable and their justification are as follows:]

APPLICABILITY

The Remote Shutdown System LCO is applicable in MODES 1, 2, and 3. This is required so that the facility can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.

This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the facility is already subcritical and in the Condition of reduced RCS energy. Under these Conditions, considerable time is available to restore necessary instrument control functions if control room instruments or control become unavailable.

A Note has been added to indicate that LCO 3.0.4 does not apply to the Remote Shutdown System LCO. This exception to LCO 3.0.4 allows normal startup during the period when the Remote Shutdown System is inoperable. Normal startup may proceed while in Condition A because the justification for Condition A Action and Completion Time are equally applicable to startup Conditions as to continued operation in MODE 1, 2, or 3. Furthermore, Remote Shutdown System

(continued)

(continued)

BASES (continued)

APPLICABILITY (continued)

equipment can generally be repaired during operation without significant risk of spurious trip.

ACTIONS

A Remote Shutdown System Division is inoperable when each function listed in Table B 3.3.6-1 is not accomplished by at least one designated Remote Shutdown System channel that satisfies the OPERABILITY criteria for the channel's function. These criteria are outlined in the LCO section of the bases.

Condition A

Condition A addresses the situation where one or more Divisions of the Remote Shutdown System is inoperable. This includes any function listed in Table B 3.3.6-1 as well as the control and transfer switches.

When a Division includes a function that only requires one channel to be OPERABLE, the failure of the single channel constitutes the failure of the function, and as a consequence, the Division becomes inoperable.

The Required Action is to restore the Divisions to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room.

For this LCO, a Note has been added to provide clarification that each [Division] is treated as an independent entity with an independent Completion Time.

Condition B

If the inoperable Division cannot be restored to OPERABLE status within 30 days, the prudent action is to place the plant in a MODE in which the LCO requirements are not applicable. This is done by placing the plant in at least MODE 3 within 6 hours and in MODE 4 within 12 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required MODES from full power in an orderly manner and without challenging plant systems.

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS

The following SRs apply to each Remote Shutdown System division.

SR 3.3.6.1

Performance of the CHANNEL CHECK once every 31 days ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value.

Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. CHANNEL CHECK will detect gross channel failure, thus it is key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION. Remote Shutdown System instrumentation should be compared to similar plant instruments located in the control room. Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the match criteria, it may be an indication that the transmitter or the signal processing equipment have drifted outside its limit. If the channels are within the match criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when Surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off-scale low current-loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Surveillance Frequency of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift which demonstrates that failure of more than one channel of a given function in any 31-day interval is a rare event.

SR 3.3.6.2

SR 3.3.6.2 verifies that each required Remote Shutdown System transfer switch and control circuit perform their intended function. This verification is performed from the

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

reactor shutdown panel and locally, as appropriate. This will ensure that if the control room becomes inaccessible, the unit can be placed and maintained in MODE 3 from the reactor shutdown panel and the local control stations. The 18-month interval was established as these Surveillances can only be performed during a facility outage. This was due to the plant conditions needed to perform the surveillance and the potential for unplanned transients if the surveillance is performed with the reactor at power. Operating experience demonstrates that Remote Shutdown System control channels seldom fail to pass the surveillance when performed on the 18-month interval.

<u>SR 3.3.6.3</u>

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector. The test verifies that the channel responds to measured parameter with the necessary range and accuracy.

Transmitter "as found" and "as left" values are recorded and used to verify drift assumptions. Field transmitters may be calibrated in place, removed and calibrated in a laboratory, or replaced with an equivalent laboratory-calibrated unit.

Resistance temperature detector (RTD) channels may be calibrated in place using cross-calibration techniques, or in a test bath after removal from piping. For cross calibration, at least one RTD should be replaced with a newly calibrated RTD during each refueling cycle to ensure accurate RTD cross calibration. This replacement RTD must be the same model as the remaining RTDs. The use of a newly calibrated RTD as a reference, ensures that RTD signal drift remains random rather than systematic, and is within the limits specified in the plant-specific setpoint analysis. The replacement interval may be extended to alternate refueling if it is demonstrated that over the extended interval, the RTD's drift is random rather than systematic. This determination may be the result of the statistical analyses of operating and calibration data from similar plants, using the same model of RTD in the same environmental conditions.

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

The Surveillance Frequency is based upon the assumption of an 18-month calibration interval, in the determination of the magnitude of equipment drift.

SR 3.3.6.4

SR 3.3.6.4 is the performance of a CHANNEL FUNCTIONAL TEST every 18 months. This test should verify the OPERABILITY of the reactor trip circuit breakers (RTCBs) open/closed indication on the remote shutdown panels, by actuating the RTCBs. The Surveillance Frequency of 18 months was chosen because the RTCBs cannot be exercised while the facility is at power. Operating experience has shown that these components usually pass the Surveillance when performed on an 18-month interval. Therefore the Frequency was concluded to be acceptable from a reliability standpoint.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, General Design Criterion 19, and Appendix R.

2. [Unit Name] FSAR, Chapter [ ], "[Title]."

Table B 3.3.6-1 (page 1 of 2)
Remote Shutdown System Instrumentation and Controls

FUNCTION/INSTRUMENT OR CONTROL PARAMETER	LOCATION	REQUIRED NUMBER OF DIVISIONS
---NOTE--- This table is for illustration purposes only. It does not attempt to encompass every function used at every plant, but does contain the types of functions commonly found.		
1. Reactivity Control		
a. Log Power Neutron Flux		[1]
b. Source Range Neutron Flux		[1]
c. Reactor Trip Circuit Breaker Position		[1 per trip breaker]
d. Manual Reactor Trip		[4]
2. Reactor Coolant System Pressure Control		
a. Pressurizer Pressure <u>OR</u> RCS Wide Range Pressure		[1]
b. Pressurizer Power Operated Relief Valve (PORV) Control and Block Valve Control		[1, controls must be for PORV & block valves on same line]
3. Decay Heat Removal via Steam Generators		
a. Reactor Coolant Hot Leg Temperature		[1 per loop]
b. Reactor Coolant Cold Leg Temperature		[1 per loop]

(continued)

(continued)

Table B 3.3.6-1 (page 2 of 2)
Remote Shutdown System Instrumentation and Controls

FUNCTION/INSTRUMENT OR CONTROL PARAMETER	LOCATION	REQUIRED NUMBER OF DIVISIONS
c. Auxiliary Feedwater Controls		[1]
d. Steam Generator Pressure		[1 per SG]
e. Steam Generator Level <u>OR</u> Auxiliary Feedwater Flow		[1 per SG]
f. Condensate Storage Tank Level		[1]
4. Reactor Coolant System Inventory Control		
a. Pressurizer Level		[1]
b. Reactor Coolant Injection Pump Controls		[1]

B 3.3 INSTRUMENTATION

B 3.3.7 <u>[Logarithmic] Power Monitoring Channels</u> (Analog and Digital)

BASES

BACKGROUND

The [logarithmic] [wide-range] power monitoring channels provide neutron flux power indication from below 1E-7% RATED THERMAL POWER (RTP) to greater than 100% RTP. They also provide reactor protection when the reactor trip circuit breakers (RTCBs) are shut, in the form of a Power Rate of Change--High (analog plants), or a Logarithmic Power Level--High Trip (digital plants).

This specification addresses MODES 3, 4, and 5 with the RTCBs open. When the RTCBs are shut, the logarithmic power monitoring channels are addressed by LCO 3.3.1, "Reactor Protection System (RPS) Instrumentation."

When the RTCBs are open, two of the four wide-range power channels must be available to monitor neutron flux power. In this application, the Reactor Protection System (RPS) channels need not be OPERABLE, since the reactor trip function is not required. By monitoring neutron flux power when the RTCBs are open, loss of SHUTDOWN MARGIN caused by boron dilution can be detected as an increase in flux. Alarms are also provided when power increases above the fixed bistable setpoints. For plants employing separate post-accident, wide-range nuclear instrumentation channels with adequate range, these can be substituted for the logarithmic power-range channels. Two channels must be OPERABLE to provide single-failure protection, and to facilitate detection of channel failure by providing channel check capability.

APPLICABLE SAFETY ANALYSES

The logarithmic power monitoring channels are necessary to monitor core reactivity changes. They are the primary means for detecting and triggering operator actions to respond to reactivity transients initiated from Conditions in which the RPS is not required to be OPERABLE. They also trigger operator actions to anticipate RPS actuation in the event of reactivity transients starting from shutdown or low-power Conditions. The logarithmic power monitoring channel's LCO requirements support compliance with 10 CFR 50, Appendix A,

(continued)

(continued)

BASES (continued)

APPLICABLE SAFETY ANALYSES (continued)

GDC 13 (Ref. 1). Reference 2 describes the specific features that are critical to compliance with the GDC.

The OPERABILITY of logarithmic power monitoring channels is necessary to meet the assumptions of the safety analyses and provide for the mitigation of accident and transient Conditions.

The logarithmic power monitoring channels satisfy Criterion 3 of the NRC Interim Policy Statement.

LCO

The LCO on the logarithmic power monitoring channels ensures that adequate information is available to verify core reactivity conditions while shutdown.

A minimum of two logarithmic power monitoring channels are required to be OPERABLE. Some plants may have four or six channels capable of performing this function. In these cases, multiple failures may be tolerated while still complying with LCO requirements. [At this facility, the following logarithmic power monitoring functions are covered by this LCO (e.g., indication only, indication and alarms, or indication and inhibits).]

A logarithmic power monitoring channel is OPERABLE when:

a. All channel components necessary to provide the required indication are functional;

b. Channel measurement uncertainties are known via test, analysis, or design information to be sufficiently small such that measurement and indication errors will not mislead operators into actions that would challenge plant safety limits; and

c. Required Surveillance testing is current and has demonstrated performance within each Surveillance test's acceptance criteria.

[For this facility, the following support systems are required to be OPERABLE to ensure logarithmic power monitoring channel OPERABILITY:]

(continued)

(continued)

BASES (continued)

LCO (continued)

[For this facility, those required support systems which, upon their failure, do not declare the logarithmic power monitoring channels inoperable and their justification are as follows:]

APPLICABILITY

In MODES 3, 4, and 5, with RTCBs open or Control Element Assembly (CEA) Drive System not capable of CEA withdrawal, logarithmic power monitoring channels must be OPERABLE to monitor core power for reactivity changes. In MODES 1 and 2, and in MODES 3, 4, and 5, with the RTCBs shut and the CEAs capable of withdrawal, the logarithmic power monitoring channels are addressed as part of the RPS in LCO 3.3.1.

The requirements for source range neutron flux monitoring in MODE 6 are addressed in LCO 3.9.2. The source range nuclear instrumentation channels provide neutron flux coverage extending an additional one to two decades below the logarithmic channels, for use during refueling, when neutron flux may be extremely low. They are built into the wide range neutron flux channels in the analog plants and in many of the post-accident channels used in both the digital and analog plants.

ACTIONS

A channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. These criteria are outlined in the LCO section of the Bases.

<u>Condition A</u>

With one required channel inoperable, it may not be possible to perform a CHANNEL CHECK to verify that the other required channel is OPERABLE. Therefore, with one or more required channels inoperable the logarithmic power monitoring function cannot be reliably performed. Consequently the Required Actions are the same for one required channel inoperable or more than one required channel inoperable. The absence of reliable neutron flux indication makes it difficult to ensure SHUTDOWN MARGIN is maintained. Required Action A.1 therefore requires that all positive reactivity additions that are under operator control, such as boron

(continued)

(continued)

BASES (continued)

ACTIONS (continued)

dilution or Reactor Coolant System (RCS) temperature changes, be halted immediately, preserving SHUTDOWN MARGIN.

SHUTDOWN MARGIN must be verified periodically to ensure that it is being maintained. Both required channels must be restored as soon as possible. The initial 4 hours and once per 12 hours thereafter to perform SHUTDOWN MARGIN verification takes into consideration that Required Action [illegible] eliminates many of the means by which SHUTDOWN MARGIN can be reduced. These Completion Times are also based on operating experience in performing the Required Actions and the fact that plant Conditions will change slowly.

SURVEILLANCE REQUIREMENTS

<u>SR 3.3.7.1</u>

SR 3.3.7.1 is the performance of a CHANNEL CHECK on each required channel every 12 hours. A CHANNEL CHECK is a comparison of the parameter indicated on one channel to a similar parameter on another channel. It is based upon the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or even something more serious. CHANNEL CHECK will detect gross channel failure, thus it is the key to verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the plant staff and should be based on a combination of the channel instrument uncertainties, including control isolation, indication, and readability. If a channel is outside of the match criteria, it may be an indication that the transmitter or the signal-processing equipment has drifted outside of its limits. If the channels are within the match criteria, it is an indication that the channels are OPERABLE.

The Surveillance interval, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. Thus, the performance of CHANNEL CHECK ensures that undetected overt channel failure is limited

(continued)

(continued)

BASES (continued)

SURVEILLANCE REQUIREMENTS (continued)

to 12 hours. Since the probability of two random failures in redundant channels, in any 12-hour period, is extremely low, CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. CHANNEL CHECK supplements less formal, but more frequent checks of channel operability during normal operational use of displays associated with the LCO required channels.

SR 3.3.7.2

A CHANNEL FUNCTIONAL TEST is performed ever 92 days to ensure that the entire channel is capable of properly indicating neutron flux. Internal test circuitry is used to feed preadjusted test signals into the preamplifier to verify channel alignment. It is not necessary to test the detector, because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This test interval is the same as that employed for the same channels in the other applicable MODES. [At this facility, the channel trip functions tested by the CHANNEL FUNCTIONAL TEST are as follows:]

SR 3.3.7.3

SR 3.3.6.3 is a the performance of a CHANNEL CALIBRATION. A CHANNEL CALIBRATION is performed every 18 months. The test is a complete check and readjustment of the logarithmic power channel from the preamplifier input through to the remote indicators. This SR is modified by a Note to indicate that it is not necessary to test the detector, because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This test interval is the same as that employed for the same channels in the other applicable MODES.

REFERENCES

1. Title 10, Code of Federal Regulations, Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

2. [Unit Name] FSAR, Section [7], "[Title]," and Section [15], "[Title]."

APPENDIX A

Acronyms

The following acronyms are used, but not defined, in the Standard Technical Specifications:

AC	alternating current
CFR	Code of Federal Regulations
DC	direct current
FSAR	Final Safety Analysis Report
LCO	Limiting Condition for Operation
SR	Surveillance Requirement
GDC	General Design Criteria or General Design Criterion

The following acronyms are used, with definitions, in the Standard Technical Specifications:

ACOT	ANALOG CHANNEL OPERATIONAL TEST
ADS	Automatic Depressurization System
ADV	atmospheric dump valve
AFD	axial flux difference
AFW	auxiliary feedwater
AIRP	air intake, recirculation, and purification
ALARA	as low as reasonably achievable
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	anticipated operational occurrence
AOT	allowed outage time
APD	axial power distribution
APLHGR	average planar linear heat generation rate
APRM	average power range monitor
APSR	axial power shaping rod
ARO	all rods out
ARC	auxiliary relay cabinets
ARS	Air Return System
ARTS	Anticipatory Reactor Trip System
ASGT	asymmetric steam generator transient
ASGTPTF	asymmetric steam generator transient protective trip function
ASI	AXIAL SHAPE INDEX
ASME	American Society of Mechanical Engineers

(continued)

APPENDIX A (continued)

ASTM	American Society for Testing Materials
ATWS	anticipated transient without scram
ATWS-RPT	anticipated transient without scram recirculation pump trip
AVV	atmospheric vent valve
BAST	boric acid storage tank
BAT	boric acid tank
BDPS	Boron Dilution Protection System
BIST	boron injection surge tank
BIT	boron injection tank
BOC	beginning of cycle
BOP	balance of plant
BPWS	banked position withdrawal sequence
BWST	borated water storage tank
BTP	Branch Technical Position
CAD	containment atmosphere dilution
CAOC	constant axial offset control
CAS	Chemical Addition System
CCAS	containment cooling actuation signal
CCGC	containment combustible gas control
CCW	component cooling water
CEA	control element assembly
CEAC	control element assembly calculator
CEDM	control element drive mechanism
CFT	core flood tank
CIAS	containment isolation actuation signal
COLR	CORE OPERATING LIMITS REPORT
COLSS	Core Operating Limits Supervisory System
CPC	core protection calculator
CPR	critical power ratio
CRA	control rod assembly
CRD	control rod drive
CRDA	control rod drop accident
CRDM	control rod drive mechanism
CREHVAC	Control Room Emergency Air Temperature Control System
CREFS	Control Room Emergency Filtration System
CREVS	Control Room Emergency Ventilation System
CRFAS	Control Room Fresh Air System
CS	core spray
CSAS	containment spray actuation signal

(continued)

CST	condensate storage tank
CVCS	Chemical and Volume Control System
DBA	Design Basis Accident
DBE	Design Basis Event
DF	decontamination factor
DG	diesel generator
DIV	drywell isolation valve
DNB	departure from nucleate boiling
DNBR	departure from nucleate boiling ratio
DOP	dioctyl phthalate
DPIV	drywell purge isolation valve
DRPI	digital rod position indicator
EAB	exclusion area boundary
ECCS	Emergency Core Cooling System
ECW	essential chilled water
ECP	estimated critical position
EDG	emergency diesel generator
EFAS	Emergency Feedwater Actuation System
EFIC	emergency feedwater initiation and control
EFCV	excess flow check valve
EFPDs	effective full power days
EFPYs	effective full power years
EFW	emergency feedwater
EHC	electro-hydraulic control
EOC	end of cycle
EOC-RPT	end of cycle recirculation pump trip
ESF	engineered safety feature
ESFAS	Engineered Safety Feature Actuation System
ESW	essential service water
EVS	Emergency Ventilation System
FBACS	Fuel Building Air Cleanup System
FCV	flow control valve
FHAVS	Fuel Handling Area Ventilation System
FSPVS	Fuel Storage Pool Ventilation System
FRC	fractional relief capacity
FR	Federal Register
FTC	fuel temperature coefficient
FWLB	feedwater line break

(continued)

HCS	Hydrogen Control System; Hydrazine Control System
HCU	hydraulic control unit
HIS	Hydrogen Ignition System
HELB	high energy line break
HEPA	high efficiency particulate air
HMS	Hydrogen Mixing System
HPCI	high pressure coolant injection
HPCS	high pressure core spray
HPI	high pressure injection
HPSI	high pressure safety injection
HPSP	high power setpoint
HVAC	heating, ventilation, and air conditioning
HZP	hot zero power
ICS	Iodine Cleanup System
IEEE	Institute of Electrical and Electronic Engineers
IGSCC	intergranular stress corrosion cracking
IRM	intermediate range monitor
ISLH	inservice leak and hydrostatic
ITC	isothermal temperature coefficient
K-relay	control relay
LCS	Leakage Control System
LEFM	linear elastic fracture mechanics
LER	Licensee Event Report
LHGR	linear heat generation rate
LHR	linear heat rate
LLS	low-low set
LOCA	loss-of-coolant accident
LOCV	loss of condenser vacuum
LOMFW	loss of main feedwater
LOP	loss of power
LOPS	loss of power start
LOVS	loss of voltage start
LPCI	low pressure coolant injection
LPCS	low pressure core spray
LPD	local power density
LPI	low pressure injection
LPRM	local power range monitor
LPSI	low pressure safety injection
LPSP	low power setpoint

(continued)

LPZ	low population zone
LSSS	limiting safety system settings
LTA	lead test assembly
LTOP	low temperature overpressure protection
MAPLHGR	maximum average planar linear heat generation rate
MAPFAC	MAPLHGR factor
$MAPFAC_f$	MAPLHGR factor, flow-dependent component
$MAPFAC_p$	MAPLHGR factor, power-dependent component
MCPR	minimum critical power ratio
MCR	main control room
MCREC	main control room environmental control
MFI	maximum flow interlock
MFIV	main feedwater isolation valve
MFLPD	maximum fraction of limiting power density
MFRV	main feedwater regulation valve
MFW	main feedwater
MG	motor generator
MOC	middle of cycle
MSIS	main steam isolation signal
MSIV	main steam isolation valve
MSLB	main steam line break
MSSV	main steam safety valve
MTC	moderator temperature coefficient
NDT	nil-ductility temperature
NDTT	nil-ductility transition temperature
NI	nuclear instrument
NIS	Nuclear Instrumentation System
NMS	Neutron Monitoring System
NPSH	net positive suction head
NSSS	Nuclear Steam Supply System
ODCM	Offsite Dose Calculation Manual
OPDRV	operation with a potential for draining the reactor vessel
OTSG	once-through steam generator
PAM	post-accident monitoring
PCCGC	primary containment combustible gas control
PCI	primary containment isolation

(continued)

PCIV	primary containment isolation valve
PCHRS	Primary Containment Hydrogen Recombiner System
PCP	Process Control Program
PCPV	primary containment purge valve
PCT	peak cladding temperature
PDIL	power dependent insertion limit
PDL	power distribution limit
PF	position factor
PIP	position indication probe
PIV	pressure isolation valve
PORV	power operated relief valve
PPS	Plant Protective System
PRA	probabilistic risk assessment
PREACS	Pump Room Exhaust Air Cleanup System: Penetration Room Exhaust Air Cleanup System
PSW	plant service water
P/T	pressure and temperature
PTE	PHYSICS TEST exception
PTLR	PRESSURE AND TEMPERATURE LIMITS REPORT
QA	quality assurance
QPT	quadrant power tilt
QPTR	quadrant power tilt ratio
QS	quench spray
RACS	Rod Action Control System
RAOC	relaxed axial offset control
RAS	recirculation actuation signal
RB	reactor building
RBM	rod block monitor
RCCA	rod cluster control assembly
RCIC	reactor core isolation cooling
RCIS	Rod Control and Information System
RCP	reactor coolant pump
RCPB	reactor coolant pressure boundary
RCS	Reactor Coolant System
REA	rod ejection accident
RHR	residual heat removal
RHRSW	residual heat removal service water
RMCS	Reactor Manual Control System
RPB	reactor pressure boundaries
RPC	rod pattern controller
RPCB	reactor power cutback

(continued)

APPENDIX A (continued)

RPIS	Rod Position Information System
RPS	Reactor Protection System
RPV	reactor pressure vessel
RS	recirculation spray
RT	reference temperature
RT_{NDT}	nil-ductility reference temperature
RTCB	reactor trip circuit breaker
RTD	resistance temperature detector
RTM	reactor trip module
RTP	RATED THERMAL POWER
RTS	Reactor Trip System
RWCU	reactor water cleanup
RWE	rod withdrawal error
RWL	rod withdrawal limiter
RWM	rod worth minimizer
RWP	Radiation Work Permit
RWST	refueling water storage tank
RWT	refueling water tank
SAFDL	specified acceptable fuel design limits
SBCS	Steam Bypass Control System
SBO	station blackout
SBVS	Shield Building Ventilation System
SCAT	spray chemical addition tank
SCI	secondary containment isolation
SCR	silicon controlled rectifier
SDC	shutdown cooling
SDV	scram discharge volume
SDM	SHUTDOWN MARGIN
SER	Safety Evaluation Report
SFRCS	Steam and Feedwater Rupture Control System
SG	steam generator
SGTR	steam generator tube rupture
SGTS	Standby Gas Treatment System
SI	safety injection
SIAS	safety injection actuation signal
SIS	safety injection signal
SIT	safety injection tank
SJAE	steam jet air ejector
SL	Safety Limit
SLB	steam line break
SLC	standby liquid control
SLCS	Standby Liquid Control System
SPMS	Suppression Pool Makeup System
SRM	source range monitor

(continued)

APPENDIX A (continued)

S/RV	safety/relief valve
S/RVDL	safety/relief valve discharge line
SSPS	Solid State Protection System
SSW	standby service water
SWS	Service Water System
STE	special test exception
STS	Standard Technical Specifications
TADOT	trip actuating device operational test
TCV	turbine control valve
TIP	transversing incore probe
TLD	thermoluminescent dosimeter
TM/LP	thermal margin/low pressure
TS	Technical Specifications
TSV	turbine stop valve
UHS	Ultimate Heat Sink
VCT	volume control tank
VFTP	Ventilation Filter Testing Program
VHPT	variable high power trip
v/o	volume percent
VS	vendor specific
ZPMB	zero power mode bypass

NRC FORM 335 (2-89) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER (Assigned by NRC. Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-1432
Vol. 2

2. TITLE AND SUBTITLE

Standard Technical Specifications
Combustion Engineering Plants

Bases (Sections2.0 - 3.3)

Draft Report for Comment

3. DATE REPORT PUBLISHED

MONTH	YEAR
January	1991

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

6. TYPE OF REPORT

DRAFT

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION – NAME AND ADDRESS (If NRC, provide Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Operational Events Assessment
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

9. SPONSORING ORGANIZATION – NAME AND ADDRESS (If NRC, type "Same as above"; if contractor, provide NRC Division, Office or Region, U.S. Nuclear Regulatory Commission, and mailing address.)

Same as above

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This draft report documents the results of the NRC staff review of new Standard Technical Specifications (STS) proposed by the Combustion Engineering Owners Group. The new STS were developed based on the criteria in the interim Commission Policy Statement on Technical Specification Improvements for Nuclear Power Reactors, dated February 6, 1987. The new STS will be used as bases for individual nuclear power plant owners to develop improved plant-specific technical specifications. The NRC staff is issuing this draft new STS for a 30 working-day comment period. Following the comment period, the NRC staff will analyze comments received, finalize the new STS, and issue them for plant-specific implementation. This report contains three volumes. Volume 1 contains the Specifications for all sections of the new STS. Volume 2 contains the Bases for Sections 2.0 - 3.3 of the new STS and Volume 3 contains the Bases for Sections 3.4 - 3.9 of the new STS.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Technical Specifications
Combustion Engineering
PWR

13. AVAILABILITY STATEMENT

Unlimited

14. SECURITY CLASSIFICATION

(This Page)

Unclassified

(This Report)

Unclassified

15. NUMBER OF PAGES

16. PRICE

NRC FORM 335 (2-89)