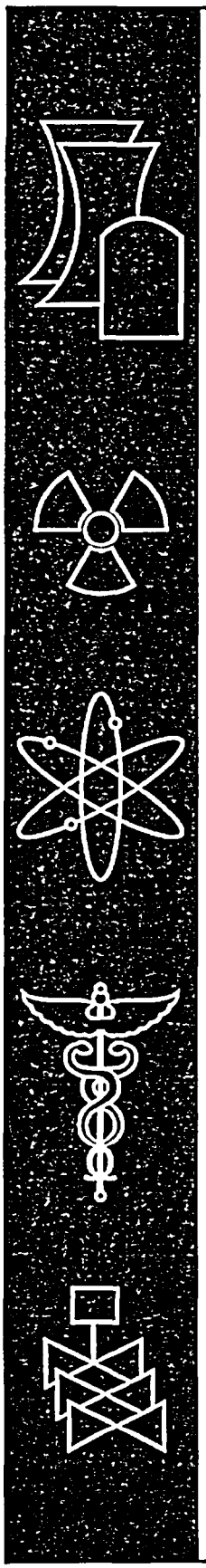
NUREG-1432
Vol. 2, Rev. 3



Standard Technical Specifications Combustion Engineering Plants

Bases

U.S. Nuclear Regulatory Commission
Office of Nuclear Reactor Regulation
Washington, DC 20555-0001

NUREG-1432
Vol. 2, Rev. 3

Standard Technical Specifications Combustion Engineering Plants

Bases

Manuscript Completed: March 2004
Date Published: June 2004

Division of Inspection Program Management
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202-512-1800
   Fax: 202-512-2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: Office of the Chief Information Officer,
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library 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—

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org
212–642–4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

PREFACE

This NUREG contains the improved Standard Technical Specifications (STS) for Combustion Engineering plants. Revision 3 incorporates the cumulative changes to Revision 1 and 2, which was published in April 1995 and April 2001, respectively. The changes reflected in Revision 3 resulted from the experience gained from license amendment applications to convert to these improved STS or to adopt partial improvements to existing technical specifications. This publication is the result of extensive public technical meetings and discussions among the Nuclear Regulatory Commission (NRC) staff and various nuclear power plant licensees, Nuclear Steam Supply System (NSSS) Owners Groups, and the Nuclear Energy Institute (NEI). The improved STS were developed based on the criteria in the Final Commission Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors, dated July 22, 1993 (58 FR 39132), which was subsequently codified by changes to Section 36 of Part 50 of Title 10 of the *Code of Federal Regulations* (10 CFR 50.36) (60 FR 36953). Licensees are encouraged to upgrade their technical specifications consistent with those criteria and conforming, to the practical extent, to Revision 3 to the improved STS. The Commission continues to place the highest priority on requests for complete conversions to the improved STS. Licensees adopting portions of the improved STS to existing technical specifications should adopt all related requirements, as applicable, to achieve a high degree of standardization and consistency.

The Table of Contents is now a Table of Contents / Revision Summary where the revision number and date are listed for each specification and bases, in lieu of traditional page numbers. Each limiting condition for operation (LCO) starts with page 1, with a specification, e.g., "2.0" or bases "B 2.0" number prefix. Subsequent approved revisions to sections will be noted in the Table of Contents, as well as on each affected page, using a decimal number to indicate the number of revisions to that section, along with the date, e.g., (Rev 3.3, 04/01/04) indicates the third approved change and date since Revision 3.0 was published. Additionally, the final page of each LCO section will be a historical listing of the changes affecting that section. This publication will be maintained in electronic format. Subsequent revisions will not be printed in hard copy. Users may access the subsequent revisions to the STS in the PDF format at (http://www.nrc.gov). This Web site will be updated as needed and the contents may differ from the last printed version. Users may print or download copies from the NRC Web site.

PAPERWORK REDUCTION ACT STATEMENT

The information collections contained in this NUREG are covered by the requirements of 10 CFR Parts 20 and 50, which were approved by the Office of Management and Budget, approval numbers 3150-0014 and 0011.

PUBLIC PROTECTION NOTIFICATION

If a means used to impose an information collection does not display a currently valid OMB control number, the NRC may not conduct or sponsor, and a person is not required to respond to, the information collection.

B 2.0 SAFETY LIMITS (SLs)

B 2.1.1 Reactor Core SLs (Analog)

BASES

BACKGROUND

GDC 10 (Ref. 1) requires and SLs ensure that specified acceptable fuel design limits are not exceeded during steady state operation, normal operation transients, and anticipated operational occurrences (AOOs). This is accomplished by having a departure from nucleate boiling (DNB) design basis, which corresponds to a 95% probability at a 95% confidence level (95/95 DNB criterion) 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 fuel centerline 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.

Fuel centerline 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 lose its integrity, resulting in an uncontrolled release of activity to the reactor coolant.

The Reactor Protective System (RPS), in combination with 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 violation of the reactor core SLs.

BASES

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 (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB and

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

The RPS setpoints, LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation," in combination with all the LCOs, are designed to prevent any anticipated combination of transient conditions for RCS temperature, pressure, and THERMAL POWER level that would result in a departure from nucleate 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 the following functions:

a. Pressurizer Pressure High trip,

b. Variable High Power trip,

c. Power Rate of Change - High trip,

d. Reactor Coolant Flow - Low trip,

e. Steam Generator Pressure - Low trip,

f. Steam Generator Level - Low trip,

g. Axial Power Distribution - High trip,

h. Thermal Margin/Low Pressure trip,

i. Steam Generator Pressure Difference trip, and

j. Steam Generator Safety Valves.

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 (ASI)," 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.

BASES

SAFETY LIMITS

The curves provided in Figure B 2.1.1-1 show the loci of points of THERMAL POWER, pressurizer pressure, and highest operating loop cold leg temperature, for which the minimum DNBR is not less than the safety analysis limit. SL 2.1.1.2 ensures that fuel centerline temperature remains below melting.

SL 2.1.1.2 ensures that fuel centerline temperature remains below the fuel melt temperature of [5080]°F during normal operating conditions or design AOOs with adjustments for burnup and burnable poison. An adjustment of [58°F per 10,000 MWD/MTU] has been established in [Topical Report CEN-386-P-A] (Ref. 3) and adjustments for burnable poisons are established based on [Topical Reports CENPD-275-P] (Ref. 4) and [CENPD-382-P-A] (Ref.5).

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 steam generator 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.

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

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the reactor core SLs.

2.2.1

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

The allowed Completion Time of 1 hour recognizes the importance of bringing the unit to a MODE of operation where this SL is not applicable and reduces the probability of fuel damage.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10, 1988.

2. FSAR, Section [ ].

3. [Topical Report CEN-386-P-A, "Verification of the Acceptability of a 1-Pin Burnup Limit of 60 MWD/kgU for Combustion Engineering 16x16 PWR Fuel," August 1992.]

4. [Topical Report CENPD-275-P, Revision 1-P-A, "CE Methodology for Core Designs Containing Gadolini-Urania Burnable Absorbers," May 1988.]

5. [Topical Report CENPD-382-P-A, "Methodology for Core Designs Containing Erbium Burnable Absorbers," August 1993.]

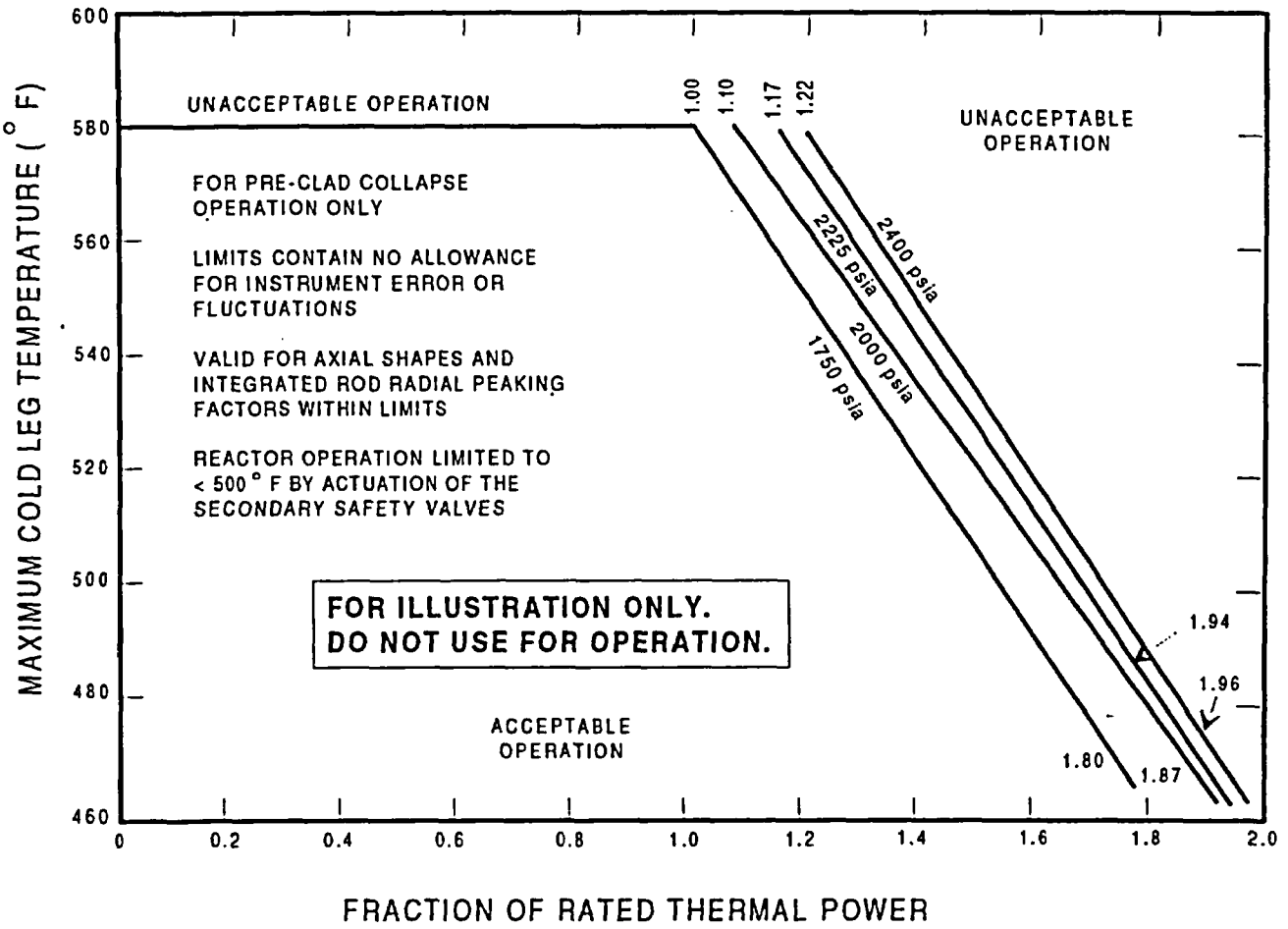


Figure 2.1.1-1 (page 1 of 1)
Reactor Core Thermal Margin Safety Limit

B 2.0 SAFETY LIMITS (SLs)

B 2.1.1 Reactor Core SLs (Digital)

BASES

BACKGROUND

GDC 10 (Ref. 1) requires and SLs ensure that specified acceptable fuel design limits are not exceeded during steady state operation, normal operational transients, and anticipated operational occurrences (AOOs). This is accomplished by having a departure from nucleate boiling (DNB) design basis, which corresponds to a 95% probability at a 95% confidence level (95/95 DNB criterion) 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 fuel centerline 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.

Fuel centerline 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.

The Reactor Protective System (RPS), in combination with 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 violation of the reactor core SLs.

BASES

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 (95/95 DNB criterion) that the hot fuel rod in the core does not experience DNB and

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

The RPS setpoints, LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation," in combination with all the LCOs, are designed to prevent any anticipated combination of transient conditions for RCS temperature, pressure, and THERMAL POWER level that would result in a departure from nucleate 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 the following functions:

a. Pressurizer Pressure - High trip,

b. Pressurizer Pressure - Low trip,

c. Linear Power Level - High trip,

d. Steam Generator Pressure - Low trip,

e. Local Power Density - High trip,

f. DNBR - Low trip,

g. Steam Generator Level - Low trip,

h. Reactor Coolant Flow - Low trip, and

i. Steam Generator Safety Valves.

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

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 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.

SL 2.1.1.2 ensures that fuel centerline temperature remains below the fuel melt temperature of [5080]°F during normal operating conditions or design AOOs with adjustments for burnup and burnable poison. An adjustment of [58°F per 10,000 MWD/MTU] has been established in [Topical Report CEN-386-P-A] (Ref. 3) and adjustments for burnable poisons are established based on [Topical Reports CENPD-275-P] (Ref. 4) and [CENPD-382-P-A] (Ref.5).

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 steam generator 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.

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

BASES

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the reactor core SLs. If SL 2.1.1.1 or SL 2.1.1.2 is violated, the requirement to go to MODE 3 places the unit in a MODE in which this SL is not applicable.

The allowed Completion Time of 1 hour recognizes the importance of bringing the unit to a MODE where this SL is not applicable and reduces the probability of fuel damage.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10, 1988.

2. FSAR, Section [ ].

3. [Topical Report CEN-386-P-A, "Verification of the Acceptability of a 1-Pin Burnup Limit of 60 MWD/kgU for Combustion Engineering 16x16 PWR Fuel," August 1992.]

4. [Topical Report CENPD-275-P, Revision 1-P-A, "CE Methodology for Core Designs Containing Gadolini-Urania Burnable Absorbers," May 1988.]

5. [Topical Report CENPD-382-P-A, "Methodology for Core Designs Containing Erbium Burnable Absorbers," August 1993.]

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure 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 to be 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 ASME Code (Ref. 2). To ensure system integrity, all RCS components are hydrostatically tested at 125% of design pressure, according to the ASME Code requirements prior to initial operation, when there is no fuel in the core. Following inception of unit operation, RCS components shall be pressure tested, in accordance with the requirements of ASME Code, Section XI (Ref. 3).

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" (Ref. 4).

APPLICABLE SAFETY ANALYSES

The RCS pressurizer safety valves, the main steam safety valves (MSSVs), and the Reactor Pressure - High 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

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 Protective System (RPS) trip setpoints (LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation"), together with the settings of the MSSVs (LCO 3.7.1, "Main Steam Safety Valves (MSSVs)") and the pressurizer safety valves, provide pressure protection for normal operation and AOOs. In particular, the Pressurizer Pressure - High trip setpoint is specifically set to provide protection against overpressurization (Ref. 5). Safety analyses for both the Pressure - High 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 any of the following:

a. Pressurizer power operated relief valves (PORVs),

b. Steam Bypass Control System,

c. Pressurizer Level Control System, or

d. Pressurizer Pressure Control System.

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 2750 psia.

APPLICABILITY

SL 2.1.2 applies in MODES 1, 2, 3, 4, and 5 because this SL could be approached or exceeded 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 unlikely that the RCS can be pressurized.

BASES

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the RCS pressure SL.

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 and be in MODE 3 within 1 hour.

With RCS pressure greater than the value specified in SL 2.1.2 in MODE 1 or 2, the pressure must be reduced to below this value. A pressure greater than the value specified in SL 2.1.2 exceeds 110% of the RCS design pressure and may challenge system integrity.

The allowed Completion Time of 1 hour provides the operator time to complete the necessary actions to reduce RCS pressure by terminating the cause of the pressure increase, removing mass or energy from the RCS, or a combination of these actions, and to establish MODE 3 conditions.

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.

Exceeding the RCS pressure SL in MODE 3, 4, or 5 is potentially 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.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 14, GDC 15, and GDC 28.
2. ASME, Boiler and Pressure Vessel Code, Section III, Article NB-7000.
3. ASME, Boiler and Pressure Vessel Code, Section XI, Article IWX-5000.
4. 10 CFR 100.
5. FSAR, Section [ ].
[6. ASME, USAS B31.1, Standard Code for Pressure Piping, 1967.]

B 2.0 SAFETY LIMITS (SLs)

B 2.1.2 Reactor Coolant System (RCS) Pressure 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 to be 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 ASME Code (Ref. 2). To ensure system integrity, all RCS components are hydrostatically tested at 125% of design pressure, according to the ASME Code requirements prior to initial operation, when there is no fuel in the core. Following inception of unit operation, RCS components shall be pressure tested, in accordance with the requirements of ASME Code, Section XI (Ref. 3).

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" (Ref. 4).

APPLICABLE SAFETY ANALYSES

The RCS pressurizer safety valves, the main steam safety valves (MSSVs), and the Reactor Pressure - High 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

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 Protective System (RPS) trip setpoints (LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation"), together with the settings of the MSSVs (LCO 3.7.1, "Main Steam Safety Valves (MSSVs)") and the pressurizer safety valves, provide pressure protection for normal operation and AOOs. In particular, the Pressurizer Pressure - High Trip setpoint is specifically set to provide protection against overpressurization (Ref. 5). Safety analyses for both the Pressure - High 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 any of the following:

a. Pressurizer power operated relief valves (PORVs),

b. Steam Bypass Control System,

c. Pressurizer Level Control System, or

d. Pressurizer Pressure Control System.

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 2750 psia.

APPLICABILITY

SL 2.1.2 applies in MODES 1, 2, 3, 4, and 5 because this SL could be approached or exceeded 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 unlikely that the RCS can be pressurized.

BASES

SAFETY LIMIT VIOLATIONS

The following SL violation responses are applicable to the RCS pressure SL.

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 and be in MODE 3 within 1 hour.

With RCS pressure greater than the value specified in SL 2.1.2 in MODE 1 or 2, the pressure must be reduced to below this value. A pressure greater that the value specified in SL 2.1.2 exceeds 110% of the RCS design pressure and may challenge system integrity.

The allowed Completion Time of 1 hour provides the operator time to complete the necessary actions to reduce RCS pressure by terminating the cause of the pressure increase, removing mass or energy from the RCS, or a combination of these actions, and to establish MODE 3 conditions.

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.

Exceeding the RCS pressure SL in MODE 3, 4, or 5 is potentially 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.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 14, GDC 15, and GDC 28.
2. ASME, Boiler and Pressure Vessel Code, Section III, Article NB-7000.
3. ASME, Boiler and Pressure Vessel Code, Section XI, Article IWX-5000.
4. 10 CFR 100.
5. FSAR, Section [ ].
[6. ASME, USAS B31.1, Standard Code for Pressure Piping, 1967.]

B 3.0 LIMITING CONDITION FOR OPERATION (LCO) APPLICABILITY

BASES

LCOs	LCO 3.0.1 through LCO 3.0.7 establish the general requirements applicable to all Specifications and apply at all times unless otherwise stated.
LCO 3.0.1	LCO 3.0.1 establishes the Applicability statement within each individual Specification as the requirement for when the LCO is required to be met (i.e., 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 that an ACTIONS 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. This Specification establishes that: a. Completion of the Required Actions within the specified Completion Times constitutes compliance with a Specification and b. Completion of the Required Actions is not required when an LCO is met within the specified Completion Time, unless otherwise specified. There are two basic types of Required Actions. The first type of Required Action specifies a time limit in which the LCO must be met. This time limit is the Completion Time 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 unit in a MODE or condition in which the Specification is not applicable. (Whether stated as a Required Action or not, correction of the entered Condition is an action that may always be considered upon entering ACTIONS.) The second type of Required Action specifies the remedial measures that permit continued operation of the unit that is not further restricted by the Completion Time. In this case, compliance with the Required Actions provides an acceptable level of safety for continued operation. Completing the Required Actions is not required when an LCO is met or is no longer applicable, unless otherwise stated in the individual Specifications.

BASES

LCO 3.0.2 (continued)

The nature of some Required Actions of some Conditions necessitates that, once the Condition is entered, the Required Actions must be completed even though the associated Conditions no longer exist. The individual LCO's ACTIONS specify the Required Actions where this is the case. An example of this is in LCO 3.4.3, "RCS Pressure and Temperature (P/T) Limits."

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. Intentional entry into ACTIONS should not be made for operational convenience. Additionally, if intentional entry into ACTIONS would result in redundant equipment being inoperable, alternatives should be used instead. Doing so limits the time both subsystems/trains of a safety function are inoperable and limits the time conditions exist which may result in LCO 3.0.3 being entered. Individual Specifications may specify a time limit for performing an SR when equipment is removed from service or bypassed for testing. In this case, the Completion Times of the Required Actions are applicable when this time limit expires, if the equipment remains removed from service or bypassed.

When a change in MODE or other specified condition is required to comply with Required Actions, the unit may enter a MODE or other specified condition in which another Specification becomes applicable. In this case, the Completion Times of the associated Required Actions would apply from the point in time that the new Specification becomes applicable and the ACTIONS Condition(s) are entered.

LCO 3.0.3

LCO 3.0.3 establishes the actions that must be implemented when an LCO is not met and either:

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

b. The condition of the unit 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 unit. Sometimes, possible combinations of Conditions are such that entering 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.

BASES

LCO 3.0.3 (continued)

This Specification delineates the time limits for placing the unit 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 intended 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.

Upon entering LCO 3.0.3, 1 hour is allowed to prepare for an orderly shutdown before initiating a change in unit 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 lower MODES of operation permit the shutdown to proceed in a controlled and orderly manner that is well within the specified maximum cooldown rate and within the capabilities of the unit, assuming that only the minimum required equipment is OPERABLE. This reduces thermal stresses on components of the Reactor Coolant System 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 are consistent with the discussion of Section 1.3, Completion Times.

A unit 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. A Condition exists for which the Required Actions have now been performed, or

c. ACTIONS exist that do not have expired Completion Times. These Completion Times are applicable from the point in time that the Condition is initially entered and not from the time LCO 3.0.3 is exited.

The time limits of LCO 3.0.3 allow 37 hours for the unit to be in MODE 5 when a shutdown is required during MODE 1 operation. If the unit is in a lower MODE of operation when a shutdown is required, the time limit for reaching the next lower MODE applies. If a lower MODE is reached in less time than allowed, however, the total allowable time to reach

BASES

LCO 3.0.3 (continued)

MODE 5, or other applicable MODE, is not reduced. For example, if MODE 3 is reached in 2 hours, then the time allowed for reaching MODE 4 is the next 11 hours, because the total time for reaching 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 lower MODE of operation in less than the total time allowed.

In MODES 1, 2, 3, and 4, LCO 3.0.3 provides actions for Conditions not covered in other Specifications. The requirements of LCO 3.0.3 do not apply in MODES 5 and 6 because the unit is already in the most restrictive Condition required by LCO 3.0.3. 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.

Exceptions to LCO 3.0.3 are provided in instances where requiring a unit shutdown, in accordance with LCO 3.0.3, would not provide appropriate remedial measures for the associated condition of the unit. An example of this is in LCO 3.7.16, "Fuel Storage Pool Water Level." LCO 3.7.16 has an Applicability of "During movement of irradiated fuel assemblies in the fuel storage pool." Therefore, this LCO can be applicable in any or all MODES. If the LCO and the Required Actions of LCO 3.7.16 are not met while in MODE 1, 2, or 3, there is no safety benefit to be gained by placing the unit in a shutdown condition. The Required Action of LCO 3.7.16 of "Suspend movement of irradiated fuel assemblies in fuel storage pool" is the appropriate Required Action to complete in lieu of the actions of LCO 3.0.3. These exceptions are addressed in the individual Specifications.

[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 allows placing the unit in a MODE or other specified condition stated in that Applicability (e.g., the Applicability desired to be entered) when unit conditions are such that the requirements of the LCO would not be met, in accordance with LCO 3.0.4.a, LCO 3.0.4.b, or LCO 3.0.4.c.

BASES

LCO 3.0.4 (continued)

LCO 3.0.4.a allows entry into a MODE or other specified condition in the Applicability with the LCO not met when the associated ACTIONS to be entered permit continued operation in the MODE or other specified condition in the Applicability for an unlimited period of time. Compliance with Required Actions that permit continued operation of the unit for an unlimited period of time in a MODE or other specified condition provides an acceptable level of safety for continued operation. This is without regard to the status of the unit before or after the MODE change. Therefore, in such cases, entry into a MODE or other specified condition in the Applicability may be made in accordance with the provisions of the Required Actions.

LCO 3.0.4.b allows entry into a MODE or other specified condition in the Applicability with the LCO not met after performance of a risk assessment addressing inoperable systems and components, consideration of the results, determination of the acceptability of entering the MODE or other specified condition in the Applicability, and establishment of risk management actions, if appropriate.

The risk assessment may use quantitative, qualitative, or blended approaches, and the risk assessment will be conducted using the plant program, procedures, and criteria in place to implement 10 CFR 50.65(a)(4), which requires that risk impacts of maintenance activities to be assessed and managed. The risk assessment, for the purposes of LCO 3.0.4.b, must take into account all inoperable Technical Specification equipment regardless of whether the equipment is included in the normal 10 CFR 50.65(a)(4) risk assessment scope. The risk assessments will be conducted using the procedures and guidance endorsed by Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." Regulatory Guide 1.182 endorses the guidance in Section 11 of NUMARC 93-01, "Industry Guideline for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants." These documents address general guidance for conduct of the risk assessment, quantitative and qualitative guidelines for establishing risk management actions, and example risk management actions. These include actions to plan and conduct other activities in a manner that controls overall risk, increased risk awareness by shift and management personnel, actions to reduce the duration of the condition, actions to minimize the magnitude of risk increases (establishment of backup success paths or compensatory measures), and determination that the proposed MODE change is acceptable. Consideration should also be given to the probability of completing restoration such that the requirements of the LCO would be met prior to the expiration of ACTIONS Completion Times that would require exiting the Applicability.

BASES

LCO 3.0.4 (continued)

LCO 3.0.4.b may be used with single, or multiple systems and components unavailable. NUMARC 93-01 provides guidance relative to consideration of simultaneous unavailability of multiple systems and components.

The results of the risk assessment shall be considered in determining the acceptability of entering the MODE or other specified condition in the Applicability, and any corresponding risk management actions. The LCO 3.0.4.b risk assessments do not have to be documented.

The Technical Specifications allow continued operation with equipment unavailable in MODE 1 for the duration of the Completion Time. Since this is allowable, and since in general the risk impact in that particular MODE bounds the risk of transitioning into and through the applicable MODES or other specified conditions in the Applicability of the LCO, the use of the LCO 3.0.4.b allowance should be generally acceptable, as long as the risk is assessed and managed as stated above. However, there is a small subset of systems and components that have been determined to be more important to risk and use of the LCO 3.0.4.b allowance is prohibited. The LCOs governing these systems and components contain Notes prohibiting the use of LCO 3.0.4.b by stating that LCO 3.0.4.b is not applicable.

LCO 3.0.4.c allows entry into a MODE or other specified condition in the Applicability with the LCO not met based on a Note in the Specification which states LCO 3.0.4.c is applicable. These specific allowances permit entry into MODES or other specified conditions in the Applicability when the associated ACTIONS to be entered do not provide for continued operation for an unlimited period of time and a risk assessment has not been performed. This allowance may apply to all the ACTIONS or to a specific Required Action of a Specification. The risk assessments performed to justify the use of LCO 3.0.4.b usually only consider systems and components. For this reason, LCO 3.0.4.c is typically applied to Specifications which describe values and parameters (e.g., [Containment Air Temperature, Containment Pressure, MCPR, Moderator Temperature Coefficient]), and may be applied to other Specifications based on NRC plant specific approval.

The provisions of this Specification should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to OPERABLE status before entering an associated MODE or other specified condition in the Applicability.

BASES

LCO 3.0.4 (continued)

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. In addition, the provisions of LCO 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that result from any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, MODE 3 to MODE 4, and MODE 4 to MODE 5.

Upon entry into a MODE or other specified condition in the Applicability with the LCO not met, LCO 3.0.1 and LCO 3.0.2 require entry into the applicable Conditions and Required Actions until the Condition is resolved, until the LCO is met, or until the unit is not within the Applicability of the Technical Specification.

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, utilizing LCO 3.0.4 is not a violation of SR 3.0.1 or SR 3.0.4 for any Surveillances that have not been performed on inoperable equipment. However, SRs must be met to ensure OPERABILITY prior to declaring the associated equipment OPERABLE (or variable within limits) and restoring compliance with the affected LCO.

LCO 3.0.5

LCO 3.0.5 establishes the allowance for restoring equipment to service under administrative controls when it has been removed from service or declared inoperable to comply with ACTIONS. The sole purpose of this Specification is to provide an exception to LCO 3.0.2 (e.g., to not comply with the applicable Required Action(s)) to allow the performance of required testing to demonstrate either:

a. The OPERABILITY of the equipment being returned to service or

b. The OPERABILITY of other equipment.

The administrative controls ensure the time the equipment is returned to service in conflict with the requirements of the ACTIONS is limited to the time absolutely necessary to perform the required testing to demonstrate OPERABILITY. This Specification does not provide time to perform any other preventive or corrective maintenance.

BASES

LCO 3.0.5 (continued)

An example of demonstrating the OPERABILITY of the equipment being returned to service is reopening a containment isolation valve that has been closed to comply with Required Actions and must be reopened to perform the required testing.

An example of demonstrating the OPERABILITY of other equipment is taking an inoperable channel or trip system out of the tripped condition to prevent the trip function from occurring during the performance of required testing on another channel in the other trip system. A similar example of demonstrating the OPERABILITY of other equipment is taking an inoperable channel or trip system out of the tripped condition to permit the logic to function and indicate the appropriate response during the performance of required testing on another channel in the same trip system.

LCO 3.0.6

LCO 3.0.6 establishes an exception to LCO 3.0.2 for support systems that have an LCO specified in the Technical Specifications (TS). This exception is provided because LCO 3.0.2 would require that the Conditions and Required Actions of the associated inoperable supported system LCO be entered solely due to the inoperability of the support system. This exception is justified because the actions that are required to ensure the unit is maintained in a safe condition are specified in the support system LCO's Required Actions. These Required Actions may include entering the supported system's Conditions and Required Actions or may specify other Required Actions.

When a support system is inoperable and there is an LCO specified for it in the TS, the supported system(s) are required to be declared inoperable if determined to be inoperable as a result of the support system inoperability. However, it is not necessary to enter into the supported systems' Conditions and Required Actions unless directed to do so by the support system's Required Actions. The potential confusion and inconsistency of requirements related to the entry into multiple support and supported systems' LCOs' Conditions and Required Actions are eliminated by providing all the actions that are necessary to ensure the unit is maintained in a safe condition in the support system's Required Actions.

However, there are instances where a support system's Required Action may either direct a supported system to be declared inoperable or direct entry into Conditions and Required Actions for the supported system. This may occur immediately or after some specified delay to perform

BASES

LCO 3.0.6 (continued)

some other Required Action. Regardless of whether it is immediate or after some delay, when a support system's Required Action directs a supported system to be declared inoperable or directs entry into Conditions and Required Actions for a supported system, the applicable Conditions and Required Actions shall be entered in accordance with LCO 3.0.2.

Specification 5.5.15, "Safety Function Determination Program (SFDP)," ensures loss of safety function is detected and appropriate actions are taken. Upon entry into LCO 3.0.6, an evaluation shall be made to determine if loss of safety function exists. Additionally, other limitations, remedial actions, or compensatory actions may be identified as a result of the support system inoperability and corresponding exception to entering supported system Conditions and Required Actions. The SFDP implements the requirements of LCO 3.0.6.

Cross train checks to identify a loss of safety function for those support systems that support multiple and redundant safety systems are required. The cross train check verifies that the supported systems of the redundant OPERABLE support system are OPERABLE, thereby ensuring safety function is retained. [A loss of safety function may exist when a support system is inoperable, and:

a. A required system redundant to system(s) supported by the inoperable support system is also inoperable (EXAMPLE B 3.0.6-1),

b. A required system redundant to system(s) in turn supported by the inoperable supported system is also inoperable (EXAMPLE B 3.0.6-2), or

c. A required system redundant to support system(s) for the supported systems (a) and (b) above is also inoperable (EXAMPLE B 3.0.6-3).

EXAMPLE B 3.0.6-1

If System 2 of Train A is inoperable and System 5 of Train B is inoperable, a loss of safety function exists in supported System 5.

EXAMPLE B 3.0.6-2

If System 2 of Train A is inoperable, and System 11 of Train B is inoperable, a loss of safety function exists in System 11 which is in turn supported by System 5.

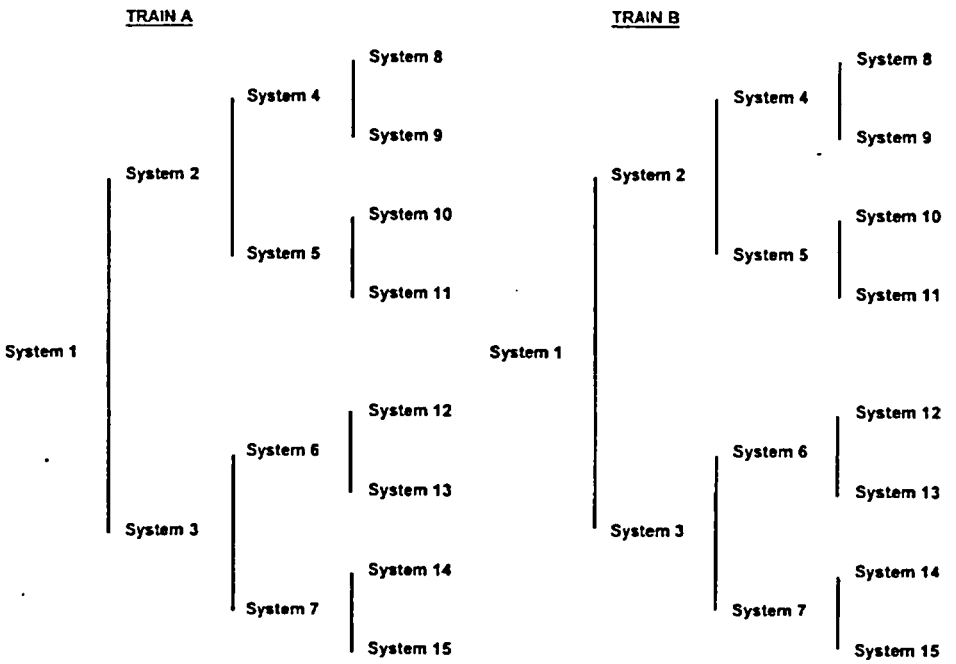
BASES

LCO 3.0.6 (continued)

EXAMPLE B 3.0.6-3

If System 2 of Train A is inoperable, and System 1 of Train B is inoperable, a loss of safety function exists in Systems 2, 4, 5, 8, 9, 10 and 11.]

If this evaluation determines that a loss of safety function exists, the appropriate Conditions and Required Actions of the LCO in which the loss of safety function exists are required to be entered.



[Figure B 3.0-1
Configuration of Trains and Systems]

This loss of safety function does not require the assumption of additional single failures or loss of offsite power. Since operations is being restricted in accordance with the ACTIONS of the support system, any resulting temporary loss of redundancy or single failure protection is taken into account. Similarly, the ACTIONS for inoperable offsite circuit(s) and inoperable diesel generator(s) provide the necessary restriction for cross train inoperabilities. This explicit cross train verification for inoperable AC electrical power sources also acknowledges that supported system(s) are not declared inoperable solely as a result of inoperability of a normal or emergency electrical power source (refer to the definition of OPERABILITY).

BASES

LCO 3.0.6 (continued)

When loss of safety function is determined to exist, and the SFDP requires entry into the appropriate Conditions and Required Actions of the LCO in which the loss of safety function exists, consideration must be given to the specific type of function affected. Where a loss of function is solely due to a single Technical Specification support system (e.g., loss of automatic start due to inoperable instrumentation, or loss of pump suction source due to low tank level) the appropriate LCO is the LCO for the

support system. The ACTIONS for a support system LCO adequately addresses the inoperabilities of that system without reliance on entering its supported system LCO. When the loss of function is the result of multiple support systems, the appropriate LCO is the LCO for the supported system.

LCO 3.0.7

Special tests and operations are required at various times over the unit'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 under either 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

BASES

LCO 3.0.7 (continued)

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 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 SURVEILLANCE REQUIREMENT (SR) APPLICABILITY

BASES

SRs

SR 3.0.1 through SR 3.0.4 establish the general requirements applicable to all Specifications and apply at all times, unless otherwise stated.

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 for which the requirements of the LCO apply, unless otherwise specified in the individual SRs. This Specification is to ensure that Surveillances are performed to verify the OPERABILITY of systems and components, and that variables are within specified limits. Failure to meet a Surveillance within the specified Frequency, in accordance with SR 3.0.2, constitutes a failure to meet an LCO. Surveillances may be performed by means of any series of sequential, overlapping, or total steps provided the entire Surveillance is performed within the specified Frequency. Additionally, the definitions related to instrument testing (e.g., CHANNEL CALIBRATION) specify that these tests are performed by means of any series of sequential, overlapping, or total steps.

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 either:

a. The systems or components are known to be inoperable, although still meeting the SRs or

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

Surveillances do not have to be performed when the unit is in a MODE or other specified condition for which the requirements of the associated LCO are 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.

Unplanned events may satisfy the requirements (including applicable acceptance criteria) for a given SR. In this case, the unplanned event may be credited as fulfilling the performance of the SR. This allowance includes those SRs whose performance is normally precluded in a given MODE or other specified condition.

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. Surveillances have to be met and performed in accordance with SR 3.0.2, prior to returning equipment to OPERABLE status.

BASES

SR 3.0.1 (continued)

Upon completion of maintenance, appropriate post maintenance testing is required to declare equipment OPERABLE. This includes ensuring applicable Surveillances are not failed and their most recent performance is in accordance with SR 3.0.2. Post maintenance testing may not be possible in the current MODE or other specified conditions in the Applicability due to the necessary unit parameters not having been established. In these situations, the equipment may be considered OPERABLE provided testing has been satisfactorily completed to the extent possible and the equipment is not otherwise believed to be incapable of performing its function. This will allow operation to proceed to a MODE or other specified condition where other necessary post maintenance tests can be completed.

Some examples of this process are:

a. Auxiliary feedwater (AFW) pump turbine maintenance during refueling that requires testing at steam pressures > 800 psi. However, if other appropriate testing is satisfactorily completed, the AFW System can be considered OPERABLE. This allows startup and other necessary testing to proceed until the plant reaches the steam pressure required to perform the testing.

b. High pressure safety injection (HPSI) maintenance during shutdown that requires system functional tests at a specified pressure. Provided other appropriate testing is satisfactorily completed, startup can proceed with HPSI considered OPERABLE. This allows operation to reach the specified pressure to complete the necessary post maintenance testing.

SR 3.0.2

SR 3.0.2 establishes the requirements for meeting the specified Frequency for Surveillances and any Required Action with a Completion Time that requires the periodic performance of the Required Action on a "once per..." interval.

SR 3.0.2 permits a 25% extension of the interval specified in the Frequency. This extension facilitates Surveillance scheduling and considers plant operating conditions that may not be suitable for conducting the Surveillance (e.g., transient conditions or other ongoing Surveillance or maintenance activities).

BASES

SR 3.0.2 (continued)

The 25% extension does not significantly degrade the reliability that results from performing the Surveillance at its specified Frequency. This is based on the recognition 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. The requirements of regulations take precedence over the TS. An example of where SR 3.0.2 does not apply is in the Containment Leakage Rate Testing Program. This program establishes testing requirements and Frequencies in accordance with the requirements of regulations. The TS cannot in and of themselves extend a test interval specified in the regulations.

As stated in SR 3.0.2, the 25% extension also does not apply to the initial portion of a periodic Completion Time that requires performance on a "once per ..." basis. The 25% extension applies to each performance after the initial performance. 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.

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

SR 3.0.3

SR 3.0.3 establishes the flexibility 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 or up to the limit of the specified Frequency, whichever is greater, 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 delay period provides adequate time to complete Surveillances that have been missed. This delay period permits the completion of a Surveillance before complying with Required Actions or other remedial measures that might preclude completion of the Surveillance.

BASES

SR 3.0.3 (continued)

The basis for this delay period includes consideration of unit conditions, adequate planning, availability of personnel, the time required to perform the Surveillance, the safety significance of the delay in completing the required Surveillance, and the recognition that the most probable result of any particular Surveillance being performed is the verification of conformance with the requirements.

When a Surveillance with a Frequency based not on time intervals, but upon specified unit conditions, operating situations, or requirements of regulations (e.g., prior to entering MODE 1 after each fuel loading, or in accordance with 10 CFR 50, Appendix J, as modified by approved exemptions, etc.) is discovered to not have been performed when specified, SR 3.0.3 allows for the full delay period of up to the specified Frequency to perform the Surveillance. However, since there is not a time interval specified, the missed Surveillance should be performed at the first reasonable opportunity.

SR 3.0.3 provides a time limit for, and allowances for the performance of, Surveillances that become applicable as a consequence of MODE changes imposed by Required Actions.

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 a flexibility which is not intended to be used as an operational convenience to extend Surveillance intervals. While up to 24 hours or the limit of the specified Frequency is provided to perform the missed Surveillance, it is expected that the missed Surveillance will be performed at the first reasonable opportunity. The determination of the first reasonable opportunity should include consideration of the impact on plant risk (from delaying the Surveillance as well as any plant configuration changes required or shutting the plant down to perform the Surveillance) and impact on any analysis assumptions, in addition to unit conditions, planning, availability of personnel, and the time required to perform the Surveillance. This risk impact should be managed through the program in place to implement 10 CFR 50.65(a)(4) and its implementation guidance, NRC Regulatory Guide 1.182, "Assessing and Managing Risk Before Maintenance Activities at Nuclear Power Plants." This Regulatory Guide addresses consideration of temporary and aggregate risk impacts, determination of risk management action thresholds, and risk management action up to and including plant

BASES

SR 3.0.3 (continued)

shutdown. The missed Surveillance should be treated as an emergent condition as discussed in the Regulatory Guide. The risk evaluation may use quantitative, qualitative, or blended methods. The degree of depth and rigor of the evaluation should be commensurate with the importance of the component. Missed Surveillances for important components should be analyzed quantitatively. If the results of the risk evaluation determine the risk increase is significant, this evaluation should be used to determine the safest course of action. All missed Surveillances will be placed in the licensee's Corrective Action Program.

If a Surveillance is not completed within the allowed delay period, then 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 applicable SRs must be met before entry into a MODE or other specified condition in the Applicability.

This Specification ensures that system and component OPERABILITY requirements and variable limits are met before entry into MODES or other specified conditions in the Applicability for which these systems and components ensure safe operation of the unit. The provisions of this Specification should not be interpreted as endorsing the failure to exercise the good practice of restoring systems or components to OPERABLE status before entering an associated MODE or other specified condition in the Applicability.

A provision is included to allow entry into a MODE or other specified condition in the Applicability when an LCO is not met due to a Surveillance not being met in accordance with LCO 3.0.4.

BASES

SR 3.0.4 (continued)

However, in certain circumstances, failing to meet an SR will not result in SR 3.0.4 restricting a MODE change or other specified condition change. When a system, subsystem, division, component, device, or variable is inoperable or outside its specified limits, the associated SR(s) are not required to be performed, per SR 3.0.1, which states that surveillances do not have to be performed on inoperable equipment. When equipment is inoperable, SR 3.0.4 does not apply to the associated SR(s) since the requirement for the SR(s) to be performed is removed. Therefore, failing to perform the Surveillance(s) within the specified Frequency does not result in an SR 3.0.4 restriction to changing MODES or other specified conditions of the Applicability. However, since the LCO is not met in this instance, LCO 3.0.4 will govern any restrictions that may (or may not) apply to MODE or other specified condition changes. SR 3.0.4 does not restrict changing MODES or other specified conditions of the Applicability when a Surveillance has not been performed within the specified Frequency, provided the requirement to declare the LCO not met has been delayed in accordance with SR 3.0.3.

The provisions of SR 3.0.4 shall not prevent entry into MODES or other specified conditions in the Applicability that are required to comply with ACTIONS. In addition, the provisions of SR 3.0.4 shall not prevent changes in MODES or other specified conditions in the Applicability that result from any unit shutdown. In this context, a unit shutdown is defined as a change in MODE or other specified condition in the Applicability associated with transitioning from MODE 1 to MODE 2, MODE 2 to MODE 3, MODE 3 to MODE 4, and MODE 4 to MODE 5.

The precise requirements for performance of SRs are specified such that exceptions to SR 3.0.4 are not necessary. The specific time frames and conditions necessary for meeting the SRs are specified in the Frequency, in the Surveillance, or both. This allows performance of Surveillances when the prerequisite condition(s) specified in a Surveillance procedure require entry into the MODE or other specified condition in the Applicability of the associated LCO prior to the performance or completion of a Surveillance. A Surveillance that could not be performed until after entering the LCO's Applicability, would have its Frequency specified such that it is not "due" until the specific conditions needed are met. Alternately, the Surveillance may be stated in the form of a Note, as not required (to be met or performed) until a particular event, condition, or time has been reached. Further discussion of the specific formats of SRs' annotation is found in Section 1.4, Frequency.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM) (Analog)

BASES

BACKGROUND

The reactivity control systems must be redundant and capable of holding the reactor core subcritical when shut down under cold conditions, in accordance with GDC 26 (Ref. 1). Maintenance of the SHUTDOWN MARGIN (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, the SDM defines the degree of subcriticality that would be obtained immediately following the insertion of all control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn.

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 provides the SDM during power operation and is 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 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits." When the unit is in the shutdown and refueling modes, the SDM requirements are met by means of 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 an SDM that ensures specified acceptable fuel design limits are not exceeded for normal operation and AOOs, with the assumption of the highest worth CEA stuck out following a reactor trip. For MODE 5, the primary safety analysis that relies on the SDM limits is the boron dilution analysis.

BASES

APPLICABLE SAFETY ANALYSES (continued)

The acceptance criteria for the SDM requirements are that specified acceptable fuel design limits are maintained. This is done by ensuring that:

a. The reactor can be made subcritical from all operating conditions, 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), 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 (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 fuel damage occurs as a result of the post trip return to power, and 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 for MODES 3 and 4 must also protect against:

BASES

APPLICABLE SAFETY ANALYSES (continued)

a. Inadvertent boron dilution,

b. An uncontrolled CEA withdrawal from a subcritical 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 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 SG and the core. The maximum positive reactivity addition that 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.

SDM satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

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, "Reactor Site Criteria," limits (Ref. 4). 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 through CEA positioning (regulating and shutdown CEA) and through the soluble boron concentration.

APPLICABILITY

In MODES 3, 4, and 5, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analyses discussed above. In MODES 1 and 2, SDM is ensured by complying with LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits," and LCO 3.1.6. 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 promptly. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. It is assumed that boration will be continued until the SDM requirements are met.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique requirement that must be satisfied. Since it is imperative to raise the boron concentration of the RCS as soon as possible, the boron concentration should be a highly concentrated solution, such as that normally found in the boric acid storage tank or the borated water storage tank. The operator should borate with the best source available for the plant conditions.

In determining the boration flow rate, the time core life must be considered. For instance, the most difficult time in core life to increase the RCS boron concentration is at the beginning of cycle, when the boron concentration may approach or exceed 2000 ppm. Assuming that a value of 1% $\Delta k/k$ must be recovered and a boration flow rate of [ ] gpm, it is possible to increase the boron concentration of the RCS by 100 ppm in approximately 35 minutes. If a boron worth of 10 pcm/ppm is assumed, this combination of parameters will increase the SDM by 1% $\Delta k/k$. These boration parameters of [ ] gpm and [ ] ppm represent typical values and are provided for the purpose of offering a specific example.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

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, which includes performing a boron concentration analysis, and complete the calculation.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.
2. FSAR, Section [ ].
3. FSAR, Section [ ].
4. 10 CFR 100.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.1 SHUTDOWN MARGIN (SDM) (Digital)

BASES

BACKGROUND

The reactivity control systems must be redundant and capable of holding the reactor core subcritical when shutdown under cold conditions, in accordance with GDC 26 (Ref. 1). Maintenance of the SHUTDOWN MARGIN (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, the SDM defines the degree of subcriticality that would be obtained immediately following the insertion of all full length control element assemblies (CEAs), assuming the single CEA of highest reactivity worth is fully withdrawn.

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 provides the SDM during power operation and is 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 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits." When the unit is in the shutdown and refueling modes, the SDM requirements are met by means of 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 an SDM that ensures specified acceptable fuel design limits are not exceeded for normal operation and AOOs, with the assumption of the highest worth CEA stuck out following a reactor trip. For MODE 5, the primary safety analysis that relies on the SDM limits is the boron dilution analysis.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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

a. The reactor can be made subcritical from all operating conditions, 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), 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 (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 fuel damage occurs as a result of the post trip return to power, and 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 for MODES 3 and 4 must also protect against:

a. Inadvertent boron dilution,

b. An uncontrolled CEA withdrawal from a subcritical condition,

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

d. CEA ejection.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

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

The SDM satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

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, "Reactor Site Criterion," limits (Ref. 4). 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.

BASES

LCO (continued)

SDM is a core physics design condition that can be ensured through CEA positioning (regulating and shutdown CEAs) and through the soluble boron concentration.

APPLICABILITY

In MODES 3, 4, and 5, the SDM requirements are applicable to provide sufficient negative reactivity to meet the assumptions of the safety analyses discussed above. In MODES 1 and 2, SDM is ensured by complying with LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits," and LCO 3.1.6. 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 promptly. A Completion Time of 15 minutes is adequate for an operator to correctly align and start the required systems and components. It is assumed that boration will be continued until the SDM requirements are met.

In the determination of the required combination of boration flow rate and boron concentration, there is no unique requirement that must be satisfied. Since it is imperative to raise the boron concentration of the RCS as soon as possible, the boron concentration should be a highly concentrated solution, such as that normally found in the boric acid storage tank or the borated water storage tank. The operator should borate with the best source available for the plant conditions.

In determining the boration flow rate, the time core life must be considered. For instance, the most difficult time in core life to increase the RCS boron concentration is at the beginning of cycle, when the boron concentration may approach or exceed 2000 ppm. Assuming that a value of 1% $\Delta k/k$ must be recovered and a boration flow rate of [ ] gpm, it is possible to increase the boron concentration of the RCS by 100 ppm in approximately 35 minutes. If a boron worth of 10 pcm/ppm is assumed, this combination of parameters will increase the SDM by 1% $\Delta k/k$. These boration parameters of [ ] gpm and [ ] ppm represent typical values and are provided for the purpose of offering a specific example.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.1.1

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, which includes performing a boron concentration analysis, and complete the calculation.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26.

2. FSAR, Section [15.4.2].

3. FSAR, Section [15.4.2].

4. 10 CFR 100.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 Reactivity Balance (Analog)

BASES

BACKGROUND

According to GDC 26, GDC 28, and GDC 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 Design Basis Accident (DBA) and transient safety analyses 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 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, "SHUTDOWN MARGIN (SDM)") in ensuring 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 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 calculational models used to generate the safety analysis are 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 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.

BASES

BACKGROUND *(continued)*

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 critical boron curve is based on steady state operation at RTP. Therefore, deviations from the predicted critical boron 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 additionally ensures 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 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 calculational 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 critical boron curve that develop during fuel depletion may be an indication that the calculational model is not adequate for core burnups beyond BOC, or that an unexpected change in core conditions has occurred.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

The reactivity balance satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

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 DBA and transient analyses are no longer valid, or that the uncertainties in the nuclear design methodology are larger than expected. A limit on the reactivity balance of ± 1% $\Delta k/k$ has been established, based on engineering 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

The limits on core reactivity must be maintained during MODES 1 and 2 because a reactivity balance must exist when the reactor is critical or producing THERMAL POWER. As the fuel depletes, core conditions are changing, and confirmation of the reactivity balance ensures the core is operating as designed. This Specification does not apply in MODES 3, 4, and 5 because the reactor is shut down and the reactivity balance is not changing.

In MODE 6, fuel loading results in a continually changing core reactivity. Boron concentration requirements (LCO 3.9.1, "Boron Concentration") ensure that fuel movements are performed within the bounds of the safety analysis. An SDM demonstration is required during the first startup following operations that could have altered core reactivity (e.g., fuel movement, or CEA replacement, or shuffling).

BASES

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 must be performed. Core conditions are evaluated to determine their consistency with input to design calculations. Measured core and process parameters are evaluated to determine that they are within the bounds of the safety analysis, and safety analysis calculational models are reviewed to verify that they are adequate for representation of the core conditions. The required Completion Time of 7 days is based on the low probability of a DBA occurring during this period, and allows sufficient time to assess the physical condition of the reactor and complete the 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.

The required Completion Time of 7 days is adequate for preparing whatever operating restrictions or Surveillances that may be required to allow continued reactor operation.

B.1

If the core reactivity cannot be restored to within the 1% $\Delta k/k$ limit, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to 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, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1

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. The SR is modified by three Notes. Note 1 in the Surveillance column indicates that the normalization of predicted core reactivity to the measured value must take place within the first 60 effective full power days (EFPD) 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 EFPD following the initial 60 EFPD 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., QPTR, etc.) for prompt indication of an anomaly. A second Note, "only required after 60 EFPD," is added to the Frequency column to allow this. Note 2 in the Surveillance column indicates that the performance of SR 3.1.2.1 is not required prior to entering MODE 2. This Note is required to allow a MODE 2 entry to verify core reactivity, because LCO Applicability is for MODES 1 and 2.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26, GDC 28, and GDC 29.
2. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.2 Reactivity Balance (Digital)

BASES

BACKGROUND

According to GDC 26, GDC 28, and GDC 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 Design Basis Accident (DBA) and transient safety analyses 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 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, "SHUTDOWN MARGIN (SDM)") in ensuring 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 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 calculational models used to generate the safety analysis are 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 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.

BASES

BACKGROUND (continued)

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 critical boron 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 that have been qualified against available test data, operating plant data, and analytical benchmarks. Monitoring reactivity balance additionally ensures 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 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 calculational 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 critical boron curve that develop during fuel depletion may be an indication that the calculational model is not adequate for core burnups beyond BOC, or that an unexpected change in core conditions has occurred.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

The reactivity balance satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

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 DBA and transient analyses are no longer valid, or that the uncertainties in the nuclear design methodology are larger than expected. A limit on the reactivity balance of ± 1% Δk/k has been established, based on engineering 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

The limits on core reactivity must be maintained during MODES 1 and 2 because a reactivity balance must exist when the reactor is critical or producing THERMAL POWER. As the fuel depletes, core conditions are changing, and confirmation of the reactivity balance ensures the core is operating as designed. This Specification does not apply in MODES 3, 4, and 5 because the reactor is shut down and the reactivity balance is not changing.

In MODE 6, fuel loading results in a continually changing core reactivity. Boron concentration requirements (LCO 3.9.1, "Boron Concentration") ensure that fuel movements are performed within the bounds of the safety analysis. An SDM demonstration is required during the first startup following operations that could have altered core reactivity (e.g., fuel movement, or CEA replacement, or shuffling).

BASES

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 must be performed. Core conditions are evaluated to determine their consistency with input to design calculations. Measured core and process parameters are evaluated to determine that they are within the bounds of the safety analysis, and safety analysis calculational models are reviewed to verify that they are adequate for representation of the core conditions. The required Completion Time of 7 days is based on the low probability of a DBA occurring during this period, and allows sufficient time to assess the physical condition of the reactor and complete the 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.

The required Completion Time of 7 days is adequate for preparing whatever operating restrictions or Surveillances that may be required to allow continued reactor operation.

B.1

If the core reactivity cannot be restored to within the 1% $\Delta k/k$, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to 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, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.2.1

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. The SR is modified by three Notes. The first Note indicates that the normalization of predicted core reactivity to the measured value must take place within the first 60 effective full power days (EFPD) 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 EFPD, following the initial 60 EFPD 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., QPTR) for prompt indication of an anomaly. A Note, "only required after 60 EFPD," is added to the Frequency column to allow this. Another Note indicates that the performance of SR 3.1.2.1 is not required prior to entering MODE 2. This Note is required to allow a MODE 2 entry to verify core reactivity because Applicability is for MODES 1 and 2.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 26, GDC 28, and GDC 29.
2. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Moderator Temperature Coefficient (MTC) (Analog)

BASES

BACKGROUND

According to GDC 11 (Ref. 1), the reactor core and its interaction with the Reactor Coolant System (RCS) 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 positive than that allowed by the LCO. 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 an 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 that are designed to achieve high burnups or that have changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 by 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 that produces the most rapid cooldown of the 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, which is assumed withdrawn. 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.

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 Policy Statement.

BASES

LCO

LCO 3.1.3 requires the MTC to be within specified limits of the COLR 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 on a positive MTC ensures that core overheating accidents will not violate the accident analysis assumptions. 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 LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on an 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 ensure 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 designs, and cannot be controlled directly once the designs have been implemented in the core. If MTC exceeds its limits, the reactor must be placed in MODE 3. 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 that would require an MTC value within the LCO limits, and the time for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1 and SR 3.1.3.2

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 > 5% RTP satisfies the confirmatory check on the most positive (least negative) MTC value. The requirement for measurement, within 7 days after reaching 40 effective full power days and b 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.

SR 3.1.3.2 is modified by a Note, which indicates that if the extrapolated MTC is more negative than the EOC COLR limit, the Surveillance may be repeated, and that shutdown must occur prior to exceeding the minimum allowable boron concentration at which MTC is projected to exceed the lower limit. An engineering evaluation is performed if the extrapolated value of MTC exceeds the Specification limits.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 11.
2. FSAR, Section [ ].
3. FSAR, Section [ ].
4. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.3 Moderator Temperature Coefficient (MTC) (Digital)

BASES

BACKGROUND

According to GDC 11 (Ref. 1), the reactor core and its interaction with the Reactor Coolant System (RCS) 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 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 positive than that allowed by the LCO. 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 an 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 that are designed to achieve high burnups or that have changes to other characteristics are evaluated to ensure that the MTC does not exceed the EOC limit.

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 by 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 that produces the most rapid cooldown of the 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, which is assumed withdrawn. 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.

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 10 CFR 50.36(c)(2)(ii).

BASES

LCO

LCO 3.1.3 requires the MTC to be within the specified limits of the COLR 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 on a positive MTC ensures that core overheating accidents will not violate the accident analysis assumptions. 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 LCO can only be ensured through measurement. The surveillance checks at BOC and MOC on an 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 ensure 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 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 designs, and cannot be controlled directly once the designs have been implemented in the core. If MTC exceeds its limits, the reactor must be placed in MODE 3. 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 that would require an MTC value within the LCO limits, and the time for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.3.1 and SR 3.1.3.2

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 > 5% RTP satisfies the confirmatory check on the most positive (least negative) MTC value. The requirement for measurement, within 7 days after reaching 40 effective full power days and a 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.

SR 3.1.3.2 is modified by a Note, which indicates that if extrapolated MTC is more negative than the EOC COLR limit, the Surveillance may be repeated, and that shutdown must occur prior to exceeding the minimum allowable boron concentration at which MTC is projected to exceed the lower limit. An engineering evaluation is performed if the extrapolated value of MTC exceeds the Specification limits.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 11.
2. FSAR, Section [ ].
3. FSAR, Section [ ].
4. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Control Element Assembly (CEA) Alignment (Analog)

BASES

BACKGROUND

The OPERABILITY (i.e., trippability) of the shutdown and regulating Control Element Assemblies (CEAs) is an initial assumption in all safety analyses that assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analysis that directly affects core power distributions and assumptions of available SDM.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10 and GDC 26 (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 CEDM moves its CEA one step (approximately ¾ inch) at a time, but at varying rates (steps per minute) depending on the signal output from the Control Element Drive Mechanism Control System (CEDMCS).

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 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.

BASES

BACKGROUND (continued)

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 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. Plant Computer CEA Position Indication System is considered highly precise (± 1 step or ± ¾ inch). If a CEA does not move one 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 two 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. 3). 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 systems. For example, CEA misalignment may be caused by a malfunction of the CEDM, CEDMCS, 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 dropped CEA could be caused by an electrical failure in the CEA coil power programmers.

The acceptance criteria for addressing CEA inoperability or misalignment are that:

a. There shall be no violations of either:

   1. Specified acceptable fuel design limits or

   2. Reactor Coolant System (RCS) pressure boundary integrity and

b. The core must remain subcritical after accident transients.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Three types of misalignment are distinguished in the safety analysis (Ref. 1). 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 requirement, 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 analyses are performed in regard to static CEA misalignment (Ref. 4). 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 nucleate boiling ratio (DNBR) 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 (SAFDLs) caused by a CEA misoperation, the accident analysis analyzed a single full length CEA drop. The most rapid approach to the DNBR 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, result in a local power and heat flux increase, and a decrease in DNBR parameters.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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

CEA alignment limits and OPERABILITY requirements satisfy Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on shutdown and regulating CEA alignments ensure that the assumptions in the safety analysis will remain valid. The requirements on CEA OPERABILITY ensure that upon reactor trip, the CEAs will be available and will be inserted to provide enough negative reactivity to shut down the reactor. The CEA OPERABILITY requirements (i.e., trippability) are separate from alignment requirements which ensure that the CEA banks maintain the correct power distribution and CEA alignment. The CEA OPERABILITY requirement is satisfied provided the CEA will fully insert in the required CEA drop time assumed in the safety analysis. CEA control malfunctions that result in the inability to move a CEA (e.g., CEA lift rod failures), but do not impact trippability, do not result in CEA inoperability.

The requirement is to maintain the CEA alignment to within [7 inches] between any CEA and its group. 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.

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 (i.e., trippability) and alignment of CEAs have 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, "SHUTDOWN MARGIN (SDM)," for SDM in MODES 3, 4, and 5, and LCO 3.9.1, "Boron Concentration," for boron concentration requirements during refueling.

BASES

ACTIONS

A.1 and A.2

If one or more CEAs (regulating or shutdown) are misaligned by > [7 inches] and ≤ [15 inches], or one CEA is misaligned by > [15 inches], continued operation in MODES 1 and 2 may continue, provided, within 1 hour, the power is reduced to ≤ 70% RTP, and within 2 hours CEA alignment is restored. Regulating CEA alignment can be restored by either aligning the misaligned CEA(s) to within [7 inches] of its group or aligning the misaligned CEA's group to within [7 inches] of the misaligned CEA. Shutdown CEA alignment can be restored by aligning the misaligned CEA(s) to within [7 inches] of its group.

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER in accordance with Figure 3.1.4-1 (in the associated LCO) ensures acceptable power distributions are maintained (Ref. 6). For small misalignments (< [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 negligible effect on the available SDM, and

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

With a large CEA misalignment (≥ [15 inches]), however, this misalignment would cause distortion of the core power distribution. This distortion may, in turn, have a significant effect on the time dependent, long term power distributions relative to those used in generating LCOs and LSSS setpoints. The effect on the available SDM and the ejected CEA worth used in the accident analysis remain small. Therefore, this condition is limited to a single CEA misalignment, while still allowing 2 hours for recovery.

In both cases, a 2 hour time period is sufficient to:

a. Identify cause of a misaligned CEA,

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

c. Minimize the effects of xenon redistribution.

BASES

ACTIONS (continued)

If a CEA is untrippable, it is not available for reactivity insertion during a reactor trip. With an untrippable CEA, meeting the insertion limits of LCO 3.1.5 and LCO 3.1.6 does not ensure that adequate SDM exists. The CEA must be returned to OPERABLE status with 2 hours or transition to MODE 3.

B.1, B.2.1, and B.2.2

The CEA motion inhibit permits CEA motion within the requirements of LCO 3.1.6, "Regulating Control Element Assembly Insertion Limits," and prevents regulating CEAs from being misaligned from other CEAs in the group.

Performing SR 3.1.4.1 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.

With the CEA motion inhibit inoperable, a Completion Time of 6 hours is allowed for restoring the CEA motion inhibit to OPERABLE status, or placing and maintaining the CEA drive switch in either the "off" or "manual" position, fully withdrawing the CEAs in groups 3 and 4, and withdrawing all CEAs in group 5 to < 5% insertion.

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 B.2.2 ensures that core perturbations in local burnup, perking factors, and SDM will not be more adverse than the Conditions assumed in the safety analyses and LCO setpoint determination (Ref. 6).

The 6 hour Completion Time takes into account Required Action B.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.

Required Action B.2.2 is modified by a Note indicating that this Required Action shall not be performed when in conflict with either Required Action A.1, A.2, or C.1.

BASES

ACTIONS (continued)

C.1

When the CEA deviation circuit is inoperable, performing SR 3.1.4.1, 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 the protection provided by the CEA inhibit and deviation circuit is not required.

D.1

If the Required Action or associated Completion Time of Condition A, Condition B, or Condition C is not met, one or more regulating or shutdown CEAs are inoperable, or two or more CEAs are misaligned by > [15 inches], the unit is required to be brought to MODE 3. By being brought to MODE 3, the unit is brought outside its MODE of applicability. Continued operation is not allowed in the case of more than one CEA misaligned from any other CEA in its group by > [15 inches], or one or more CEAs inoperable. This is because these cases are indicative of a loss of SDM and power distribution, and a loss of safety function, respectively.

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

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

Verification that individual CEA positions are within [7 inches] (indicated reed switch positions) of all other CEAs in the group at Frequencies of within 1 hour of any CEA movement of > 7.5 inches and every 12 hours. The CEA position verification after each movement of > 7.5 inches ensures that the CEAs in that group are properly aligned at the time when CEA misalignments are most likely to have occurred. The 12 hour Frequency allows the operator to detect a CEA that is 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.2

Demonstrating the CEA motion inhibit OPERABLE verifies that the CEA motion inhibit is functional, even if it is not regularly operated. The 92 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.

SR 3.1.4.3

Demonstrating the CEA deviation circuit is OPERABLE verifies the circuit is functional. The 92 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 3.1.4.4

Verifying each CEA is trippable would require that each CEA be tripped. In MODES 1 and 2, tripping each CEA would result in radial or axial power tilts, or oscillations. Therefore, individual CEAs are exercised every 92 days to provide increased confidence that all CEAs continue to be trippable, even if they are not regularly tripped. A movement of [5 inches] is adequate to demonstrate 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. Between required performances of SR 3.1.4.4, if a CEA(s) is discovered to be immovable, but remains trippable, the CEA is considered to be OPERABLE. At any time, if a CEA(s) is immovable, a determination of the trippability (OPERABILITY) of the CEA(s) must be made, and appropriate action taken.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.5

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 CEA's travel. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Since this Surveillance 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 at a Frequency of once every 18 months. 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 3.1.4.6

Verification of CEA drop times determined that the maximum CEA drop time permitted is consistent with the assumed drop time used in that safety analysis (Ref. 7). Measuring drop times prior to reactor criticality, after reactor vessel head removal, ensures that reactor internals and CEDM will not interfere with CEA motion or drop time and 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. This SR is performed prior to criticality, based on the need to perform this Surveillance under the conditions that apply during a unit outage and because of the potential for an unplanned unit transient if the Surveillance were performed with the reactor at power.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ].
4. FSAR, Section [ ].
5. FSAR, Section [ ].
6. FSAR, Section [ ].
7. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.4 Control Element Assembly (CEA) Alignment (Digital)

BASES

BACKGROUND

The OPERABILITY (i.e., trippability) of the shutdown and regulating Control Element Assemblies (CEAs) is an initial assumption in all safety analyses that assume CEA insertion upon reactor trip. Maximum CEA misalignment is an initial assumption in the safety analyses that directly affects core power distributions and assumptions of available SDM.

The applicable criteria for these reactivity and power distribution design requirements are 10 CFR 50, Appendix A, GDC 10 and GDC 26 (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 control element drive mechanisms (CEDMs). Each CEDM moves its CEA one step (approximately ¾ inch) at a time, but at varying rates (steps per minute) depending on the signal output from the Control Element Drive Mechanism Control System (CEDMCS).

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. Part length CEAs are not credited in the safety analyses for shutting down the reactor, as are the regulating and shutdown groups. The part length CEAs are used solely for ASI control.

BASES

BACKGROUND (continued)

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 CEDMCS 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 ± ¾ inch). If a CEA does not move one 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 two 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. 3). 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 systems. For example, CEA misalignment may be caused by a malfunction of the CEDM, CEDMCS, 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 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 are that:

a. There shall be no violations of either:

   1. Specified acceptable fuel design limits or

   2. Reactor Coolant System (RCS) pressure boundary integrity and

b. The core must remain subcritical after accident transients.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 requirement, 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 analyses are performed in regard to static CEA misalignment (Ref. 4). 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].

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 centerline 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, and a decrease in core power are produced. 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. 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.

CEA alignment limits and OPERABILITY requirements satisfy Criteria 2 and 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on shutdown and regulating CEA alignments ensure that the assumptions in the safety analysis will remain valid. The requirements on CEA OPERABILITY ensure that upon reactor trip, the CEAs will be available and will be inserted to provide enough negative reactivity to shut down the reactor. The CEA OPERABILITY requirements (i.e., trippability) are separate from the alignment requirements which ensure that the CEA banks maintain the correct power distribution and CEA alignment. The CEA OPERABILITY requirement is satisfied provided the CEA will fully insert in the required CEA drop time assumed in the safety analysis. CEA control malfunctions that result in the inability to move a CEA (e.g., CEA lift coil failures), but that do not impact trippability, do not result in CEA inoperability.

BASES

LCO (continued)

The requirement is to maintain the CEA alignment to within [7 inches] between any CEA and its group. 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.

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 (i.e., trippability) and alignment of CEAs have 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, "SHUTDOWN MARGIN (SDM)," for SDM in MODES 3, 4, and 5, and LCO 3.9.1, "Boron Concentration," for boron concentration requirements during refueling.

ACTIONS

A.1 and A.2

If one or more CEAs (regulating, shutdown or part length) are misaligned by [7 inches] and ≤ [19 inches], or one CEA misaligned by > [19 inches], continued operation in MODES 1 and 2 may continue, provided, within 1 hour, the power is reduced in accordance with Figure 3.1.4-1, and within 2 hours CEA alignment is restored.

Regulating and part length CEA alignment can be restored by either aligning the misaligned CEA(s) to within [7 inches] of its group or aligning the misaligned CEA's group to within [7 inches] of the misaligned CEA. Shutdown CEA alignment can be restored by aligning the misaligned CEA(s) to within [7 inches] of its group.

Xenon redistribution in the core starts to occur as soon as a CEA becomes misaligned. Reducing THERMAL POWER in accordance with Figure 3.1.4-1 (in the accompanying LCO) ensures acceptable power distributions are maintained (Ref. 6). For small misalignments (< [19 inches]) of the CEAs, there is:

BASES

ACTIONS (continued)

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 negligible effect on the available SDM, and

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

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 the time dependent, long term power distributions relative to those used in generating LCOs and LSSS setpoints. The effect on the available SDM and the ejected CEA worth used in the accident analysis remain small. Therefore, this condition is limited to the single CEA misalignment, while still allowing 2 hours for recovery. In both cases, a 2 hour time period is sufficient to:

a. Identify cause of a misaligned CEA,

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

c. Minimize the effects of xenon redistribution.

The CEA must be returned to OPERABLE status within 2 hours or transition to MODE 3.

B.1

If a Required Action or associated Completion Time of Condition A is not met, one or more full length CEAs are inoperable, or two or more CEAs are misaligned by > [19 inches], the unit is required to be brought to MODE 3. By being brought to MODE 3, the unit is brought outside its MODE of applicability. This is because these cases are indicative of a loss of SDM and power distribution, and a loss of safety function, respectively.

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

BASES

ACTIONS (continued)

Continued operation is not allowed in the case of more than one CEA(s) misaligned from any other CEA in its group by > [19 inches], or with one or more full length CEAs inoperable

SURVEILLANCE REQUIREMENTS

SR 3.1.4.1

Verification that individual CEA 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 that is 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.

SR 3.1.4.2

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.

SR 3.1.4.3

Verifying each full length CEA is trippable would require that each CEA be tripped. In MODES 1 and 2 tripping each full length CEA would result in radial or axial power tilts, or oscillations. Therefore individual full length CEAs are exercised every 92 days to provide increased confidence that all full length CEAs continue to be trippable, even if they are not regularly tripped. A movement of [5 inches] is adequate to demonstrate motion without exceeding the alignment limit when only one full length 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 (Ref. 7). Between required performances of SR 3.1.4.3, if a CEA(s) is discovered to be immovable, the CEA is considered to be OPERABLE. At anytime, if a CEA(s) is immovable, a determination of the trippability (OPERABILITY) of that CEA(s) must be made, and appropriate action taken.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.4.4

Performance of a CHANNEL FUNCTIONAL TEST of each reed switch position transmitter channel ensures the channel is OPERABLE and capable of indicating CEA position. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. 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 at a Frequency of once every 18 months. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint.

SR 3.1.4.5

Verification of full length 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, ensures the reactor internals and CEDM will not interfere with CEA motion or drop time, and 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. This SR is performed prior to criticality due to the plant conditions needed to perform the SR and the potential for an unplanned plant transient if the Surveillance were performed with the reactor at power.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ].
4. FSAR, Section [ ].

BASES

REFERENCES (continued)

5. FSAR, Section [ ].

6. FSAR, Section [ ].

7. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Shutdown Control Element Assembly (CEA) Insertion Limits (Analog)

BASES

BACKGROUND

The insertion limits of the shutdown Control Element Assemblies (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 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 shutdown CEAs are arranged into groups that are radially symmetric. Therefore, movement of the shutdown 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 design calculations are performed with the assumption that the shutdown CEAs are withdrawn prior to the regulating CEAs. The shutdown CEAs can be fully withdrawn without the core going critical. This provides available negative reactivity for SDM in the event of boration errors. 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 affect core power, burnup distribution, and add negative reactivity to shut down the reactor upon receipt of a reactor trip signal.

APPLICABLE SAFETY ANALYSES

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

CEAs are considered fully withdrawn at 129 inches, since this position places them outside the active region of the core.

On a reactor trip, all CEAs (shutdown and regulating), except the most reactive CEA, are assumed to insert into the core. The shutdown and regulating 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 3.1.6, "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, "SHUTDOWN MARGIN (SDM)") 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 CEA as well as regulating CEA insertion limits and inoperability or misalignment are that:

a. There be no violation of either:

   1. Specified acceptable fuel design limits or

   2. Reactor Coolant System pressure boundary damage and

b. The core remains subcritical after accident transients.

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

The shutdown CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

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.

BASES

APPLICABILITY

The shutdown CEAs must be within their insertion limits, with the reactor in MODES 1 and 2. The Applicability in MODE 2 begins anytime any regulating CEA is not fully inserted. 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. In MODE 3, 4, 5, or 6, the shutdown CEAs are fully inserted in the core and contribute to the SDM. Refer to LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," for SDM requirements in MODES 3, 4, and 5. LCO 3.9.1, "Boron Concentration," ensures adequate SDM in MODE 6.

This LCO has been modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.4. This SR verifies the freedom of the CEAs to move, and requires the shutdown CEAs to move below the LCO limits, which would normally violate the LCO.

ACTIONS

A.1

Prior to entering this condition, the shutdown CEAs were fully withdrawn. If a shutdown CEA(s) is then inserted into the core, its potential negative reactivity is added to the core as it is inserted.

If the CEA(s) is not restored to within limits within 1 hour, then an additional 1 hour is allowed for restoring the CEA(s) to within limits. The 2 hour total Completion Time allows the operator adequate time to adjust the CEA(s) in an orderly manner and is consistent with the required Completion Times in LCO 3.1.4, "Control Element Assembly (CEA) Alignment."

B.1

When Required Action A.1 or A.2 cannot be met or completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

Verification that the shutdown CEAs are within their insertion limits 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.

2. 10 CFR 50.46.

3. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.5 Shutdown Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the shutdown Control Element Assemblies (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 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 shutdown CEAs are arranged into groups that are radially symmetric. Therefore, movement of the shutdown 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 design calculations are performed with the assumption that the shutdown CEAs are withdrawn prior to the regulating CEAS. The shutdown CEAs can be fully withdrawn without the core going critical. This provides available negative reactivity for SDM in the event of boration errors. 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 affect core power, burnup distribution, and add negative reactivity to shut down the reactor upon receipt of a reactor trip signal.

APPLICABLE SAFETY ANALYSES

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

CEAs are considered fully withdrawn at 145 inches, since this position places them outside the active region of the core.

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 and regulating 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 3.1.6, "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, "SHUTDOWN MARGIN (SDM)") 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 CEA as well as regulating CEA insertion limits and inoperability or misalignment are that:

a. There be no violation of either:

   1. Specified acceptable fuel design limits or

   2. Reactor Coolant System pressure boundary damage integrity and

b. The core remains subcritical after accident transients.

The shutdown CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

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.

BASES

APPLICABILITY

The shutdown CEAs must be within their insertion limits, with the reactor in MODES 1 and 2. The Applicability in MODE 2 begins any time any regulating CEA is not fully inserted. 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. In MODE 3, 4, 5, or 6, the shutdown CEAs are fully inserted in the core and contribute to the SDM. Refer to LCO 3.1.1, "SHUTDOWN MARGIN (SDM)," for SDM requirements in MODES 3, 4, and 5. LCO 3.9.1, "Boron Concentration," ensures adequate SDM in MODE 6.

This LCO has been modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.5, which verifies the freedom of the CEAs to move, and requires the shutdown CEAs to move below the LCO limits, which would normally violate the LCO.

ACTIONS

A.1

Prior to entering this Condition, the shutdown CEAs were fully withdrawn. If a shutdown CEA is then inserted into the core, its potential negative reactivity is added to the core as it is inserted.

If the CEA(s) is not restored to within limits within 1 hour, then an additional 1 hour is allowed for restoring the CEA(s) to within limits. The 2 hour total Completion Time allows the operator adequate time to adjust the CEA(s) in an orderly manner and is consistent with the required Completion Times in LCO 3.1.4, "Control Element Assembly (CEA) Alignment."

B.1

When Required Action A.1 or Required Action A.2 cannot be met or completed within the required Completion Time, a controlled shutdown should be commenced. The allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.5.1

Verification that the shutdown CEAs are within their insertion limits 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, verification of shutdown CEA position at a Frequency of 12 hours is adequate to ensure that the shutdown CEAs are within their insertion limits. Also, the Frequency takes into account other information available to the operator in the control room for the purpose of monitoring the status of the shutdown CEAs.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

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

BASES

BACKGROUND

The insertion limits of the regulating Control Element Assemblies (CEAs) are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions, assumptions of available 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," 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 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 group sequence and overlap limits are specified in the COLR.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are 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 3.1.6, LCO 3.2.4, "AZIMUTHAL POWER TILT (Tq)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," provide limits on control component operation and on monitored process variables to ensure the core operates within the linear heat rate (LCO 3.2.1, "Linear Heat Rate (LHR)"), total planar radial peaking factor (F^T_{XY}) (LCO 3.2.2, "Total Planar Radial Peaking Factor (F^T_{XY})"), and total integrated radial peaking factor (F_r^T) (LCO 3.2.3, "Total Integrated Radial Peaking Factor (F_r^T)") 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^T_{XY} and

BASES

BACKGROUND (continued)

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^T_r 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 requires 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 3.1.6 are specified for the plant, which has been designed primarily for base loaded operation, but has the ability to accommodate a limited amount of load maneuvering.

The 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 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 other accident requiring termination by a Reactor Protection System trip function.

BASES

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 (the 95/95 DNB criterion) that the hot fuel CEA in the core does not experience a DNB condition,

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 3), 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).

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 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 to shut down the reactor to hot zero power. SDM assumes the maximum worth CEA remains fully withdrawn upon trip (Ref. 4).

The most limiting SDM requirements for MODE 1 and 2 conditions at BOC are determined by the requirements of several transients, e.g., loss of flow, seized rotor, etc. However, the most limiting SDM requirements for MODES 1 and 2 at EOC come from just one transient, Steam Line Break (SLB). The requirements of the SLB event at EOC for both the full power and no load conditions are significantly larger than those of any other event at that time in cycle and, also, considerably larger than the most limiting requirements at BOC.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Although the most limiting SDM requirements at EOC are much larger than those at BOC, the available SDMs obtained via the scramming of the CEAs are also substantially larger due to the much lower boron concentration at EOC. To verify that adequate SDMs are available throughout the cycle to satisfy the changing requirements, calculations are performed at both BOC and EOC. It has been determined that calculations at these two times in cycle are sufficient since the differences between available SDMs and the limiting SDM requirements are the smallest at these times in cycle. The measurement of CEA bank worth performed as part of the Startup Testing Program demonstrates that the core has the expected shutdown capability. Consequently, adherance to LCOs 3.1.5 and 3.1.6 provides assurance that the available SDMs at any time in cycle will exceed the limiting SDM requirements at that time in cycle.

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 that 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. 5).

The regulating CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on regulating CEAs sequence, overlap, and physical insertion, as defined in the COLR, 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. 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.

The power dependent insertion limit (PDIL) alarm circuit is required to be OPERABLE for notification that the CEAs are outside the required insertion limits. When the PDIL alarm circuit is inoperable, the verification of CEA positions is increased to ensure improper CEA alignment is identified before unacceptable flux distribution occurs.

BASES

APPLICABILITY

The 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 indicating the LCO requirement is suspended during SR 3.1.4.4. This SR verifies the freedom of the CEAs to move, and requires the regulating CEAs to move below the LCO limits, which would normally violate the LCO. The Note also allows the LCO to be not applicable during reactor power cutback operation, which inserts a selected CEA group (usually group 5) during loss of load events.

ACTIONS

A.1 and A.2

Operation beyond the transient insertion limit may result in a loss of SDM and excessive peaking factors. The transient insertion limit should not be violated during normal operation; this violation, however, may occur during transients when the operator is manually controlling the CEAs in response to changing plant conditions. When the regulating groups are inserted beyond the transient insertion limits, actions must be taken to either withdraw the regulating groups beyond the limits or to reduce THERMAL POWER to less than or equal to that allowed for the actual CEA insertion limit. Two hours provides a reasonable time to accomplish this, allowing the operator to deal with current plant conditions while limiting peaking factors to acceptable levels.

B.1 and B.2

If the CEAs are inserted between the long term steady state insertion limits and the transient insertion limits for intervals > 4 hours per 24 hour period, and the short term steady state insertions are exceeded, peaking factors can develop that are of immediate concern (Ref. 6).

Verifying 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. Fifteen minutes provides adequate time for the operator to verify if the short term steady state insertion limits are exceeded.

BASES

ACTIONS (continued)

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 LHR 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. 7).

C.1

With the regulating CEAs inserted between the long term steady state insertion limit and the transient insertion limit, and with the core approaching the 5 effective full power days (EFPD) per 30 EFPD or 14 EFPD per 365 EFPD limits, the core approaches the acceptable limits placed on operation with flux patterns outside those assumed in the long term burnup assumptions (Ref. 8). 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 cannot continue. A Completion Time of 2 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 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 from the chemical addition and makeup systems, and to cause the regulating CEAs to withdraw to the acceptable region. It is reasonable to continue operation for 2 hours after it is discovered that the 5 day or 14 day EFPD limit has been exceeded. This Completion Time is based on limiting the potential xenon redistribution, the low probability of an accident, and the steps required to complete the action.

D.1

When the PDIL alarm circuit is inoperable, performing SR 3.1.6.1 within 1 hour and once per 4 hours thereafter ensures improper CEA alignments are identified before unacceptable flux distributions occur.

BASES

ACTIONS (continued)

E.1

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

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

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 acceptable 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 3.1.6.1 is modified by a Note indicating that entry is allowed into MODE 2 for 12 hours without having performed the SR. This is necessary, since the unit must be in the applicable MODES in order to perform Surveillances that demonstrate the LCO limits are met.

SR 3.1.6.2

Verification of the accumulated time of CEA group insertion between the long term steady state insertion limits and the transient insertion limits ensures 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.

SR 3.1.6.3

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 that identify improper CEA alignments.

BASES

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46
3. FSAR, Section [ ], Section [ ], and Section [ ].
4. FSAR, Section [ ].
5. FSAR, Section [ ].
6. FSAR, Section [ ].
7. FSAR, Section [ ].
8. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

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

BASES

BACKGROUND

The insertion limits of the regulating control element assemblies (CEAs) are initial assumptions in all safety analyses that assume CEA insertion upon reactor trip. The insertion limits directly affect core power distributions, assumptions of available 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," 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 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 group sequence and overlap limits are specified in the COLR.

The regulating CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are 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 3.1.6; LCO 3.2.4, "Departure from Nucleate Boiling Ratio (DNBR)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," provide limits on control component operation and on monitored process variables to ensure the core operates within LCO 3.2.1, "Linear Heat Rate (LHR)," LCO 3.2.2, "Planar Radial Peaking Factor (Fxy)," and LCO 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," limits in the COLR. Operation within the LHR limits given in the COLR prevents power peaks that would exceed

BASES

BACKGROUND (continued)

the loss of coolant accident (LOCA) limits derived by the Emergency Core Cooling Systems 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, F_{xyxy}, and DNBR 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 analyses 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 3.1.6 are specified for the plant, which has been designed for primarily base loaded operation, but has the ability to accommodate a limited amount of load maneuvering.

The regulating CEA insertion and alignment limits, ASI and 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 other accident requiring termination by a Reactor Protection System trip function.

BASES

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, part length CEA insertion, ASI, and 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 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 (the 95/95 DNB criterion) that the hot fuel CEA in the core does not experience a DNB condition,

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 3), 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).

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 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. 4).

The most limiting SDM requirements for MODE 1 and 2 conditions at BOC are determined by the requirements of several transients, e.g., loss of flow, seized rotor, etc. However, the most limiting SDM requirements for MODES 1 and 2 at EOC come from just one transient, steam line break (SLB). The requirements of the SLB event at EOC for both the full power and no load conditions are significantly larger than those of any other event at that time in cycle and, also, considerably larger than the most limiting requirements at BOC.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Although the most limiting SDM requirements at EOC are much larger than those at BOC, the available SDMs obtained via the scramming of the CEAs are also substantially larger due to the much lower boron concentration at EOC. To verify that adequate SDMs are available throughout the cycle to satisfy the changing requirements, calculations are performed at both BOC and EOC. It has been determined that calculations at these two times in cycle are sufficient since the differences between available SDMs and the limiting SDM requirements are the smallest at these times in cycle. The measurement of CEA bank worth performed as part of the Startup Testing Program demonstrates that the core has the expected shutdown capability. Consequently, adherance to LCOs 3.1.5 and 3.1.6 provides assurance that the available SDMs at any time in cycle will exceed the limiting SDM requirements at that time in cycle.

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 that 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. 5).

The regulating CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The limits on regulating CEA sequence, overlap, and physical insertion, as defined in the COLR, 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. 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.

The power dependent insertion limit (PDIL) alarm circuit is required to be OPERABLE for notification that the CEAs are outside the required insertion limits. When the PDIL alarm circuit is inoperable, the verification of CEA positions is increased to ensure improper CEA alignment is identified before unacceptable flux distribution occurs.

BASES

APPLICABILITY

The 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 is modified by a Note indicating the LCO requirement is suspended during SR 3.1.4.3. This SR verifies the freedom of the CEAs to move, and requires the regulating CEAs to move below the LCO limits, which would normally violate the LCO. The Note also allows the LCO to be not applicable during reactor power cutback operation, which inserts a selected CEA group (usually group 5) during loss of load events.

ACTIONS

A.1 and A.2

Operation beyond the transient insertion limit may result in a loss of SDM and excessive peaking factors. The transient insertion limit should not be violated during normal operation; this violation, however, may occur during transients when the operator is manually controlling the CEAs in response to changing plant conditions. When the regulating groups are inserted beyond the transient insertion limits, actions must be taken to either withdraw the regulating groups beyond the limits or to reduce THERMAL POWER to less than or equal to that allowed for the actual CEA insertion limit. Two hours provides a reasonable time to accomplish this, allowing the operator to deal with current plant conditions while limiting peaking factors to acceptable levels.

B.1 and B.2

If the CEAs are inserted between the long term steady state insertion limits, the transient insertion limits for intervals > 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. 6).

Additionally, since the CEAs can be in this condition without misalignment, penalty factors are not inserted in the core protection calculators to compensate for the developing peaking factors. Verifying 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. Fifteen minutes provides adequate time for the operator to verify if the short term steady state insertion limits are exceeded.

BASES

ACTIONS (continued)

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 LHR 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. 7).

C.1

With the regulating CEAs inserted between the long term steady state insertion limit and the transient insertion limit, and with the core approaching the 5 effective full power days (EFPD) per 30 EFPD, or 14 EFPD per 365 EFPD limits, the core approaches 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 cannot continue. A Completion Time of 2 hours is a reasonable time 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 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 from the chemical addition and makeup systems, and to cause the regulating CEAs to withdraw to the acceptable region. It is reasonable to continue operation for 2 hours after it is discovered that the 5 day or 14 day EFPD limit has been exceeded. This Completion Time is based on limiting the potential xenon redistribution, the low probability of an accident, and the steps required to complete the action.

D.1 and D.2

With the Core Operating Limit 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. 8). 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.

BASES

ACTIONS (continued)

E.1

With the PDIL circuit inoperable, performing SR 3.1.6.1 within 1 hour and every 4 hours thereafter 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 Completion Time of 6 hours is reasonable, based on operating experience, for reaching MODE 3 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.6.1

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 acceptable limits, and provides 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 3.1.6.1 is modified by a Note indicating that entry is allowed into MODE 2 for 12 hours without having performed the SR. This is necessary, since the unit must be in the applicable MODES in order to perform Surveillances that demonstrate the LCO limits are met.

SR 3.1.6.2

Verification of the accumulated time of CEA group insertion between the long term steady state insertion limits and the transient insertion limits ensures 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.1.6.3

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 that identify improper CEA alignments.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ], Section [ ], and Section [ ].
4. FSAR, Section [ ].
5. FSAR, Section [ ].
6. FSAR, Section [ ].
7. FSAR, Section [ ].
8. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Special Test Exception (STE) - SHUTDOWN MARGIN (SDM) (Analog)

BASES

BACKGROUND

The primary purpose of the SHUTDOWN MARGIN (SDM) Special Test Exception (STE) is to permit relaxation of existing LCOs to allow the performance of certain PHYSICS TESTS. These tests are constructed to determine the control element assembly (CEA) worth.

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

BASES

BACKGROUND (continued)

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

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 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 (SDM)",

b. LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits," and

c. LCO 3.1.6, "Regulating Control Element Assembly (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 SDM CEA group height, insertion, and alignment. Additionally, the LCOs governing Reactor Coolant System (RCS) flow, reactor inlet temperature, and pressurizer pressure contribute to maintaining departure from nucleate boiling (DNB) parameter limits. The initial condition criteria for accidents sensitive to

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 (of those CEAs actually withdrawn) 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 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 criterion 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 SDM; and by ensuring that shutdown reactivity is available, equivalent to the reactivity worth of the estimated highest worth withdrawn 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, T_q and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the 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 COLR.

As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

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 worth of the regulating and shutdown CEAs. The SDM requirements of LCO 3.1.1, the shutdown CEA insertion limits of LCO 3.1.5, and the regulating CEA insertion limits of LCO 3.1.6 may be suspended.

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, as indicated by the Note, 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 for initiating 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.

SURVEILLANCE REQUIREMENTS

SR 3.1.7.1

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 operator to verify that each CEA position is within the acceptance criteria.

SR 3.1.7.2

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, ensures that the CEA will insert on a trip signal. The Frequency ensures that the CEAs are OPERABLE prior to reducing SDM to less than the limits of LCO 3.1.1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SR is modified by a Note which allows the SR to not be performed during initial power escalation following a refueling outage if SR 3.1.4.6 has been met during that refueling outage. This allows the CEA drop time test, which also proves the CEAs are trippable, to be credited for this SR.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter [14].
6. 10 CFR 50.46.
7. FSAR, Chapter [15].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.7 Part Length Control Element Assembly (CEA) Insertion Limits (Digital)

BASES

BACKGROUND

The insertion limits of the part length control element assemblies (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 CEAs are used for precise reactivity control of the reactor. The positions of the regulating CEAs are 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 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits," LCO 3.1.7, LCO 3.2.4, "Departure From Nucleate Boiling Ratio (DNBR)," and LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," 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, "Linear Heat Rate (LHR)"), planar peaking factor (F_{xy}) (LCO 3.2.2, "Planar Radial Peaking Factors (F_{xy})"), and LCO 3.2.4 limits in the COLR.

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 Systems 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 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

BASES

BACKGROUND (continued)

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 3.1.7 are specified for the plant, which has been designed primarily for base loaded operation, but 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, ASI, and 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 (the 95/95 DNB criterion) that the hot fuel CEA in the core does not experience a DNB condition,

c. During an ejected CEA accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. 3), 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).

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 LHRs.

The regulating CEA insertion limits satisfy Criterion 2 of 10 CFR 50.36(c)(2)(ii). The part length CEAs are required due to the potential peaking factor violations that could occur if part length CEAs exceed insertion limits.

LCO

The limits on part length CEA insertion, as defined in the COLR, must be maintained because they serve the function of preserving power distribution.

APPLICABILITY

The part length insertion limits shall be maintained with the reactor in MODE 1 > 20% RTP. These limits must be maintained, since they preserve the assumed power distribution. Applicability in lower MODES is not required, since the power distribution assumptions would not be exceeded in these MODES.

This LCO has been modified by a Note suspending the LCO requirement while exercising part length CEAs. Exercising part length CEAs may require moving them outside their insertion limits.

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 (EFPD) out of any 30 EFPD period, or for 14 EFPD 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. 4). Restoring the CEAs to within limits or reducing THERMAL POWER to that fraction of 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 Completion Time of 2 hours is reasonable for restoring the part length CEAs to within the allowed limits.

BASES

ACTIONS (continued)

C.1

When a Required Action cannot be completed within the required Completion Time, a controlled shutdown should commence. A Completion Time of 4 hours is reasonable, based on operating experience, for reducing power to ≤ 20 RTP from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.1.7.1

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 power dependent insertion limit alarm circuit and other information about CEA group positions available to the operator in the control room.

REFERENCES

1. 10 CFR 50, Appendix A, GDC 10 and GDC 26.
2. 10 CFR 50.46.
3. FSAR, Section [ ].
4. FSAR, Section [ ].

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.8 Special Test Exceptions (STE) - MODES 1 and 2 (Analog)

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 Special Test Exceptions (STE) 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 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. Ensure 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. Ensure 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 is required prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at power operation. The PHYSICS TESTS requirements for reload fuel cycles ensure that the operating characteristics of the core are consistent with the design predictions, and that the core can be operated as designed (Ref. 4).

BASES

BACKGROUND (continued)

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.

In this test, the following LCOs are suspended:

LCO 3.1.3, "Moderator Temperature Coefficient (MTC),"
LCO 3.1.4, "Control Element Assembly (CEA) Alignment,"
LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits,"
LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits,"
LCO 3.2.2, "Total Planar Radial Peaking Factor (F^T_{XY}),"
LCO 3.2.3, "Total Integrated Radial Peaking Factor (F^T_r)" and
LCO 3.2.4, "AZIMUTHAL POWER TILT (T_q)."

The safety analysis (Ref. 6) 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% RTP and the associated trip setpoints are required to ensure [explain].

BASES

APPLICABLE SAFETY ANALYSES (continued)

The individual LCOs governing CEA group height, insertion and alignment, ASI, F^T_{XY}, F^T_r, 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. 7). 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 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 F^T_{XY}, F^T_r, T_q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the 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 COLR.

As described in LCO 3.0.7, compliance with Special Test Exceptions LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

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 nonnormal 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 3.1.3, LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, LCO 3.2.2, LCO 3.2.3, and LCO 3.2.4 may be suspended during the performance of PHYSICS TESTS, provided THERMAL POWER is restricted to test power plateau, which shall not exceed 85% RTP.

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 < 85% RTP ensures that LHRs are maintained within acceptable limits.

ACTIONS

A.1

If THERMAL POWER exceeds the test power plateau, THERMAL POWER must be reduced to restore the additional thermal margin provided by the reduction. The 15 minute Completion Time ensures that prompt action shall be taken to reduce THERMAL POWER to within acceptable limits.

B.1 and B.2

If Required Action A.1 cannot be completed within the required Completion Time, PHYSICS TESTS must be suspended within 1 hour. Allowing 1 hour for suspending PHYSICS TESTS allows the operator sufficient time to change any abnormal CEA configuration back to within the limits of LCO 3.1.4, LCO 3.1.5, and LCO 3.1.6.

BASES

ACTIONS (continued)

Suspension of PHYSICS TESTS exceptions requires restoration of each of the applicable LCOs to within specification.

SURVEILLANCE REQUIREMENTS

SR 3.1.8.1

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. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter [14].
6. FSAR, Section [15.3.2.1].
7. 10 CFR 50.46.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.8 Special Test Exceptions (STE) - SHUTDOWN MARGIN (SDM) (Digital)

BASES

BACKGROUND

The primary purpose of the SHUTDOWN MARGIN (SDM) Special Test Exceptions (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.

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

BASES

BACKGROUND (continued)

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

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 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 (SDM),"

b. LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits," and

c. LCO 3.1.6, "Regulating Control Element Assembly (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 SDM 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

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 accidents 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 (of those CEAs actually withdrawn) 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 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 criterion 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 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 withdrawn 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, T_Q, and ASI, which represent initial condition input (power peaking) to the accident analysis. Also involved are the 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 COLR.

As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

BASES

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 STE is required to permit the periodic verification of the actual versus predicted worth of the regulating and shutdown CEAs. The SDM requirements of LCO 3.1.1, the shutdown CEA insertion limits of LCO 3.1.5, and the regulating CEA insertion limits of LCO 3.1.6 may be suspended.

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 as indicated by the Note, 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 withdrawn CEA, restoration of the minimum SDM requirements must be accomplished by increasing the RCS boron concentration. The required Completion Time of 15 minutes for initiating 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.

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 operator 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 at least a 50% withdrawn position, ensures that the CEA will insert on a trip signal. The Frequency ensures that the CEAs are OPERABLE prior to reducing SDM to less than the limits of LCO 3.1.1.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The SR is modified by a Note which allows the SR to not be performed during initial power escalation following a refueling outage if SR 3.1.4.5 has been met during that refueling outage. This allows the CEA drop time test, which also proves the CEAs are trippable, to be credited for this SR.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter 14.
6. 10 CFR 50.46.
7. FSAR, Chapter 15.

B 3.1 REACTIVITY CONTROL SYSTEMS

B 3.1.9 Special Test Exceptions (STE) - MODES 1 and 2 (Digital)

BASES

BACKGROUND

The primary purpose of these MODES 1 and 2 Special Test Exceptions (STE) 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 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. Ensure 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. Ensure 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 is required prior to initial criticality, after each refueling shutdown, and during startup, low power operation, power ascension, and at power operation. The PHYSICS TESTS requirements for reload fuel cycles ensure 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.

BASES

BACKGROUND (continued)

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 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:

LCO 3.1.3, "Moderator Temperature Coefficient (MTC),"
LCO 3.1.4, "Control Element Assembly (CEA) Alignment,"
LCO 3.1.5, "Shutdown Control Element Assembly (CEA) Insertion Limits,"
LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits,"
LCO 3.1.7, "Part Length Control Element Assembly (CEA) Insertion Limits,"
LCO 3.2.2, "Planar Radial Peaking Factors," and
LCO 3.2.3, "AZIMUTHAL POWER TILT (T_q)."

The safety analysis (Ref. 6) 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% RTP and the associated trip setpoints are required to ensure [explain].

The individual LCOs governing CEA group height, insertion and alignment, 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

BASES

APPLICABLE SAFETY ANALYSES (continued)

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. 7). 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 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 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 COLR.

As described in LCO 3.0.7, compliance with Special Test Exception LCOs is optional, and therefore no criteria of 10 CFR 50.36(c)(2)(ii) apply. Special Test Exception LCOs provide flexibility to perform certain operations by appropriately modifying requirements of other LCOs. A discussion of the criteria satisfied for the other LCOs is provided in their respective Bases.

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 nonnormal CEA configurations,

BASES

LCO (continued)

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 3.1.3, LCO 3.1.4, LCO 3.1.5, LCO 3.1.6, LCO 3.1.7, LCO 3.2.2, and LCO 3.2.3 may be suspended during the performance of PHYSICS TESTS provided THERMAL POWER is restricted to test power plateau, which shall not exceed 85% RTP.

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 < 85% RTP ensures that LHRs are maintained within acceptable limits.

ACTIONS

A.1

If THERMAL POWER exceeds the test power plateau in MODE 1, THERMAL POWER must be reduced to restore the additional thermal margin provided by the reduction. The 15 minute Completion Time ensures that prompt action shall be taken to reduce THERMAL POWER to within acceptable limits.

B.1 and B.2

If Required Action A.1 cannot be completed within the required Completion Time, PHYSICS TESTS must be suspended within 1 hour. Allowing 1 hour for suspending PHYSICS TESTS allows the operator sufficient time to change any abnormal CEA configuration back to within the limits of LCO 3.1.4, LCO 3.1.5, and LCO 3.1.6.

Suspension of PHYSICS TESTS exceptions requires restoration of each of the applicable LCOs to within specification.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.1.9.1

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 departure from nucleate boiling ratio 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.

REFERENCES

1. 10 CFR 50, Appendix B, Section XI.
2. 10 CFR 50.59.
3. Regulatory Guide 1.68, Revision 2, August 1978.
4. ANSI/ANS-19.6.1-1985, December 13, 1985.
5. FSAR, Chapter [14].
6. FSAR, Section [15.3.2.1].
7. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR) (Analog)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 satisfies 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 controlling the axial power distribution.

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 linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F^T_{XY}), Total Integrated Radial Peaking Factor (F^T_r), T_q, and 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 or the Incore Detector Monitoring System, provides adequate monitoring of the core power distribution and is capable of verifying that the LHR is within its limits. The Excore Detector Monitoring System performs this function by continuously monitoring 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.

In conjunction with the use of the Excore Detector Monitoring System and in establishing ASI limits, the following assumptions are made:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{xy} is within the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors and alarms that have been established for the individual incore detector segments, ensuring that the peak LHRs are 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,

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.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). 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 accident analyses (Ref. 1), with due regard for the correlations between measured quantities, the power distribution, and uncertainties in determining the 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 are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, 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. 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 ranges used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while the unit is operating at conditions outside the limits of these LCOs during normal operation. Fuel cladding damage could result, however, if an accident or AOO occurs 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 can correspondingly increase local LHR.

The LHR satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNB ratio 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 does not exceed 2200°F.

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

With the LHR exceeding its limit, excessive fuel damage could occur following an accident. In this Condition, prompt action must be taken to restore the LHR to within the specified limits. 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. The 1 hour Completion Time also allows the operator sufficient time for evaluating core conditions and for initiating proper corrective actions.

B.1

If the LHR cannot be returned to within its specified limits, THERMAL POWER must be reduced. The change to MODE 2 provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power MODE 1 conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

A Note was added to the SRs to require LHR to be determined by either the Excore Detector Monitoring System or the Incore Detector Monitoring System.

SR 3.2.1.1

Performance of this SR verifies that the Excore Detector Monitoring System can accurately monitor the LHR. Therefore, this SR is only applicable when the Excore Detector Monitoring System is being used to determine the LHR. The 31 day Frequency is appropriate for this SR because it is consistent with the requirements of SR 3.3.1.3 for calibration of the excore detectors using the incore detectors.

The SR is modified by a Note that states that the SR is only required to be met when the Excore Detection Monitoring System is being used to determine LHR. The reason for the Note is that the excore detectors input neutron flux information into the ASI calculation.

SR 3.2.1.2 and SR 3.2.1.3

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.

Performance of these SRs verifies 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.

A 31 day Frequency is consistent with the historical testing frequency of the reactor monitoring system. The SRs are modified by two Notes. Note 1 allows the SRs to be met only when the Incore Detector Monitoring System is being used to determine LHR. Note 2 states that the SRs are not required to be performed when THERMAL POWER is < 20% RTP. The accuracy of the neutron flux information from the incore detectors is not reliable at THERMAL POWER < 20% RTP.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.1 Linear Heat Rate (LHR) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO limits or prevents 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 accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits the damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 xenon distribution skewing, which is a significant factor in controlling the axial power distribution.

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).

BASES

BACKGROUND (continued)

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 calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bow and grid spacers. It is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution 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 continuously calculating an actual value of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

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 experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow determined from the maximum average assembly burnup of the batch. 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.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is 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 during AOOs by initiating reactor trips.

BASES

BACKGROUND (continued)

The COLSS continually generates an assessment of the calculated margin for specified LHR and 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 that indicate CEA positions. In this case, the CPCs assume a minimum core power of 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 LPD or low DNBR trips in the RPS initiate a reactor trip prior to the exceeding of fuel design limits.

The LHR and DNBR algorithms are valid within the limits on ASI, F_{xy} and T_Q. These limits are obtained directly from initial core or reload analysis.

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation or AOOs (Ref. 4).

The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (GDC 26, Ref. [ ]).

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 determining the 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). Peak cladding temperatures exceeding 2200°F cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing the LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. 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 ranges used in the accident analyses.

Fuel cladding damage does not normally occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident or AOO occurs 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 can correspondingly increase local LHR.

The LHR satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

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 LHR ensures that in the event of a LOCA the peak temperature of the fuel cladding does not exceed 2200°F.

BASES

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:

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 ratios at relatively low core power levels and

b. As a result of this inaccuracy, the CPCs assume minimum core power of 20% RTP when generating LPD and DNBR trip signals. When core power is below 20% RTP, the core is operating well below its thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1

Operation at or below the COLSS calculated power limit based on the LHR ensures that the LHR limit is not exceeded. If the COLSS calculated core power limit based on the LHR exceeds the operating limit, restoring the LHR to within limit in 1 hour ensures that prompt action is taken to reduce LHR to below the specified limit. One hour is a reasonable time to return LHR to within limits when the limit is exceeded without a trip due to events such as a dropped CEA or an axial xenon oscillation.

B.1, B.2.1, and B.2.2

If the COLSS is not available the OPERABLE LPD 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 fuel cladding temperature does not exceed 2200°F. Four hours is allowed for restoring the LHR limit to within the region of acceptable operation. This duration is reasonable because the COLSS allows the plant to operate with less LHR margin (closer to the LHR limit than when monitoring the CPCs).

When operating with the COLSS out of service there is a possibility of a slow undetectable transient that degrades the LHR slowly over the 4 hour period and is then followed by an AOO or an accident. To remedy this, the CPC calculated values of LHR are monitored every 15 minutes when the COLSS is out of service. The 15 minute Frequency is adequate to allow the operator to identify an adverse trend in conditions that could result in an approach to the LHR limit. Also, a maximum allowable

BASES

ACTIONS (continued)

change in the CPC calculated LHR ensures that further degradation requires the operators to take immediate action to restore LHR to within limits or reduce reactor power to comply with the Technical Specifications (TS). With an adverse trend, 1 hour is allowed for restoring LHR to within limits if the COLSS is not restored to OPERABLE status. Implementation of this requirement ensures that reductions in core thermal margin are quickly detected, and if necessary, results in a decrease in reactor power and subsequent compliance with the existing COLSS out of service TS limits.

With no adverse trend, 4 hours is allowed to restore the LHR to within limits if the COLSS is not restored to OPERABLE status. This duration is reasonable because the Frequency of the CPC determination of LHR is increased and if operation is maintained steady, the likelihood of exceeding the LHR limit during this period is not increased. The likelihood of induced reactor transients from an early power reduction is also decreased.

C.1

If the LHR cannot be returned to within its limit or the LHR cannot be determined because of the COLSS and CPC inoperability, core power must be reduced. Reduction of core power 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. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.1.1

With the COLSS out of service, the operator must monitor the LHR with each OPERABLE local power density channel. A 2 hour Frequency is sufficient to allow the operator to identify trends that would result in an approach to the LHR limits.

This SR is modified by a Note that states that the SR is only required to be met when the COLSS is out of service. 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 LHR.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.2.1.2

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 kilowatts per foot ensures the operator is alerted when conditions approach the LHR operating limit.

The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

REFERENCES

1. FSAR, Section [15].
2. FSAR, Section [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50.46, Appendix A, GDC 10.
5. 10 CFR 50.46.

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 LCO (Total Planar Radial Peaking Factor (F^T_{XY})) is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO decreases or prevents 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 accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System trip function. This LCO limits damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 (LSSS) and this LCO are based on 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 controlling the axial power distribution.

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).

BASES

BACKGROUND (continued)

The limits on LHR, F^T_{XY}, Total Integrated Radial Peaking Factor (F_r^T), T_q, and 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 or the Incore Detector Monitoring System, provides adequate monitoring of the core power distribution and is 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.

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 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{XY} does not exceed the limits of this LCO.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms that have been established for the individual incore detector segments ensure that the peak LHRs are 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,

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.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 3, GDC 10). The Power Distribution and CEA Insertion and Alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck, fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This limiting 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 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. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, 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. 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 ranges used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while at conditions outside the limits of these LCOs during normal operation. Fuel cladding damage could result, however, should an accident or AOO 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 LHR.

F^T_{XY} satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNB ratio operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limitation on LHR ensures that in the event of a LOCA the peak temperature of the fuel cladding does not exceed 2200°F.

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

A Note modifies Condition A to require Required Actions A.1 and A.2 to be completed if the Condition is entered. This ensures that corrective action is taken prior to unrestricted operation.

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 3.1.6), because these additional restrictions adequately ensure 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 3.1.6.

BASES

ACTIONS (continued)

B.1

If F_r^T cannot be returned to within its limit, THERMAL POWER must be reduced. A change to MODE 2 provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.2.1

The periodic Surveillance to determine the calculated F^T_{XY} ensures that 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 the reactor exceeding 70% RTP ensures that the core is properly loaded.

Performance of the Surveillance every 31 days of accumulated operation in MODE 1 provides reasonable assurance that unacceptable changes in the F^T_{XY} are promptly detected.

The power distribution map can only be obtained after THERMAL POWER exceeds 20% RTP because the incore detectors are not reliable below 20% RTP.

The SR is modified by a Note that requires that SR 3.2.2.2 and SR 3.2.2.3 be completed each time SR 3.2.1.1 is completed. (Values computed by these SRs are required to perform SR 3.2.2.1.) The Note also requires that the incore detectors be used to determine F^T_{XY} by using them to obtain a power distribution map with all full length CEAs above the long term steady state insertion limits, as specified in the COLR.

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 ensures that the calculated value of F^T_{XY} accurately reflects the condition of the core.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency for these Surveillances is in accordance with the Frequency requirements of SR 3.2.2.1, because these SRs provide information to complete SR 3.2.2.1.

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.2 Planar Radial Peaking Factors (F_{xy}) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents 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 accident, ejected control element assembly (CEA) accident, or other postulated accident requiring termination by a Reactor Protection System (RPS) trip function. This LCO limits damage to the fuel cladding during an accident by ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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. 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 xenon distribution skewing, which is a significant factor in controlling axial power distribution. 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 linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

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 bow and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution 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 values. The CPCs perform this function by continuously calculating actual values of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

DNBR penalty factors are 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 experience greater rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow determined from the maximum average assembly burnup of the batch. 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.

The COLSS indicates continuously to the operator how near the core is to the operating limits and provides an audible alarm if an operating limit is 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.

BASES

BACKGROUND (continued)

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 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 that indicates CEA position. In this case, the CPCs assume a minimum core power of 20% 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 LPD or low DNBR trips in the RPS initiate a reactor trip before fuel design limits are exceeded.

The limits on ASI, F_{xy}, and 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 or AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA 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 SDM 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. 4 and 5). This result 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 the uncertainties in the determination of power distribution.

BASES

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). Peak cladding temperatures exceeding 2200°F cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. 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 ranges used in the accident analyses.

Fuel cladding damage does not normally occur because of conditions outside the limits of these LCOs for ASI, F_{xy}, and T_Q during normal operation. However, fuel cladding damage results if an accident or AOO occurs 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 LHR.

F_{xy} satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

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 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}) ensures that the limits calculated by the COLSS and CPCs remain valid.

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:

a. The incore neutron detectors that provide input to the COLSS, which then calculates the operating limits, are inaccurate because of the poor signal to noise ratio that they experience at relatively low core power levels and

BASES

APPLICABILITY (continued)

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the LPD and DNBR trip signals. When the core power is below 20% RTP, 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

When the F^M_{XY} values exceed the F^C_{XY} values used in the COLSS and CPCs, nonconservative 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. The 6 hour Completion Time provides the time required to calculate the required multipliers and make the necessary adjustments to the CPC addressable constants. During this period the DNBR and LHR setpoints may be slightly nonconservative but DNBR and LHR are still within limits. Therefore, 6 hours is an acceptable Completion Time to perform these actions considering the low probability of an accident occurring during this time period.

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 CPCs to values $\geq F^M_{XY}$. The 6 hour Completion Time provides the time required to calculate the required multipliers and make the necessary adjustments to the CPC addressable constants. During this period the DNBR and LHR setpoints may be slightly nonconservative but DNBR and LHR are still within limits. Therefore, 6 hours is an acceptable Completion Time to perform these actions considering the low probability of an accident occurring during this time period.

BASES

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 COLSS and CPC 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} values are $\leq F^C_{XY}$ values used in the COLSS and CPCs. It ensures that the F^C_{XY} values used remain valid throughout the fuel cycle. A Frequency of 31 EFPD is acceptable because the power distribution changes only slightly with the amount of fuel burnup. Determining the F^M_{XY} values after each fuel loading when THERMAL POWER is > 40% RTP, but prior to its exceeding 70% RTP, ensures that the core is properly loaded.

REFERENCES

1. FSAR, Section [15].
2. FSAR, Section [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50.46, Appendix A, GDC 10.
5. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 Total Integrated Radial Peaking Factor (F^T_{XY}) (Analog)

BASES

BACKGROUND

The purpose of this LCO (Total Integrated Radial Peaking Factor (F^T_r)) is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 (LSSS) 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 controlling the axial power distribution.

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).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F^T_{XY}), F^T_r, T_q, and 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 or 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.

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following conditions are assumed:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms established for the individual incore detector segments ensure that the peak LHRs are 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,

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.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) and AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). 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 are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, 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}, and F^T_r limits specified in the COLR, and within the T_q limits. 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while at conditions outside the limits of these LCOs during normal operation. Fuel cladding damage could result, however, if an accident or AOO occurs 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 LHR.

F^T_r satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO limits for power distribution are based on correlations between power peaking and measured variables used as inputs to LHR and DNB ratio operating limits. The LCO limits for power distribution, 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 does not exceed 2200°F.

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

A Note modifying Condition A requires Required Actions A.1, A.2, and A.3 to be completed if the Condition is entered. This ensures that corrective action is taken prior to unrestricted operation.

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 3.1.6, and establishing a revised upper THERMAL POWER limit) because these additional restrictions provide adequate provisions to ensure that the assumptions used in establishing the LHR, LCO, and LSSS remain valid. Six hours to return F_r^T to within its limits by adjusting the ASI limits based on maximum power allowed for F^T_{XY} is reasonable and ensures that all CEAs meet the long term steady state insertion limits of LCO 3.1.6.

BASES

ACTIONS (continued)

B.1

If F_r^T cannot be returned to within its limit, THERMAL POWER must be reduced. A change to MODE 2 provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach MODE 2 from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.3.1

The periodic Surveillance to determine the calculated F_r^T ensures that 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% RTP ensures that the core is properly loaded.

Performance of the Surveillance every 31 days of accumulated operation in MODE 1 provides reasonable assurance that unacceptable changes in the F^T_r are promptly detected.

The power distribution map can only be obtained after THERMAL POWER exceeds 20% RTP because the incore detectors are not reliable below 20% RTP.

The SR is modified by a Note that requires SR 3.2.3.2 and SR 3.2.3.3 be completed each time SR 3.2.3.1 is completed. This procedure is required because the values computed by these SRs are required to perform this SR.

SR 3.2.3.2 and SR 3.2.3.3

Measuring the values of F_r^T and T_q each time a value of F_r^T is calculated ensures that the calculated value of F_r^T accurately reflects the condition of the core.

The Frequency for these Surveillances is in accordance with the requirements of SR 3.2.3.1 because these SRs provide information to complete SR 3.2.2.1.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.3 AZIMUTHAL POWER TILT (T_Q) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO either limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full 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, (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 xenon distribution skewing, which is a significant factor in controlling axial power distribution.

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).

BASES

BACKGROUND (continued)

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 calculated by the CE-1 Correlation (Ref. 3) and corrected for such factors as rod bow and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution 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 continuously calculating actual values of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

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 the assembly. Fuel assemblies that incur higher than average burnup experience greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow that is determined from the maximum average assembly burnup of the batch. 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 caused by the lower radial power peaks in the higher burnup batches.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is 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.

BASES

BACKGROUND (continued)

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 that indicates CEA position. In this case, the CPCs assume a minimum core power of 20% RTP. This threshold is set at 20% RTP because the power range excore neutron flux detection 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 initiate a reactor trip prior to exceeding fuel design limits.

The limits on the ASI, F_{xy}, and 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 and AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During a CEA ejection accident, the fission energy input to the fuel must not exceed 280 cal/gm (Ref. [5]), and

d. The control rods must be capable of shutting down the reactor with a minimum required SDM with the highest worth control rod stuck fully withdrawn (Ref. [6]).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 1). This result 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. 2) 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 (LHGR) so that the peak cladding temperature does not exceed 2200°F (Ref. 1). Peak cladding temperatures exceeding 2200°F cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. The latter are process variables that characterize the three dimensional power distribution of the reactor core. Operation within the limits of these variables ensures that their actual values are within the range used in the accident analyses.

Fuel cladding damage does not normally occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident or AOO occurs due to 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 increased local LHRs.
T_Q satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

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. $T_Q > 0.10$ is not expected. If it occurs, 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.

BASES

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:

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 that 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 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

If the measured T_Q is greater than the T_Q allowance used in the CPCs but ≤ 0.10, nonconservative trip setpoints may be calculated. Required Action A.1 restores 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 does not occur within this time.

If the T_Q cannot be restored within 2 hours, the T_Q allowance in the CPCs must be adjusted, per Required Action A.2, to be equal to or greater than the measured value of T_Q to ensure that the design safety margins are maintained.

B.1, B.2, and B.3

Required Actions B.1, B.2, and B.3 are modified by a Note that requires all subsequent actions be performed if power reduction commences prior to restoring $T_Q \leq 0.10$. This requirement ensures that corrective action is taken before unrestricted power operation resumes.

If the measured $T_Q > 0.10$, THERMAL POWER is reduced to $\leq$ 50% RTP within 4 hours. The 4 hours allows enough time to take action to restore T_Q prior to reducing power and limits the probability of operation with a power distribution out of limits. Such actions include performing SR 3.2.3.2, which provides a value of T_Q that can be used in subsequent actions.

BASES

ACTIONS (continued)

Also in the case of a tilt generated by a CEA misalignment, the 4 hours allows recovery of the CEA misalignment, because a measured $T_Q > 0.10$ is not expected. If it occurs, continued operation of the reactor may be necessary to discover the cause of the tilt. Operation then 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.

If the measured T_Q is not restored to within its specified limits, the reactor continues to operate with an axial power distribution mismatch. Continued operation in this configuration may induce an axial xenon oscillation, which results in increased LHGRs when the xenon redistributes. If the measured T_Q cannot be restored to within its limit within 4 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 while maintaining a power level sufficiently high enough to allow the tilt to be analyzed.

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. After power has been reduced to ≤ 50% RTP, the rate and magnitude of changes in the core flux are greatly reduced. Therefore, 16 hours is an acceptable time period to allow for reduction of the Linear Power Level - High trip setpoints, Required Action B.2. The 16 hour Completion Time allowed to reduce the Linear Power Level - High trip setpoints is required to perform the actions necessary to reset the trip setpoints.

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.

The Completion Time of Required Action B.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.

BASES

ACTIONS (continued)

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 ≥ 95% RTP provides an acceptable exit from this action after the measured T_Q has been returned to an acceptable value.

C.1

If the measured T_Q cannot be restored or determined within its specified limit, core power must be reduced. Reduction of core power 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. 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.

With the COLSS out of service, the operator must calculate T_Q and verify that it is within its specified limits. The 12 hour Frequency is sufficient to identify slowly developing T_Q's before they exceed the limits of this LCO. Also, the 12 hour Frequency prevents significant xenon redistribution.

SR 3.2.3.2

Verification that the COLSS T_Q alarm actuates at a value less than the value used in the CPCs ensures that the operator is alerted if T_Q approaches its operating limit. The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.2.3.3

Independent confirmation of the validity of the COLSS calculated T_Q ensures that the COLSS accurately identifies T_Q's.

The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

REFERENCES

1. FSAR, Section [15].
2. FSAR, Section [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50.46, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 AZIMUTHAL POWER TILT (T_q) (Analog)

BASES

BACKGROUND

The purpose of this LCO (AZIMUTHAL POWER TILT (T_q)) is to limit the core power distribution to the initial values assumed in the accident analyses. Operation within the limits imposed by this LCO limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 controlling the axial power distribution.

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 for linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F^T_{XY}), Total Integrated Radial Peaking Factor (F^T_r), T_q, and 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 or the Incore Detector Monitoring System, provides adequate monitoring of the core power distribution and is capable of verifying that the LCO limits are not exceeded. The Excore Detector Monitoring System performs this function by continuously monitoring ASI with OPERABLE quadrant symmetric excore neutron detectors and by verifying ASI is maintained within the limits specified in the COLR.

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 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms that have been established for the individual incore detector segments ensure that the peak LHRs are 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,

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.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs preclude core power distributions that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This process 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 determining the power distribution.

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate (LHGR) so that the peak cladding temperature does not exceed 2200°F (Ref. 4). High peak cladding temperatures are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, 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}, and F^T_r limits specified in the COLR, and within the T_q limits. 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while the reactor is operating at conditions outside these LCOs during otherwise normal operation. Fuel cladding damage could result, however, if an accident or AOO occurs from initial conditions outside the limits of these LCOs. Changes in the power distribution cause increased power peaking and correspondingly increased local LHRs.

The T_q satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and the measured variables used as inputs to the LHR and DNB operating limits. The power distribution LCO limits, except T_q, are provided in the COLR. The limits on LHR ensure that in the event of a LOCA, the peak temperature of the fuel cladding does not exceed 2200°F.

APPLICABILITY

In MODE 1 with THERMAL POWER > 50% RTP, T_q must be maintained within the limits assumed in accident analysis to ensure that fuel damage does not result following an AOO. In other MODES, this LCO does not apply because THERMAL POWER is not sufficient to require a limit on T_q.

ACTIONS

A.1 and A.2

If the measured T_q is > [0.03] and < 0.10, the calculation of T_q may be nonconservative. T_q must be restored within 2 hours or F^T_{XY} and F^T_r must be determined to be within the limits of LCO 3.2.2 and LCO 3.2.3, 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 cannot occur within this time. The 8 hour Completion Time ensures changes in F^T_{XY} and F^T_r can be identified before the limits of LCO 3.2.2 and LCO 3.2.3, respectively, are exceeded.

B.1

If Required Actions and associated Completion Times of Condition A are not met, THERMAL POWER must be reduced to ≤ 50% RTP. This requirement provides reasonable assurance that the core is operating within its thermal limits and places the core in a conservative condition. Four hours is a reasonable time to reach 50% RTP in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

C.1, C.2, and C.3

With $T_q > 0.10$, F^T_{XY} and F^T_r must be within their specified limits 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^T_{XY} and F^T_r are within limits, operation may proceed for a total of 2 hours after the Condition is entered while attempts are made to restore T_q to within its limit.

If $T_q \leq 0.10$ cannot be achieved, power must be reduced to ≤ 50% RTP within 2 hours. If the tilt is generated due to a CEA misalignment, operating at ≤ 50% RTP allows for the recovery of the CEA. Except as a result of CEA misalignment, $T_q > 0.10$ is not expected; if it occurs, continued operation of the reactor may be necessary to discover the cause of the tilt. If this procedure is followed, operation is restricted to only those conditions required to identify the cause of the tilt. It is necessary to account explicitly for power asymmetries because the radial power peaking factors used in core power distribution calculations are based on an untilted power distribution.

If T_q is not restored to within its limits, the reactor continues to operate with an axial power distribution mismatch. Continued operation in this configuration may induce an axial xenon oscillation that causes increased LHRs 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 ≤ 50% RTP within 2 hours provides conservative protection from increased peaking due to potential xenon redistribution. The Required Actions are modified by a Note that requires all subsequent actions to be performed once power reduction commences after entering the Condition if T_q is not restored to < 0.10. This procedure ensures corrective action is taken before unrestricted power operation resumes. Following THERMAL POWER reduction to ≤ 50% RTP, T_q must be restored to ≤ [0.03] before THERMAL POWER is increased (Required Action C.3). 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 C.3 is

BASES

ACTIONS (continued)

modified with a Note to indicate that the cause of the out of limit condition must be corrected prior to increasing THERMAL POWER. This Note also indicates that subsequent power operation above 50% RTP may proceed provided that the measured T_q is verified ≤ [0.03] at least once per hour for 12 hours, or until verified at 95% RTP. This ensures that the power distribution is responding as predicted. The Completion Time of 12 hours is a historical value that allows an acceptable exit from the LCO after the T_q value is verified acceptable for 12 hours or until 95% RTP is reached.

SURVEILLANCE REQUIREMENTS

SR 3.2.4.1

T_q must be calculated at 12 hour intervals. The 12 hour Frequency prevents significant xenon redistribution between Surveillances.

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.4 Departure from Nucleate Boiling Ratio (DNBR) (Digital)

BASES

BACKGROUND

The purpose of this 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 either limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 controlling axial power distribution.

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).

BASES

BACKGROUND (continued)

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 systems that monitor core power distribution online: the Core Operating Limits Supervisory System (COLSS) and the core protection calculators (CPCs). The COLSS and CPCs that monitor the core power distribution are capable of verifying that the LHR and 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 continuously calculating an actual value of DNBR and LPD for comparison with the respective trip setpoints.

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 experience a greater magnitude of rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty that is applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow that is determined from the maximum average assembly burnup of the batch. 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.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm when an operating limit is 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 during AOOs by initiating a reactor trip.

BASES

BACKGROUND (continued)

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 that indicates CEA position. In this case, the CPCs assume a minimum core power of 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 initiate a reactor trip prior to the exceeding of fuel design limits.

The limits on ASI, F_{xy}, and 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 or AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (Ref. 7).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). 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.

BASES

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. 4). Peak cladding temperatures exceeding 2200°F may cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. 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).

Fuel cladding damage does not normally occur from conditions outside the limits of these LCOs during normal operation. However, fuel cladding damage could result if an accident or AOO occurs 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.

DNBR satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

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 based on DNBR calculated by the COLSS. In the event that the COLSS is in service but neither of the two CEACs is OPERABLE, the DNBR is 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 must be reduced by the allowance specified in the COLR.

BASES

LCO (continued)

In instances for which the COLSS is out of service and either one or both of the CEACs are OPERABLE, the DNBR is maintained by operating within the acceptable region specified in the COLR as shown in Figure 3.2.4-1, in the COLR, and using any OPERABLE CPC channel. Alternatively, when the COLSS is out of service and neither of the two CEACs is OPERABLE, the DNBR is maintained by operating within the acceptable region specified in the COLR for this condition as shown in Figure 3.2.4-2, in the COLR, 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 assumptions that 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 ensures that an acceptable minimum DNBR is maintained in the event of a loss of flow transient.

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:

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 that 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 the thermal limits and the resultant CPC calculated LPD and DNBR trips are highly conservative.

ACTIONS

A.1

Operating at or above the minimum required value of the DNBR ensures that an acceptable minimum DNBR is 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, 1 hour is a reasonable time for 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.

BASES

ACTIONS (continued)

B.1, B.2.1, and B.2.2

If the COLSS is not available the OPERABLE DNBR channels are monitored to ensure that the DNBR is not exceeded. Maintaining the DNBR within this specified range ensures that no postulated accident results in consequences more severe than those described in the FSAR, Chapter 15. A 4 hour Frequency is allowed to restore the DNBR limit to within the region of acceptable operation. This Frequency is reasonable because the COLSS allows the plant to operate with less DNBR margin (closer to the DNBR limit) than when monitoring with the CPCs.

When operating with the COLSS out of service there is a possibility of a slow undetectable transient that degrades the DNBR slowly over the 4 hour period and is then followed by an anticipated operational occurrence or an accident. To remedy this, the CPC calculated values of DNBR are monitored every 15 minutes when the COLSS is out of service. The 15 minute Frequency is adequate to allow the operator to identify an adverse trend in conditions that could result in an approach to the DNBR limit. Also, a maximum allowable change in the CPC calculated DNBR ensures that further degradation requires the operators to take immediate action to restore DNBR to within limits or reduce reactor power to comply with the Technical Specifications (TS). With an adverse trend, 1 hour is allowed for restoring DNBR to within limits if the COLSS is not restored to OPERABLE status. Implementation of this requirement ensures that reductions in core thermal margin are quickly detected and, if necessary, results in a decrease in reactor power and subsequent compliance with the existing COLSS out of service TS limits.

With no adverse trend, 4 hours is allowed for restoring the DNBR to within limits if the COLSS is not restored to OPERABLE status. This duration is reasonable because the Frequency of the CPC determination of DNBR has been increased, and, if operation is maintained steady, the likelihood of exceeding the DNBR limit during this period is not increased. The likelihood of induced reactor transients from an early power reduction is also decreased.

BASES

ACTIONS (continued)

C.1

If the DNBR cannot be restored or determined within the allowed times of Conditions A and B, core power must be reduced. Reduction of core power to < 20% RTP ensures that the core is operating within its thermal limits and places the core in a conservative condition based on trip setpoints generated by the CPCs, which assume a minimum core power of 20% RTP.

The allowed Completion Time of 6 hours is reasonable, based on operating experience, to reach 20% RTP from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.4.1

With the COLSS out of service, 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 of the COLR, 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.

This SR is modified by a Note that states that the SR is only required to be met when the COLSS is out of service. 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.

SR 3.2.4.2

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 is alerted when operating conditions approach the DNBR operating limit. The 31 day Frequency for performance of this SR is consistent with the historical testing frequency of reactor protection and monitoring systems. The Surveillance Frequency for testing protection systems was extended to 92 days by CEN 327. Monitoring systems were not addressed in CEN 327; therefore, this Frequency remains at 31 days.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. FSAR, Section [ ].
7. 10 CFR 50, Appendix A, GDC 26.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.5 AXIAL SHAPE INDEX (ASI) (Analog)

BASES

BACKGROUND

The purpose of this LCO (AXIAL SHAPE INDEX (ASI)) is to limit the core power distribution to the initial values assumed in the accident analysis. Operation within the limits imposed by this LCO either limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring that the plant is operating within acceptable bounding conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 controlling the axial power distribution.

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 linear heat rate (LHR) and departure from nucleate boiling (DNB).

BASES

BACKGROUND (continued)

The limits on LHR, Total Planar Radial Peaking Factor (F^T_{XY}), Total Integrated Radial Peaking Factor (F^T_r), T_q, and 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.

In conjunction with the use of the Excore Detector Monitoring System and in establishing the ASI limits, the following conditions are assumed:

a. The CEA insertion limits of LCO 3.1.5, "Shutdown CEA Insertion Limits," and LCO 3.1.6, "Regulating CEA Insertion Limits," are satisfied,

b. The T_q restrictions of LCO 3.2.4 are satisfied, and

c. F^T_{xy} does not exceed the limits of LCO 3.2.2.

The Incore Detector Monitoring System continuously provides a more direct measure of the peaking factors, and the alarms that have been established for the individual incore detector segments ensure that the peak LHR is maintained within the limits specified in the COLR. The setpoints for these alarms include tolerances, set in conservative directions, as follows:

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.

BASES

APPLICABLE SAFETY ANALYSES

The fuel cladding must not sustain damage as a result of normal operation (Condition 1) or AOOs (Condition 2) (Ref. 3, GDC 10). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 4),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 3, GDC 10),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (Ref. 3, GDC 26).

The power density at any point in the core must be limited to maintain the fuel design criteria (Ref. 4). This limitation 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 among 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 are assumed to cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, 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, and F_r^T limits specified in the COLR, and within the T_q limits. 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 ranges used in the accident analyses.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding damage does not normally occur while the reactor is operating at conditions outside these LCOs during normal operation. Fuel cladding damage results, however, when an accident or AOO occurs 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 ASI satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to the LHR and DNB operating limits. These power distribution LCO limits, except T_q, are provided in the COLR. The limitation on LHR ensures that in the event of a LOCA, the peak temperature of the fuel cladding does not exceed 2200°F.

The limitation on ASI, along with the limitations of LCO 3.3.1, "Reactor Protection System Instrumentation," represents a conservative envelope of operating conditions consistent with the assumptions that have been analytically demonstrated adequate for maintaining 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 ensures that an acceptable minimum margin from DNB conditions is maintained in the event of any AOO, including a loss of flow transient.

APPLICABILITY

In MODE 1 with THERMAL POWER > 20% RTP, 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 THERMAL POWER is not sufficient to require a limit on the core power distribution. Below 20% RTP the incore detector accuracy is not reliable.

ACTIONS

A.1

Operating the core within ASI limits specified in the COLR and within the limits of LCO 3.3.1 ensures an acceptable margin for DNB and for maintaining local power density in the event of an AOO. Maintaining ASI within limits also ensures that the limits of 10 CFR 50.46 are not exceeded during accidents. The Required Actions to restore ASI must be completed within 2 hours to limit the duration the plant is operated outside the initial conditions assumed in the accident analyses. In addition, this Completion Time is sufficiently short that the xenon distribution in the core cannot change significantly.

BASES

ACTIONS (continued)

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. Reducing THERMAL POWER to ≤ 20% RTP provides reasonable assurance that the core is operating farther from thermal limits and places the core in a conservative condition. Four hours is a reasonable amount of time, based on operating experience, to reduce THERMAL POWER to ≤ 20% RTP in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.2.5.1

Verifying that the ASI is within the specified limits provides reasonable assurance that the core is not approaching DNB conditions. A Frequency of 12 hours is adequate for the operator to identify trends in conditions that 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.

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. 10 CFR 50, Appendix A.
4. 10 CFR 50.46.

B 3.2 POWER DISTRIBUTION LIMITS

B 3.2.5 AXIAL SHAPE INDEX (ASI) (Digital)

BASES

BACKGROUND

The purpose of this LCO is to limit the core power distribution to the initial values assumed in the accident analysis. Operation within the limits imposed by this LCO either limits or prevents 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 accident, ejected control element assembly (CEA) accident, 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 ensuring that the plant is operating within acceptable conditions at the onset of a transient.

Methods of controlling the power distribution include:

a. Using full 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 (e.g., a CEA drop or misoperation of the unit) that cause margin degradations.

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 xenon distribution skewing, which is a significant factor in controlling axial power distribution.

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).

BASES

BACKGROUND (continued)

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 bow and grid spacers, and it is accepted as an appropriate margin to DNB for all operating conditions.

There are two systems that monitor core power distribution online: the Core Operating Limit Supervisory System (COLSS) or the core protection calculators (CPCs). The COLSS and CPCs monitor the core power distribution and are capable of verifying that the LHR and 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 continuously calculating actual values of DNBR and local power density (LPD) for comparison with the respective trip setpoints.

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 experience greater rod bow. Conversely, fuel assemblies that receive lower than average burnup experience less rod bow. In design calculations for a reload core, each batch of fuel is assigned a penalty that is applied to the maximum integrated planar radial power peak of the batch. This penalty is correlated with the amount of rod bow that is determined from the maximum average assembly burnup of the batch. 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.

The COLSS indicates continuously to the operator how far the core is from the operating limits and provides an audible alarm if an operating limit is 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.

BASES

BACKGROUND (continued)

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 that indicates CEA position. In this case, the CPCs assume a minimum core power of 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 initiate a reactor trip prior to the exceeding of fuel design limits.

The limits on ASI, F_{xy}, and 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 or AOOs (Ref. 4). The power distribution and CEA insertion and alignment LCOs prevent core power distributions from reaching levels that violate the following fuel design criteria:

a. During a LOCA, peak cladding temperature must not exceed 2200°F (Ref. 5),

b. During a loss of flow accident, there must be at least 95% probability at the 95% confidence level (the 95/95 DNB criterion) that the hot fuel rod in the core does not experience a DNB condition (Ref. 4),

c. During an ejected CEA 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 SDM with the highest worth control rod stuck fully withdrawn (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 among measured quantities, the power distribution, and uncertainties in the determination of power distribution.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Fuel cladding failure during a LOCA is limited by restricting the maximum linear heat generation rate (LHGR) so that the peak cladding temperature does not exceed 2200°F (Ref. 5). Peak cladding temperatures exceeding 2200°F may cause severe cladding failure by oxidation due to a Zircaloy water reaction.

The LCOs governing LHR, ASI, and RCS ensure that these criteria are met as long as the core is operated within the ASI and F_{xy} limits specified in the COLR, and within the T_Q limits. 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 normally occur from conditions outside these LCOs during normal operation. However, fuel cladding damage results when an accident or AOO occurs due to 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 ASI satisfies Criterion 2 of 10 CFR 50.36(c)(2)(ii).

LCO

The power distribution LCO limits are based on correlations between power peaking and certain measured variables used as inputs to 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 does not drop below the DNBR Safety Limit for AOOs.

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:

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 that they experience at relatively low core power levels.

BASES

APPLICABILITY (continued)

b. As a result of this inaccuracy, the CPCs assume a minimum core power of 20% RTP when generating the 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 strongly 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 duration 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.

B.1

If the ASI is not restored to within its specified limits within the required Completion Time, the reactor continues to operate with an axial power distribution mismatch. Continued operation in this configuration induces an axial xenon oscillation, and results in increased LHGRs when the xenon redistributes. Reducing thermal power to ≤ 20% RTP reduces the maximum LHR to a value that does not exceed the fuel design limits if a design basis event occurs. The allowed Completion Time of 4 hours is reasonable, based on operating experience, to reduce power in an orderly manner and without challenging plant systems.

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 if an ASI limit is 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 that affect the ASI, such as xenon redistribution or CEA drive mechanism malfunctions, cause slow changes in the ASI, which can be discovered before the limits are exceeded.

BASES

REFERENCES

1. FSAR, Chapter [15].
2. FSAR, Chapter [6].
3. CE-1 Correlation for DNBR.
4. 10 CFR 50, Appendix A, GDC 10.
5. 10 CFR 50.46.
6. FSAR, Section [ ].
7. 10 CFR 50, Appendix A, GDC 26.

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protective System (RPS) Instrumentation - Operating (Analog)

BASES

BACKGROUND

The Reactor Protective System (RPS) initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and breaching the reactor coolant pressure boundary during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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.

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The trip setpoint is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytic Limit and thus ensuring that the SL would not be exceeded. As such, the trip setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the trip setpoint plays an important role in ensuring that SLs are not exceeded. As such, the trip setpoint meets the definition of an LSSS (Ref. 1) and could be used to meet the requirement that they be contained in the Technical Specifications.

BASES

BACKGROUND (continued)

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and therefore the LSSS as defined by 10 CFR 50.36 is the same as the OPERABILITY limit for these devices. However, use of the trip setpoint to define OPERABILITY in Technical Specifications and its corresponding designation as the LSSS required by 10 CFR 50.36 would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protective device with a setting that has been found to be different from the trip setpoint due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the trip setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to reset the device to the trip setpoint to account for further drift during the next surveillance interval.

Use of the trip setpoint to define "as found" OPERABILITY and its designation as the LSSS under the expected circumstances described above would result in actions required by both the rule and Technical Specifications that are clearly not warranted. However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value which, as stated above, is the same as the LSSS.

The Allowable Valuable specified in Table 3.3.1-1 serves as the LSSS such that a channel is OPERABLE if the trip setpoint is found not to exceed the Allowable Value during the CHANNEL FUNCTIONAL TEST (CFT). As such, the Allowable Value differs from the trip setpoint by an amount primarily equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has

BASES

BACKGROUND (continued)

not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to have exceeded the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Note that, although the channel is "OPERABLE" under these circumstances, the trip setpoint should be left adjusted to a value within the established trip setpoint calibration tolerance band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System (RCS) pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 2) and 10 CFR 100 (Ref. 3) 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 (Ref. 3) limits. Different accident categories allow a different fraction of these limits based on probability of 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,

BASES

BACKGROUND (continued)

- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses measurement channels and bistable trip units. It also addresses the automatic bypass removal feature for those trips with operating bypasses. The RPS Logic and RTCBs are addressed in LCO 3.3.3, "Reactor Protective System (RPS) Logic and Trip Initiation."

The role of each of these modules in the RPS, including those associated with the logic and RTCBs, 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.

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.

BASES

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 Features 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. 2). 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 or prevent a required trip from occurring.

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 Standard 279-1971 (Ref. 4).

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:

- Steam Generator Level - Low

  This trip uses the lower of the two steam generator levels as an input to a common bistable.

BASES

BACKGROUND (continued)

- Steam Generator Pressure - Low

  This trip uses the lower of the two steam generator pressures as an input to a common bistable.

- Variable High Power Trip (VHPT) - High

  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 that tracks power levels downward 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.

- Thermal Margin/Low Pressure (TM/LP) and Steam Generator Pressure Difference

  Q power is only one of several inputs to the TM/LP trip. Other inputs include internal ASI and cold leg temperature based on the higher of two cold leg resistance temperature detectors. The TM/LP trip setpoint is a complex function of these inputs and represents a minimum acceptable RCS pressure to be compared to actual RCS pressure in the TM/LP trip unit.

  Steam generator pressure is also an indirect input to the TM/LP trip via the Steam Generator Pressure Difference. This Function provides a reactor trip when the secondary pressure in either steam generator 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 ensure TM/LP trip if an asymmetric steam generator transient is detected.

- Axial Power Distribution (APD) - High

  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.

BASES

BACKGROUND (continued)

Bistable Trip Units

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 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 bistable trip units 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 errors - for those RPS channels that must function in harsh environments, as defined by 10 CFR 50.49 (Ref. 6) - Allowable Values specified in Table 3.3.1-1, in the accompanying LCO, are

BASES

BACKGROUND (continued)

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. 7). 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 interval between surveillances. A channel is inoperable if its actual setpoint is not within its required Allowable Value.

Setpoints in accordance with the Allowable Value will ensure that SLs of Chapter 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 the accompanying LCO 3.3.1, the Allowable Values of Table 3.3.1-1 are the LSSS.

RPS Logic

The RPS Logic, addressed in LCO 3.3.3, consists of both Matrix and Initiation Logic and employs a scheme that provides a reactor trip when bistables in any two out 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.

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.

BASES

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 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 RTCB 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, trip channel bypass contacts, and interconnecting matrix wiring between bistable and auxiliary trip units, up to but not including the matrix relays. Contacts in the bistable and auxiliary trip units are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

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 on 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.

BASES

BACKGROUND (continued)

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, Steam Generator Pressure - Low, APD - High, TM/LP, and Steam Generator Pressure Difference. [The Loss of Load trip, Power Rate of Change - High, and APD - High operating bypasses are automatically enabled and disabled.]

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear, addressed in LCO 3.3.3 and shown in Figure B 3.3.1-1, 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.

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 half of the CEAs (a half trip). Any one inoperable breaker in a channel will make the entire channel inoperable.

BASES

BACKGROUND (continued)

Each set of RTCBs is operated by either a Manual Trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two, as shown in Figure B 3.3.1-1. Depressing both push buttons in either set will result in a reactor trip.

When a Manual 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 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.
FSAR, Section [7.2] (Ref. 8), explains RPS testing in more detail.

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 5 takes credit for most RPS trip Functions. Functions not specifically credited in the accident analysis are part of the NRC approved licensing basis for the plant. These Functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate Function performance. Other Functions, such as the Loss of Load trip, are purely equipment protective, and their use minimizes the potential for equipment damage.

The specific safety analyses applicable to each protective Function are identified below:

1. Variable High Power Trip (VHPT) - High

   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:

   - Uncontrolled CEA withdrawal event,
   - Excess load,

BASES

APPLICABLE SAFETY ANALYSES (continued)

- Excess feedwater heat removal event,
- CEA ejection event, and
- Main steam line break (MSLB) (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.

2. Power Rate of Change - High

The Power Rate of Change - High trip is used to trip the reactor when excore [logarithmic] power indicates an excessive rate of change. The Power Rate of Change - High Function minimizes transients for events such as a continuous CEA withdrawal or a boron 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 at > 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 3.3.13, "[Logarithmic] Power Monitoring Channels," to be OPERABLE. LCO 3.3.13 ensures the [logarithmic] 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:

- Loss of RCS flow,
- Loss of nonemergency AC power,
- Reactor coolant pump (RCP) seized shaft,
- RCP sheared shaft, and
- Certain MSLB events.

The loss of RCS flow and of nonemergency AC power events are AOOs where fuel integrity is maintained. The RCP seized shaft, sheared shaft, and MSLBs are accidents where fuel damage may result.

BASES

APPLICABLE SAFETY ANALYSES (continued)

4. Pressurizer Pressure - High

The Pressurizer Pressure - High trip, in conjunction with pressurizer safety valves and main steam safety valves (MSSVs), provides protection against overpressure conditions in the RCS during the following events:

- Loss of condenser vacuum with a concurrent loss of offsite power,
- Loss of condenser vacuum with a concurrent loss of one 6.9 kV bus,
- Isolation of turbine at 102% power,
- Feedwater System pipe breaks between the steam generator and check valve,
- CEA withdrawal, and
- Loss of feedwater flow.

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 ensures 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 Steam Generator Pressure - Low trip provides protection against an excessive rate of heat extraction from the steam generators, 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

7.a, 7.b. Steam Generator A and B Level - Low

The Steam Generator A Level - Low and Steam Generator B Level - Low trips are required for the following events:

- Steam System piping failures,
- Feedwater System pipe breaks,
- Inadvertent opening of a steam generator atmospheric dump valve (ADV),
- Loss of normal feedwater, and
- Asymmetric loss of feedwater.

The Steam Generator Level - Low trip ensures that low DNBR, high local 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. Axial Power Distribution (APD) - High

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 that corresponds to the temperature for fuel centerline melting will occur. This trip is the primary protection against fuel centerline melting.

9. Thermal Margin

a. Thermal Margin/Low Pressure (TM/LP)

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:

BASES

APPLICABLE SAFETY ANALYSES (continued)

- Excess load (inadvertent opening of a steam generator ADV),
- RCS depressurization (inadvertent safety or power operated relief valves (PORVs) opening),
- Steam generator tube rupture, and
- 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 although only the LOCA is expected to result in fuel damage. 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 T_Q, and the maximum CEA deviation permitted for continuous operation are assumed in the generation of this trip Function. In addition, CEA group sequencing in accordance with LCO 3.1.6, "Regulating Control Element Assembly (CEA) Insertion Limits," is assumed. Finally, the maximum insertion of CEA banks that can occur during any AOO prior to a VHPT is assumed.

b. Steam Generator Pressure Difference

The Steam Generator Pressure Difference provides protection for those AOOs associated with secondary system malfunctions that result in asymmetric primary coolant temperatures. The most limiting event is closure of a single main steam isolation valve. Steam Generator Pressure Difference is provided by comparing the secondary pressure in both steam generators 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 a trip well before reaching the 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.

Interlocks/Bypasses

The bypasses and their Allowable Values are addressed in footnotes to Table 3.3.1-1. They are not otherwise addressed as specific Table entries.

The automatic bypass removal features must function as a backup to manual actions for all safety related trips to ensure the trip Functions are not operationally bypassed when the safety analysis assumes the Functions are not bypassed. The RPS operating bypasses are:

Zero power mode bypass (ZPMB) removal on the TM/LP, Steam Generator Pressure Difference, and reactor coolant low flow trips when THERMAL POWER is < 1E-4% 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.

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 removal is also effected by these bistables when conditions are no longer satisfied.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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.

Steam Generator Pressure - Low bypass removal. The Steam Generator Pressure - Low trip is manually enabled below the pretrip setpoint. The permissive is removed, and the bypass automatically removed, when the Steam Generator Pressure - Low pretrip clears.

The RPS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all instrumentation performing an RPS Function to be OPERABLE. Failure of any required portion of the instrument channel 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 may be 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 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 are 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. 7).

BASES

LCO (continued)

The following Bases for each trip Function identify the above RPS trip Function criteria items that are applicable to establish the trip Function OPERABILITY.

1. Variable High Power Trip (VHPT) - High

This LCO requires all four channels of the VHPT to be OPERABLE in MODES 1 and 2.

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. The 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 setpoint due to calibration and instrument errors, the maximum actual steady state THERMAL POWER level at which a trip would be actuated is 112% 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 analysis. There is no uncertainty applied to the step.

2. Power Rate of Change - High

This LCO requires four channels of 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.

The high power rate of change trip serves as a backup to the administratively enforced startup rate limit. The Function is not credited in the accident analyses; therefore, the Allowable Value for the trip or bypass Functions is not derived from analytical limits.

BASES

LCO (continued)

3. Reactor Coolant Flow - Low

This LCO requires four channels of Reactor Coolant Flow - Low to be OPERABLE in MODES 1 and 2.

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 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.

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 uncertainty, 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.

The 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 is 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.

The Pressurizer Pressure - High trip concurrent with PORV operation avoids unnecessary operation of the pressurizer safety valves.

5. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) that are 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.

BASES

LCO (continued)

6. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low per steam generator to be OPERABLE in MODES 1 and 2.

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 difference between the Allowable Value and the safety analysis value of 600 psia includes harsh environment uncertainties.

The Function may be manually bypassed as steam generator pressure is reduced during controlled plant shutdowns. This bypass is permitted at a preset steam generator pressure. The 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 steam generator pressure increases above the preset pressure.

7.a, 7.b. Steam Generator Level – Low

This LCO requires four channels of Steam Generator Level - Low per steam generator to be OPERABLE in MODES 1 and 2.

The Allowable Value is sufficiently below the normal operating level for the steam generators 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 top of the feed ring. The difference between the Allowable Value and the measurement value includes 10 inches of measurement uncertainty. The specified setpoint ensures there will be sufficient water inventory to provide a 10 minute margin before auxiliary feedwater is required for the removal of decay heat.

BASES

LCO (continued)

8. Axial Power Distribution (APD) - High

This LCO requires four channels of APD - High to be OPERABLE in MODE 1 ≥ 15% RTP.

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.

The APD trip is automatically bypassed at < 15% RTP, where it is not required for reactor protection.

9. Thermal Margin

a. Thermal Margin/Low Pressure (TM/LP)

This LCO requires four channels of TM/LP to be OPERABLE in MODES 1 and 2.

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.

b. Steam Generator Pressure Difference

This LCO requires four channels of Steam Generator Pressure Difference to be OPERABLE in MODES 1 and 2.

BASES

LCO (continued)

The Allowable Value is high enough to avoid trips caused by normal operation and minor transients, but ensures 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 Steam Generator Pressure Difference is subject to the ZPMB, since it is an input to the TM/LP trip and is not required for protection at low power levels.

10. Loss of Load

The LCO requires four Loss of Load trip channels to be OPERABLE in MODE 1 ≥ 15% RTP.

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, steam generator safety valves, or PORVs in the event of a Loss of Load. The Nuclear Steam Supply System and the Steam Dump System are capable of accommodating the Loss of Load without requiring the use of the above equipment.

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 are inadvertently bypassed.

The 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.

The interlock Allowable Values are based on analysis requirements for the bypassed functions. These are discussed above as part of the LCO discussion for the affected Functions.

BASES

APPLICABILITY

This LCO is applicable in accordance with Table 3.3.1-1. 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, maintaining the SLs during AOOs and assisting the ESFAS in providing acceptable consequences during accidents. Exceptions are addressed in footnotes to the table. Exceptions to this APPLICABILITY are:

- The APD - High Trip and Loss of Load are only applicable in MODE 1 ≥ 15% RTP because they may be automatically bypassed at < 15% RTP, where they are no longer needed.

- The Power Rate of Change - High trip, RPS Logic, RTCBs, and Manual Trip are also required in MODES 3, 4, and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events. The Power Rate of Change - High trip in these lower MODES is addressed in LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown." The RPS Logic in MODES 1, 2, 3, 4, and 5 is addressed in LCO 3.3.3.

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 ensuring adequate SDM.

ACTIONS

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) 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 trip unit is found inoperable, then all affected Functions provided by that channel must be declared inoperable, and the plant 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.

BASES

ACTIONS (continued)

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Times of each inoperable Function will be tracked separately for each Function, starting from the time the Condition was entered.

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

Condition A applies to the failure of a single channel in any RPS automatic trip Function. RPS coincidence logic is normally two-out-of-four.

If one RPS bistable trip unit or associated instrument channel is inoperable, startup or power operation is allowed to continue, providing the inoperable trip unit is placed in bypass or trip within 1 hour (Required Action A.1). With one channel in bypass, no additional random failure of a single channel could spuriously trip the reactor and a valid trip signal can still trip the reactor. With one channel in trip, an additional random failure of a single channel could spuriously trip the reactor. Therefore, it is preferable to place an inoperable channel in bypass rather than trip.

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 while ensuring that the risk involved in operating with the failed channel is acceptable.

The failed channel is restored to OPERABLE status or is placed in trip within [48] hours (Required Action A.2.1 or Required Action A.2.2). Required Action A.2.1 restores the full capability of the Function.

[Required Action A.2.2 places the Function in a one-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip.]

The Completion Time of [48] hours 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.

BASES

ACTIONS (continued)

B.1 and B.2

Condition B applies to the failure of two channels in any RPS automatic trip Function.

Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels while ensuring that 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.

One channel should be restored to OPERABLE status within [48] hours for reasons similar to those stated under Condition A. After one channel is restored to OPERABLE status, 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.2 must be placed in trip if more than [48] hours have elapsed since the initial channel failure.

C.1 and C.2

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.

The Completion Time of 24 hours is adequate to perform the SR while minimizing the risk of operating in an unsafe condition.

BASES

ACTIONS (continued)

D.1, D.2.1, D.2.2.1, and D.2.2.2

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 A, 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 A.

E.1, E.2.1, and E.2.2

Condition E applies to two inoperable automatic bypass removal channels. If the bypass removal channels 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 B, and the bypass either removed or the bypass removal channel repaired. Also, Required Action E.2.2 provides for the restoration of the one affected automatic trip channel to OPERABLE status within the rules of Completion Time specified under Condition B. Completion Times are consistent with Condition B.

F.1

Condition F is entered when the Required Action and associated Completion Time of Conditions A, B, C, D, or E are not met for the Axial Power Distribution and Loss of Load Trip Functions.

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. The allowed Completion Time of 6 hours to reduce THERMAL POWER to < 15% RTP is reasonable, based on operating experience, to decrease power to < 15% RTP from full power conditions in an orderly manner and without challenging plant systems.

BASES

ACTIONS (continued)

G.1

Condition G is entered when the Required Action and associated Completion Time of Conditions A, 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. The allowed Completion Time of 6 hours to be in MODE 3 is reasonable, based on operating experience, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant systems.

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.

----------REVIEWER'S NOTE----------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff SER that establishes the acceptability of each topical report for that plant (Ref. 9).

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 normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. 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.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. 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 3.3.1.2

A daily calibration (heat balance) is performed when THERMAL POWER is ≥ 20%. The daily calibration shall consist of adjusting the "nuclear power calibrate" potentiometers to agree with the 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 Calibration 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 calculation.

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 Frequency is modified by a Note indicating this Surveillance must be performed within 12 hours after THERMAL POWER is ≥ 20% RTP. The secondary calorimetric is inaccurate at lower power levels. The 12 hours allows time requirements for plant stabilization, data taking, and instrument calibration.

A second Note indicates the daily calibration may be suspended during PHYSICS TESTS. This ensures that calibration is proper preceding and following physics testing at each plateau, recognizing that during testing, changes in power distribution and RCS temperature may render the calorimetric inaccurate.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 Frequency indicates the Surveillance is required within 12 hours after THERMAL POWER is ≥ [20]% RTP. Uncertainties in the excore and incore measurement process make it impractical to calibrate when THERMAL POWER is < [20]% RTP. The Completion Time of 12 hours allows time for plant stabilization, data taking, and instrument calibration. If the excore detectors are not properly calibrated to agree with the incore detectors, power is restricted during subsequent operations because of increased uncertainty associated with using uncalibrated excore detectors. The 31 day 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 Frequency.

SR 3.3.1.4

A CHANNEL FUNCTIONAL TEST is performed on each RPS instrument channel, except Loss of Load and Power Rate of Change, every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, The RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 8. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

BASES

SURVEILLANCE REQUIREMENTS (continued)

Bistable Tests

The bistable setpoint must be found to trip within the Allowable Values specified in the LCO and left set consistent with the assumptions of the plant specific setpoint analysis (Ref. 7). As found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference 10.

A test signal is 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. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

Matrix Logic Tests

Matrix Logic tests are addressed in LCO 3.3.3. 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.

Trip Path Tests

Trip Path (Initiation Logic) tests are addressed in LCO 3.3.3. 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 Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10).

BASES

SURVEILLANCE REQUIREMENTS (*continued*)

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. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [10].

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 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 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 and Power Rate of Change channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. 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 Evaluation" (Ref. 10). 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

SR 3.3.1.8 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the frequency extension analysis. The requirements for this review are outlined in Reference [10].

The Frequency is based upon the assumption of an 18 month calibration interval for the determination of the magnitude of equipment drift.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 3.3.1.9

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 surveillances of a given channel of n x 18 months, where n is the number of channels in the function. The Frequency of

[18] months 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.

----------REVIEWER'S NOTE----------
Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

BASES

SURVEILLANCE REQUIREMENTS (continued)

A Note is added to indicate that the neutron detectors are 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).

REFERENCES

1. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."
2. 10 CFR 50, Appendix A, GDC 21.
3. 10 CFR 100.
4. IEEE Standard 279-1971, April 5, 1972.
5. FSAR, Chapter [14].
6. 10 CFR 50.49.
7. "Plant Protection System Selection of Trip Setpoint Values."
8. FSAR, Section [7.2].
9. NRC Safety Evaluation Report, [Date].
10. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.
11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

BASES

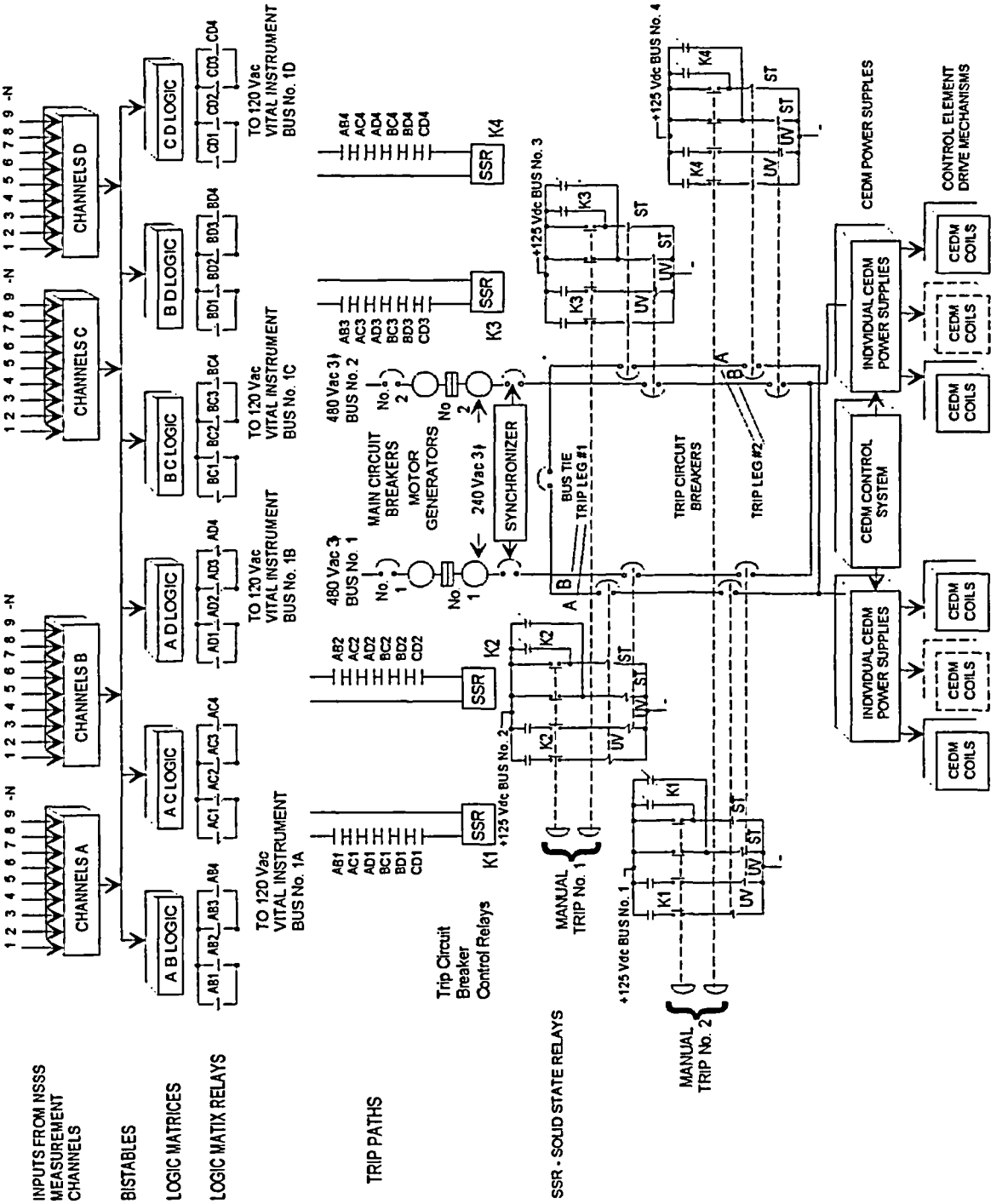


Figure B 3.3.1-1 (page 1 of 1)
Functional Diagram of the Two-Out-of-Four Logic and RTCB Configuration

B 3.3 INSTRUMENTATION

B 3.3.1 Reactor Protective System (RPS) Instrumentation - Operating (Digital)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and breaching the reactor coolant pressure boundary (RCPB) during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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.

Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded." The Analytic Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that a SL is not exceeded. Any automatic protection action that occurs on reaching the Analytic Limit therefore ensures that the SL is not exceeded. However, in practice, the actual settings for automatic protective devices must be chosen to be more conservative than the Analytic Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

The trip setpoint is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytic Limit and thus ensuring that the SL would not be exceeded. As such, the trip setpoint accounts for uncertainties in setting the device (e.g., calibration), uncertainties in how the device might actually perform (e.g., repeatability), changes in the point of action of the device over time (e.g., drift during surveillance intervals), and any other factors which may influence its actual performance (e.g., harsh accident environments). In this manner, the trip setpoint plays an important role in ensuring that SLs are not exceeded. As such, the trip setpoint meets the definition of an LSSS (Ref. 1) and could be used to meet the requirement that they be contained in the Technical Specifications.

BASES

BACKGROUND (continued)

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." For automatic protective devices, the required safety function is to ensure that a SL is not exceeded and therefore the LSSS as defined by 10 CFR 50.36 is the same as the OPERABILITY limit for these devices. However, use of the trip setpoint to define OPERABILITY in Technical Specifications and its corresponding designation as the LSSS required by 10 CFR 50.36 would be an overly restrictive requirement if it were applied as an OPERABILITY limit for the "as found" value of a protective device setting during a Surveillance. This would result in Technical Specification compliance problems, as well as reports and corrective actions required by the rule which are not necessary to ensure safety. For example, an automatic protective device with a setting that has been found to be different from the trip setpoint due to some drift of the setting may still be OPERABLE since drift is to be expected. This expected drift would have been specifically accounted for in the setpoint methodology for calculating the trip setpoint and thus the automatic protective action would still have ensured that the SL would not be exceeded with the "as found" setting of the protective device. Therefore, the device would still be OPERABLE since it would have performed its safety function and the only corrective action required would be to reset the device to the trip setpoint to account for further drift during the next surveillance interval.

Use of the trip setpoint to define "as found" OPERABILITY and its designation as the LSSS under the expected circumstances described above would result in actions required by both the rule and Technical Specifications that are clearly not warranted. However, there is also some point beyond which the device would have not been able to perform its function due, for example, to greater than expected drift. This value needs to be specified in the Technical Specifications in order to define OPERABILITY of the devices and is designated as the Allowable Value which, as stated above, is the same as the LSSS.

The Allowable Valuable specified in Table 3.3.1-1 serves as the LSSS such that a channel is OPERABLE if the trip setpoint is found not to exceed the Allowable Value. As such, the Allowable Value differs from the trip setpoint by an amount primarily equal to the expected instrument loop uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will still meet the LSSS definition and ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the

BASES

BACKGROUND (continued)

surveillance interval. If the actual setting of the device is found to have exceeded the Allowable Value the device would be considered inoperable from a Technical Specification perspective. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required. Note that, although the channel is "OPERABLE" under these circumstances, the trip setpoint should be left adjusted to a value within the established trip setpoint calibration tolerance band, in accordance with uncertainty assumptions stated in the referenced setpoint methodology (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling (DNB),
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System (RCS) pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 2) and 10 CFR 100 (Ref. 3) 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 (Ref. 3) limits. Different accident categories allow a different fraction of these limits based on probability of 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,

BASES

BACKGROUND (continued)

- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses measurement channels and bistable trip units. It also addresses the automatic bypass removal feature for those trips with operating bypasses. The RPS Logic and RTCBs are addressed in LCO 3.3.4, "Reactor Protective System (RPS) Logic and Trip Initiation." The CEACs are addressed in LCO 3.3.3, "Control Element Assembly Calculators (CEACs)."

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.

The excore nuclear instrumentation, the core protection calculators (CPCs), and the CEACs, though complex, are considered components in the measurement channels of the Linear Power Level - High, Logarithmic 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 may also be used as inputs to Engineered Safety Features Actuation System (ESFAS) bistables, and most provide indication in the control room. 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.

BASES

BACKGROUND (continued)

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. 2). 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 or prevent a required trip from occurring.

----------REVIEWER'S NOTE----------

In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated and approved by the NRC staff. Plants not currently licensed so as to credit four channel independence and that desire this capability must have approval of the NRC staff documented by an NRC Safety Evaluation Report (SER) (Ref. 4).

Adequate channel to channel independence includes physical and electrical independence of each channel from the others. This allows operation in two-out-of-three logic with one channel removed from service until following the next MODE 5 entry. Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control, this arrangement meets the requirements of IEEE Standard 279-1971 (Ref. 5).

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 DNBR - Low and LPD - High pretrip and trip signals. The 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 speed,

BASES

BACKGROUND (continued)

- 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 (APD) (based on excore flux levels and CEA positions), calculation of coolant flow (based on pump speed), and calculation of calibrated average power level (based on excore flux levels and ΔT power).

The DNBR calculation considers primary pressure, inlet temperature, coolant flow, average power, APD, 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 APD, average power, radial peaking factors (based upon target CEA position), and CEAC penalty factors to calculate the current value of compensated peak power density. An 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 cathode ray tube (CRT), which is switchable between CEACs. The CRT displays individual CEA positions and current values of the penalty factors from the selected CEAC.

BASES

BACKGROUND (continued)

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.

CEACs are addressed in LCO 3.3.3.

Bistable Trip Units

Bistable trip units, mounted in the Plant Protection System (PPS) cabinet, receive an analog input from the measurement channels. They 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, B, C, and D, for each RPS parameter, one for each measurement channel. Bistables 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 a reactor trip (two-out-of-four logic).

Some measurement channels provide contact outputs to the PPS. In these cases, there is no bistable card, and opening the contact input directly de-energizes the associated bistable relays. These include the Loss of Load trip and the CPC generated DNBR - Low and LPD - High trips.

The trip setpoints used in the bistables are based on the analytical limits derived from the accident analysis (Ref. 6). 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. 7), Allowable Values specified in Table 3.3.1-1, in the accompanying LCO, are

BASES

BACKGROUND (continued)

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. 8). 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 interval between surveillances. A channel is inoperable if its actual setpoint is not within its Allowable Value.

Setpoints in accordance with the Allowable Value will ensure that SLs of Chapter 2.0, "SAFETY LIMITS (SLs)," 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.

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. FSAR, Section [7.2] (Ref. 9), provides more detail on RPS testing. Processing transmitter calibration is normally performed on a refueling basis.

RPS Logic

The RPS Logic, addressed in LCO 3.3.4, consists of both Matrix and Initiation Logic and 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.

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.

BASES

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, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

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

BASES

BACKGROUND (continued)

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 on 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.

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 are normally 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, and CPC (DNBR - Low and LPD - High).

The Loss of Load trip bypass is automatically enabled and disabled.

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear, addressed in LCO 3.3.4, 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.

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.

BASES

BACKGROUND (continued)

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 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 Trip push buttons, arranged in two sets of two. Depressing both push buttons in either set will result in a reactor trip.

When a Manual 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 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. FSAR, Section [7.2] (Ref. 9), explains RPS testing in more detail.

APPLICABLE SAFETY ANALYSES

Design Basis Definition

The RPS is designed to ensure that the following operational criteria are met:

- The associated actuation will occur when the parameter monitored by each channel reaches its setpoint and the specific coincidence logic is satisfied,
- Separation and redundancy are maintained to permit a channel to be out of service for testing or maintenance while still maintaining redundancy within the RPS instrumentation network.

Each of the analyzed accidents and transients can be detected by one or more RPS Functions. The accident analysis takes credit for most of the RPS trip Functions. Those functions for which no credit is taken, termed equipment protective functions, are not needed from a safety perspective.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Each RPS setpoint is chosen to be consistent with the function of the respective trip. The basis for each trip setpoint falls into one of three general categories:

Category 1: To ensure that the SLs are not exceeded during AOOs,

Category 2: To assist the ESFAS during accidents, and

Category 3: To prevent material damage to major plant components (equipment protective).

The RPS maintains the SLs during AOOs and mitigates the consequences of DBAs in all MODES in which the RTCBs are closed.

Each of the analyzed transients and accidents can be detected by one or more RPS Functions. Functions not specifically credited in the accident analysis are part of the NRC staff approved licensing basis for the plant. Noncredited Functions include the Loss of Load. This trip is purely equipment protective, and its use minimizes the potential for equipment damage.

The specific safety analysis applicable to each protective function are identified below:

1. Linear Power Level - High

   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).

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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 logarithmic power is < 1E-4%. For events originating above this power level, other trips provide adequate protection.

MODES 3, 4, and 5, with the RTCBs closed, are addressed in LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown."

In MODES 3, 4, or 5, with the RTCBs open or the CEAs not capable of withdrawal, the Logarithmic Power Level - High trip does not have to be OPERABLE. However, the indication and alarm portion of two logarithmic 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 3.3.13, "[Logarithmic] Power Monitoring Channels."

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 (MSSVs), it provides protection against overpressurization of the RCPB 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).

4. Pressurizer Pressure - Low

The Pressurizer Pressure - Low trip is provided to trip the reactor to assist the ESF System in the event of loss of coolant accidents (LOCAs). During a LOCA, the SLs may be exceeded; however, the consequences of the accident will be acceptable. A Safety Injection Actuation Signal (SIAS) and a Containment Isolation Actuation Signal (CIAS) are initiated simultaneously.

BASES

APPLICABLE SAFETY ANALYSES (continued)

5. Containment Pressure - High

The Containment Pressure - High trip prevents exceeding the containment design pressure psig during a design basis LOCA or main steam line break (MSLB) accident. During a LOCA or MSLB the SLs may be exceeded; however, the consequences of the accident will be acceptable. An SIAS and CIAS are initiated simultaneously.

6, 7. Steam Generator Pressure - Low

The Steam Generator #1 Pressure - Low and Steam Generator #2 Pressure - Low trips provide protection against an excessive rate of heat extraction from the steam generators and resulting rapid, uncontrolled cooldown of the RCS. This trip is needed to shut down the reactor and assist the ESF System in the event of an MSLB or main feedwater line break accident. A main steam isolation signal (MSIS) is initiated simultaneously.

8, 9. Steam Generator Level – Low

The Steam Generator #1 Level - Low and Steam Generator #2 Level - Low trips ensure 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 a Steam Generator Atmospheric Dump Valve (AOO),
- Loss of Normal Feedwater Event (AOO), and
- Feedwater System Pipe Break (Accident).

10, 11. Reactor Coolant Flow – Low

The Reactor Coolant Flow, Steam Generator #1 - Low and Reactor Coolant Flow, Steam Generator #2 - Low trips provides protection against an RCP Sheared Shaft Event. The DNBR limit may be exceeded during this event; however, the trip ensures the consequences are acceptable.

BASES

APPLICABLE SAFETY ANALYSES (continued)

12. Loss of Load

The Loss of Load (turbine stop valve control oil pressure) is anticipatory for the loss of heat removal capabilities for 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 RPS Loss of Load reactor trip channels receive their input from sensors mounted on high pressure turbine stop valve (TSV) actuators. Since there are four TSVs, one actuator per TSV and one sensor per actuator, each sensor sends its signal to a different RPS channel. When the control oil pressure drops to the appropriate setpoint, a reactor trip signal is generated.

13. Local Power Density – High

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. The DNBR - Low and LPD - High trips provide plant protection during the following AOOs and assist the ESF systems in the mitigation of the following accidents.

The LPD - High trip provides protection against fuel centerline melting due to the occurrence of excessive local power density peaks during the following AOOs:

- Decrease in Feedwater Temperature,
- Increase in Feedwater Flow,
- Increased Main Steam Flow (not due to the steam line rupture) Without Turbine Trip,
- Uncontrolled CEA Withdrawal From Low Power,
- Uncontrolled CEA Withdrawal at Power, and
- CEA Misoperation; Single Part Length CEA Drop.

BASES

APPLICABLE SAFETY ANALYSES (continued)

For the events listed above (except CEA Misoperation; Single Part Length CEA Drop), DNBR - Low will trip the reactor first, since DNB would occur before fuel centerline melting would occur.

14. Departure from Nucleate Boiling Ratio (DNBR) - Low

The CPCs perform the calculations required to derive the DNBR and LPD parameters and their associated RPS trips. The DNBR - Low and LPD - High trips provide plant protection during the following AOOs and assist the ESF systems in the mitigation of the following accidents.

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,
- Total Loss of Forced Reactor Coolant Flow,
- Single Reactor Coolant Pump (RCP) Shaft Seizure,
- Uncontrolled CEA Withdrawal From Low Power,
- Uncontrolled CEA Withdrawal at Power,
- CEA Misoperation; Full Length CEA Drop,

BASES

APPLICABLE SAFETY ANALYSES (continued)

- CEA Misoperation; Part Length CEA Subgroup Drop,
- Primary Sample or Instrument Line Break, and
- Steam Generator Tube Rupture.

In the above list, only the steam generator tube rupture, the RCP shaft seizure, and the sample or instrument line break are accidents. The rest are AOOs.

Interlocks/Bypasses

The bypasses and their Allowable Values are addressed in footnotes to Table 3.3.1-1. They are not otherwise addressed as specific Table entries.

The automatic bypass removal features must function as a backup to manual actions for all safety related trips to ensure the trip Functions are not operationally bypassed when the safety analysis assumes the Functions are not bypassed. The basis for each of the operating 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. DNBR - Low and LPD - High, and

e. Pressurizer Pressure - Low.

The RPS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires all instrumentation performing an RPS Function to be OPERABLE. Failure of any required portion of the instrument channel renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

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. With one channel in each Function trip channel bypassed, this effectively places the plant in a two-out-of-three logic configuration in those Functions.

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 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 are consistent with the assumptions of the plant specific setpoint calculations. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value. 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. 8).

The Bases for the individual Function requirements are as follows:

1. Linear Power Level - High

   This LCO requires all four channels of Linear Power Level - High to be OPERABLE in MODES 1 and 2.

   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.

2. Logarithmic Power Level - High

   This LCO requires all four channels of 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.

BASES

LCO (continued)

The MODES 3, 4, and 5 Condition is addressed in LCO 3.3.2.

The Allowable Value is high 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 logarithmic power is above 1E-4% to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when logarithmic power decreases below 1E-4%. Above 1E-4%, the Linear Power Level - High and Pressurizer Pressure - High trips provide protection for reactivity transients.

The trip may be manually bypassed during physics testing pursuant to LCO 3.4.17, "RCS Loops - Test Exceptions." During this testing, the Linear Power Level - High trip and administrative controls provide the required protection.

3. Pressurizer Pressure - High

This LCO requires four channels of Pressurizer Pressure - High to be OPERABLE in MODES 1 and 2.

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 valves during normal plant operation. In the event of a complete loss of electrical load from 100% power, this setpoint ensures the reactor trip will take place, thereby limiting further heat input to the RCS and consequent pressure rise. The pressurizer safety valves may lift to prevent overpressurization of the RCS.

4. Pressurizer Pressure - Low

This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1 and 2.

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.

BASES

LCO (continued)

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 < 400 psia. 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 500 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 pressure increases above 500 psia.

5. Containment Pressure - High

The LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. It is set low enough to initiate a reactor trip when an abnormal condition is indicated.

6, 7. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator #1 Pressure - Low and Steam Generator #2 Pressure - Low to be OPERABLE in MODES 1 and 2.

This 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.

BASES

LCO (continued)

The trip setpoint may be manually decreased as steam generator pressure is reduced during controlled plant cooldown, provided the margin between steam generator pressure and the setpoint is maintained < 200 psia. This allows for controlled depressurization of the secondary system while still maintaining an active reactor trip setpoint and MSIS setpoint, until the time is reached when the setpoints are no longer needed to protect the plant. The setpoint increases automatically as steam generator pressure increases until the specified trip setpoint is reached.

8, 9. Steam Generator Level – Low

This LCO requires four channels of Steam Generator #1 Level - Low and Steam Generator #2 Level - Low for each steam generator to be OPERABLE in MODES 1 and 2.

The Allowable Value is sufficiently below the normal operating level for the steam generators 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 Signals (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 may be manually bypassed 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.

10, 11. Reactor Coolant Flow – Low

This LCO requires four channels of Reactor Coolant Flow, Steam Generator #1 - Low and Reactor Coolant Flow, Steam Generator #2 - Low to be OPERABLE in MODES 1 and 2. The Allowable Value is set low enough to allow for 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 to maintain DNBR under the expected pressure conditions for this event.

BASES

LCO (continued)

The Reactor Coolant Flow - Low trip may be manually bypassed when logarithmic power is less than 1E-4%. This allows for de-energization of one or more 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, "RCS Loops - MODE 3," LCO 3.4.6, "RCS Loops - MODE 4," and LCO 3.4.7, "RCS Loops - MODE 5, Loops Filled," ensure adequate RCS flow rate is maintained. The bypass is automatically removed when logarithmic power increases above 1E-4%, as sensed by the wide range (logarithmic) nuclear instrumentation. When below the power range, the Reactor Coolant Flow - Low is not required for plant protection.

12. Loss of Load

This LCO requires four channels of Loss of Load trip to be OPERABLE in MODES 1 and 2.

The Steam Bypass Control System is capable of passing 45% of the full power main steam flow (45% RTP bypass capability) directly to the condenser without causing the MSSVs to lift. The Nuclear Steam Supply System 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 MSSV 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. Both the bypass and bypass removal, when above 55% power, are automatically performed.

Loss of Load trip is equipment protective and not credited in the accident analysis. As such, the 55% bypass power permissive is a nominal value and does not include any instrument uncertainties.

BASES

LCO (continued)

13. Local Power Density – High

This LCO requires four channels of LPD - High to be OPERABLE.

The LCO on the CPCs ensures that the SLs are maintained during all AOOs and the consequences of accidents are acceptable.

A CPC is not considered inoperable if CEAC inputs to the CPC are inoperable. The Required Actions required in the event of CEAC channel failures ensure the CPCs are capable of performing their safety Function.

The CPC channels may be manually bypassed below 1E-4%, as sensed by the logarithmic nuclear instrumentation. This bypass is enabled manually 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 with Pressurizer Pressure - Low or RCPs off.

During special testing pursuant to LCO 3.4.17, the CPC channels may be manually bypassed when THERMAL POWER is below 5% RTP to allow special testing without generating a reactor trip. The Linear Power Level - High trip setpoint is reduced, so as to provide protection during testing.

14. Departure from Nucleate Boiling Ratio (DNBR) – Low

This LCO requires four channels of DNBR - Low to be OPERABLE.

The LCO on the CPCs ensures that the SLs are maintained during all AOOs and the consequences of accidents are acceptable.
A CPC is not considered inoperable if CEAC inputs to the CPC are inoperable. The Required Actions required in the event of CEAC channel failures ensure the CPCs are capable of performing their safety Function.

BASES

LCO (continued)

The CPC channels may be manually bypassed below 1E-4%, as sensed by the logarithmic nuclear instrumentation. This bypass is enabled manually 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 with Pressurizer Pressure - Low or RCPs off.

During special testing pursuant to LCO 3.4.17, the CPC channels may be manually bypassed when THERMAL POWER is below 5% RTP to allow special testing without generating a reactor trip. The Linear Power Level - High trip setpoint is reduced, so as to provide protection during testing.

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 are inadvertently bypassed.

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 2), 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.

BASES

APPLICABILITY

Most RPS trips are required to be OPERABLE in MODES 1 and 2 because the reactor is critical in these MODES. The reactor 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. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM. Exceptions to this are:

- The Logarithmic Power Level - High trip, RPS Logic RTCBs, and Manual Trip are required in MODES 3, 4, and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events.

The Logarithmic Power Level - High trip in these lower MODES is addressed in LCO 3.3.2. The Logarithmic Power Level - High trip is bypassed prior to MODE 1 entry and is not required in MODE 1. The RPS Logic in MODES 1, 2, 3, 4, and 5 is addressed in LCO 3.3.4.

ACTIONS

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) 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 trip unit 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.

BASES

ACTIONS (continued)

A Note has been added to the ACTIONS. The Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Times of each inoperable Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1 and A.2

Condition A applies to the failure of a single trip channel or associated instrument channel inoperable in any RPS automatic trip Function. RPS coincidence logic is two-out-of-four.

If one RPS channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip in 1 hour (Required Action A.1). The 1 hour allotted to 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. The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel in bypass, the coincidence logic is now in a two-out-of-three configuration.

The Completion Time of prior to entering MODE 2 following the next MODE 5 entry is based on adequate channel to channel independence, which allows a two-out-of-three channel operation since no single failure will cause or prevent a reactor trip.

B.1

Condition B applies to the failure of two channels in any RPS automatic trip Function.

Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels while ensuring 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.

BASES

ACTIONS (continued)

One of the two inoperable channels will need to be restored to operable status prior to the next required CHANNEL FUNCTIONAL TEST, because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one RPS channel, and placing a second channel in trip will result in a reactor trip. Therefore, if one RPS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic bypass removal channel inoperable. If the inoperable bypass removal channel for any bypass channel cannot be restored to OPERABLE status within 1 hour, 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 A, and the affected automatic trip channel placed in bypass or trip. The bypass removal channel and the automatic trip channel must be repaired prior to entering MODE 2 following the next MODE 5 entry. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

D.1 and D.2

Condition D applies to two inoperable automatic bypass removal channels. If the bypass removal channels for two operating bypasses cannot be restored to OPERABLE status within 1 hour, 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 B, and the bypass either removed or one automatic trip channel placed in bypass and the other in trip within 1 hour. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST, or the plant must shut down per LCO 3.0.3 as explained in Condition B.

BASES

ACTIONS (continued)

E.1

Condition E 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. CEAC OPERABILITY is addressed in LCO 3.3.3.

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. The Completion Time of 12 hours is adequate considering the low probability of undetected failure, the consequences of a single channel failure, and the time required to perform a CHANNEL FUNCTIONAL TEST.

F.1

Condition F applies if an OPERABLE CPC has three or more autorestarts in a 12 hour period.

CPCs and CEACs will attempt to autorestart if they detect a fault condition, such as a calculator malfunction or loss of power. A successful autorestart restores the calculator to operation; however, excessive autorestarts might be indicative of a calculator problem.

If a nonbypassed CPC has three or more autorestarts, it may not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed on the CPC to ensure it is functioning properly. Based on plant operating experience, the Completion Time of 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 online diagnostics.

G.1

Condition G is entered when the Required Action and associated Completion Time of Condition A, B, C, D, E, or F are not met.

BASES

ACTIONS (continued)

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 allowed Completion Time of 6 hours is reasonable, based on operating experience, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant systems.

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.

----------REVIEWER'S NOTE----------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff SER that establishes the acceptability of each topical report for that unit.

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 normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. 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.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

In the case of RPS trips with multiple inputs, such as the DNBR and LPD inputs to the CPCs, a CHANNEL CHECK must be performed on all inputs.

SR 3.3.1.2

The RCS flow rate indicated by each CPC is verified, as required by a Note, to be less than or equal to the actual RCS total flow rate every 12 hours when THERMAL POWER is ≥ 70% RTP. The 12 hours after reaching 70% RTP is for plant stabilization, data taking, and flow verification. This check (and if necessary, the adjustment of the CPC addressable constant flow coefficients) ensures that the DNBR setpoint is conservatively adjusted with respect to actual flow indications, as determined by the Core Operating Limits Supervisory System (COLSS).

SR 3.3.1.3

The CPC autorestart count is checked every 12 hours to monitor the CPC and CEAC for normal operation. If three or more autorestarts of a nonbypassed CPC occur within a 12 hour period, the CPC may not be completely reliable. Therefore, the Required Action of Condition F must be performed. The Frequency is based on 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 ≥ 20%. The Linear Power Level signal and the CPC 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 (and, if necessary, the adjustment of the Linear Power Level signal and the CPC addressable constant coefficients) are adequate to ensure that the accuracy of these CPC calculations is maintained within the analyzed error margins. The power level must be > 20% RTP to obtain accurate data. At lower power levels, the accuracy of calorimetric data is questionable.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 Frequency is modified by a Note indicating this Surveillance need only be performed within 12 hours after reaching 20% RTP. The 12 hours after reaching 20% RTP is required for plant stabilization, data taking, and flow verification. The secondary calorimetric is inaccurate at lower power levels. A second Note in the SR indicates the SR may be suspended during PHYSICS TESTS. The conditional suspension of the daily calibrations under strict administrative control is necessary to allow special testing to occur.

SR 3.3.1.5

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. The Note indicates the Surveillance is performed within 12 hours after THERMAL POWER is ≥ 70% RTP. This check (and, if necessary, the adjustment of the CPC addressable flow constant coefficients) 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 Frequency is adequate, as instrument drift is minimal and changes in actual flow rate are minimal over core life.

SR 3.3.1.6

The three vertically mounted excore nuclear instrumentation detectors in each channel are used to determine APD 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 3.3.1.12, which adjusts the gains of the three detector amplifiers for shape annealing. SR 3.3.1.6 ensures that the preassigned gains are still proper. Power must be > 15% because the CPCs do not use the excore generated signals for axial flux shape information at low power levels. The Note allowing 12 hours after reaching 15% RTP is required for plant stabilization and testing.

The 31 day Frequency is adequate because the demonstrated long term drift of the instrument channels is minimal.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.7

A CHANNEL FUNCTIONAL TEST on each channel except Loss of Load, power range neutron flux, and logarithmic power level channels is performed every 92 days to ensure the entire channel will perform its intended function when needed. The SR is modified by two Notes. Note 1 is a requirement to verify the correct CPC addressable constant values are installed in the CPCs when the CPC CHANNEL FUNCTIONAL TEST is performed. Note 2 allows the CHANNEL FUNCTIONAL TEST for the Logarithmic Power Level - High channels to be performed 2 hours after logarithmic power drops below 1E-4% and is required to be performed only if the RTCBs are closed.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 9. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

Bistable Tests

A test signal is 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. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the interval between surveillance interval extension analysis. The requirements for this review are outlined in Reference [10].

Matrix Logic Tests

Matrix Logic tests are addressed in LCO 3.3.4. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Trip Path Tests

Trip path (Initiation Logic) tests are addressed in LCO 3.3.4. 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, thereby 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 Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10).

The CPC and CEAC channels and excore nuclear instrumentation channels are tested separately.

The excore 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.

The quarterly CPC CHANNEL FUNCTIONAL TEST is performed using software. This software includes preassigned addressable constant values that may differ from the current values. Provisions are made to store the addressable constant values on a computer disk prior to testing and to reload them after testing. A Note is added to the Surveillance Requirements to verify that the CPC CHANNEL FUNCTIONAL TEST includes the correct values of addressable constants. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.1.8

A Note indicates that neutron detectors are excluded from CHANNEL CALIBRATION. A CHANNEL CALIBRATION of the power range neutron flux channels every 92 days ensures that the channels are reading accurately and within tolerance (Ref. 10). The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the interval between surveillance interval extension analysis. The requirements for this review are outlined in Reference 10. Operating experience has shown this Frequency to be satisfactory. The 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 3.3.1.6). In addition, the associated control room indications are monitored by the operators.

[SR 3.3.1.9

The characteristics and Bases for this Surveillance are as described for SR 3.3.1.7. This Surveillance 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 will ensure the channel will perform its equipment protective function if needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Note allowing 2 hours after reaching 55% RTP is necessary for Surveillance performance. This Surveillance cannot be performed below 55% RTP, since the trip is bypassed.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

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 sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [10].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis as well as operating experience and consistency with the typical [18] month fuel cycle.

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 3.3.1.4) and the monthly linear subchannel gain check (SR 3.3.1.6).

SR 3.3.1.11

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the CPCs. The CHANNEL FUNCTIONAL TEST shall include the injection of a signal as close to the sensors as practicable to verify OPERABILITY including alarm and trip Functions. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The basis for the [18] month Frequency is that the CPCs perform a continuous self monitoring function that 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 do not occur in any given [18] month interval.

SR 3.3.1.12

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 or verify 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 the shape annealing matrix coefficients.

Incore detectors are inaccurate at low power levels. THERMAL POWER should be significant but < 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. Operating experience has shown this Frequency to be acceptable.

SR 3.3.1.13

SR 3.3.1.13 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.1.7, except SR 3.3.1.13 is applicable only to bypass functions and is performed once within 92 days prior to each startup. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical

BASES

SURVEILLANCE REQUIREMENTS (continued)

Specifications tests at least once per refueling interval with applicable extensions. 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 Surveillance within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 10). 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 3.3.1.7 or SR 3.3.1.9. Therefore, further testing of the bypass function after startup is unnecessary.

SR 3.3.1.14

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 surveillances of a given channel of n x 18 months, where n is the number of channels in the function. The Frequency of [18] months 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.

----------REVIEWER'S NOTE----------

Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

BASES

SURVEILLANCE REQUIREMENTS (continued)

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

A Note is added to indicate that the neutron detectors are 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 3.3.1.4).

REFERENCES

1. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."
2. 10 CFR 50, Appendix A, GDC 21.
3. 10 CFR 100.
4. NRC Safety Evaluation Report.
5. IEEE Standard 279-1971, April 5, 1972.
6. FSAR, Chapter [14].
7. 10 CFR 50.49.
8. "Plant Protection System Selection of Trip Setpoint Values."
9. FSAR, Section [7.2].
10. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.
11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

B 3.3 INSTRUMENTATION

B 3.3.2 Reactor Protective System (RPS) Instrumentation - Shutdown (Analog)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and reactor coolant pressure boundary integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) 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 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO applies only to the Power Rate of Change - High trip Functions and associated instrument channels in MODES 3, 4, and 5 with any of the RTCBs closed and any Control Element Assembly (CEA) capable of being withdrawn. In MODES 1 and 2, this trip Function is addressed in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating." LCO 3.3.13, "[Logarithmic] Power Monitoring Channels," applies when the RTCBs are open or CEA Drive System is not capable of CEA withdrawal. In the case of LCO 3.3.13, the logarithmic power instrumentation channels are required for monitoring neutron flux, although the trip Function is not required.

Measurement Channels and Trip Units

The measurement channels providing input to the Power Rate of Change - High Function consist of wide range nuclear instrumentation channels using neutron flux leakage from the reactor vessel.

Other aspects of the Power Rate of Change - High trip are similar to the other measurement channels and bistable trip units. These are addressed in the Background section of LCO 3.3.1.

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 3 takes credit for most RPS trip Functions. Functions not specifically credited in the accident analysis were qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the plant. These Functions may provide protection for conditions that do not require dynamic transient analysis to demonstrate Function performance. Other Functions, such as the Loss of Load trip, are purely equipment protective, and their use minimizes the potential for equipment damage.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 trip is not required for protection. It serves as a backup to the administratively enforced startup rate limit.

The Power Rate of Change - High Function minimizes transients for events such as a continuous CEA withdrawal or a boron dilution event from low power levels. The Power Rate of Change - High trip is automatically bypassed at < 1E-4% RTP, as sensed by the wide range nuclear instrument (NI) Level 2 bistable, when poor counting statistics may lead to erroneous indication. It is also bypassed at > 12% RTP, where moderator temperature coefficient and fuel temperature coefficient make high rate of change of power unlikely. This bypass is effected by the power range NI Level 1 bistable. Automatic bypass removal is also effected by these bistables. 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 to be OPERABLE. LCO 3.3.13 ensures the wide range channels are available to detect and alert the operator to a boron dilution event.

The RPS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all instrumentation performing an RPS Function to be OPERABLE. Failure of any required portion of the instrument channel or bypass removal channel renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

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.

This LCO requires four channels of Power Rate of Change - High to be OPERABLE in MODES 3, 4, and 5, when the RTCBs are closed and the CEA Drive System is capable of CEA withdrawal. MODE 1 and 2 requirements are addressed in LCO 3.3.1. This trip is not credited in the safety analysis. Therefore, the Allowable Value specified in SR 3.3.4.2 is not derived from an analytical limit.

BASES

APPLICABILITY

This LCO is applicable to the Power Rate of Change - High reactor trip in MODES 3, 4 and 5. MODES 1 and 2 are addressed in LCO 3.3.1.

The power rate of change trip is required in MODES 3, 4, and 5, with the RTCBs closed and a CEA capable of being withdrawn to provide backup protection for boron dilution and CEA withdrawal events. The power rate of change trip is not credited in the safety analysis, but is part of the NRC approved licensing basis for the plant.

The power rate of change trip has operating bypasses discussed in the LCO section. In MODES 3, 4, and 5, the emphasis is placed on return to power events. The reactor is protected in these MODES by ensuring adequate SDM.

ACTIONS

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) 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 plant 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.

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

Condition A applies to the failure of a single channel of the Power Rate of Change - High RPS automatic trip Function.

BASES

ACTIONS (continued)

RPS coincidence logic is normally two-out-of-four. If one RPS bistable trip unit or associated instrument channel is inoperable, startup or power operation is allowed to continue, providing the inoperable trip unit is placed in bypass or trip within 1 hour (Required Action A.1). With one channel in bypass, no additional random failure of a single channel could spuriously trip the reactor and a valid trip signal can still trip the reactor. With one channel in trip, an additional random failure of a single channel could spuriously trip the reactor. Therefore, it is preferable to place an inoperable channel in bypass rather than trip.

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, while ensuring 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 A.2.1 or Required Action A.2.2). Required Action A.2.1 restores the full capability of the Function. Required Action A.2.2 places the Function in 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.

B.1 and B.2

Condition B applies to the failure of two channels in the Power Rate of Change - High RPS automatic trip Function.

Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion Time is sufficient to allow the operator to take all appropriate actions for the failed channels, while ensuring 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.

BASES

ACTIONS (continued)

[The bypassed channel should be restored to OPERABLE status within 48 hours for reasons similar to those stated under Condition A. After one channel is restored to OPERABLE status, 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.2 shall be placed in trip if more than 48 hours have elapsed since the initial channel failure.]

C.1, C.2.1, C.2.2.1, and C.2.2.2

Condition C applies to one automatic bypass removal channel inoperable. If the bypass removal channel cannot be restored to OPERABLE status, the associated Power Rate of Change - High 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 A, and the bypass either removed or the bypass removal channel repaired. The Bases for the Required Actions and Completion Times are the same as discussed for Condition A.

D.1, D.2.1, and D.2.2

Condition D applies to two inoperable automatic bypass removal channels. If the bypass removal channels cannot be restored to OPERABLE status, the associated Power Rate of Change - High 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 B, and the bypass either removed or the bypass removal channel repaired. Also, Required Action D.2.2 provides for the restoration of the one affected automatic trip channel to OPERABLE status within the rules of Completion Time specified under Condition B. Completion Times are consistent with Condition B.

E.1

Condition E is entered when the Required Actions and associated Completion Times of Condition A, B, C, or D are not met.

BASES

ACTIONS (continued)

If Required Actions associated with these Conditions cannot be completed within the required Completion Time, opening the RTCBs brings the reactor to a MODE where the LCO does not apply and ensures no CEA withdrawal will occur. The basis for the Completion Time of 6 hours is that it is adequate to complete the Required Actions without challenging plant systems, including the insertion of CEAs for plants that normally maintain CEAs withdrawn when shut down.

SURVEILLANCE REQUIREMENTS

----------REVIEWER'S NOTE----------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that plant.

SR 3.3.2.1

Performance of the CHANNEL CHECK on each wide range channel once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally 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.

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 criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.2

A CHANNEL FUNCTIONAL TEST on the power rate of change channels is performed once every 92 days to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Power Rate of Change - High trip Function is required during startup operation and is bypassed when shut down or > 15% RTP. Additionally, operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 92 days prior to each reactor startup.

SR 3.3.2.3

SR 3.3.2.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.2.2, except SR 3.3.2.3 is applicable only to bypass Functions and is performed once within 92 days prior to each startup. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

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 Surveillance within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5). 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 3.3.2.2. Therefore, further testing of the bypass function after startup is unnecessary.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.4

SR 3.3.2.4 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

Only the Allowable Values are specified for each RPS trip Function. Nominal trip setpoints are specified 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 are 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. 4).

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference 5.

The Frequency is based upon the assumption of an [18] month calibration interval in the determination of the magnitude of equipment drift.

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.

BASES

REFERENCES

1. 10 CFR 50, Appendix A.
2. 10 CFR 100.
3. FSAR, Chapter [14].
4. "Plant Protection System Selection of Trip Setpoint Values."
5. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.2 Reactor Protective System (RPS) Instrumentation - Shutdown (Digital)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core fuel design limits and reactor coolant pressure boundary (RCPB) integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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 limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) 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 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO applies only to the Logarithmic Power Level - High trip in MODES 3, 4, and 5 with the RTCBs closed. In MODES 1 and 2, this trip Function is addressed in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating." LCO 3.3.13, "[Logarithmic] Power Monitoring Channels," applies when the RTCBs are open. In the case of LCO 3.3.13, the logarithmic channels are required for monitoring neutron flux, although the trip Function is not required.

Measurement Channels and Bistable Trip Units

The measurement channels providing input to the Logarithmic Power Level - High trip consist of the four logarithmic nuclear instrumentation channels detecting neutron flux leakage from the reactor vessel. Other aspects of the Logarithmic Power Level - High trip are similar to the other measurement channels and bistables. These are addressed in the Background section of LCO 3.3.1.

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 can be similarly tested. FSAR, Section [7.2] (Ref. 3), provides more detail on RPS testing.

APPLICABLE SAFETY ANALYSES

The RPS functions to maintain the SLs during AOOs and mitigates the consequence of DBAs in all MODES in which the RTCBs are closed.

Each of the analyzed transients and accidents can be detected by one or more RPS Functions. Functions not specifically credited in the accident analysis were qualitatively credited in the safety analysis and the NRC staff approved licensing basis for the plant. Noncredited Functions include the Loss of Load. The Loss of Load trip is purely equipment protective, and its use minimizes the potential for equipment damage.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 Control Element Assembly (CEA) Drive System capable of CEA withdrawal, protection is required for CEA withdrawal events originating when logarithmic power is < 1E-4%. For events originating above this power level, other trips provide adequate protection.

MODES 3, 4, and 5, with the RTCBs closed, are addressed in this LCO. MODE 2 is addressed in LCO 3.3.1.

In MODES 3, 4, or 5, with the RTCBs open or the CEAs not capable of withdrawal, the Logarithmic Power Level - High trip does not have to be OPERABLE. However, the indication and alarm portion of two logarithmic 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 3.3.13.

The RPS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires the Logarithmic Power Level - High RPS Function to be OPERABLE. Failure of any required portion of the instrument channel renders the affected channel(s) inoperable and reduces the reliability of the affected Function.

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. With one channel in each Function trip channel bypassed, this effectively places the plant in a two-out-of-three logic configuration in those Functions. 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).

This LCO requires all 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 closed and the CEA Drive System is capable of CEA withdrawal.

BASES

LCO (continued)

The Allowable Value specified in SR 3.3.2.4 is high 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 safety margin for unacceptable fuel cladding damage should a CEA withdrawal event occur.

The Logarithmic Power Level - High trip may be bypassed when logarithmic power is above 1E-4% to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when logarithmic power decreases below 1E-4%. Above 1E-4%, the Linear Power Level - High and Pressurizer Pressure - High trips provide protection for reactivity transients.

The trip may be manually bypassed during physics testing pursuant to LCO 3.4.17, "RCS Loops - Test Exceptions." During this testing, the Linear Power Level - High trip and administrative controls provide the required protection.

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 Engineered Safety Features Actuation System (ESFAS) in providing acceptable consequences during accidents. 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 ensuring adequate SDM. Exceptions to this are:

- The Logarithmic Power Level - High trip, RPS Logic RTCBs, and Manual Trip are required in MODES 3, 4, and 5, with the RTCBs closed, to provide protection for boron dilution and CEA withdrawal events. The Logarithmic Power Level - High trip in these lower MODES is addressed in this LCO. The RPS Logic in MODES 1, 2, 3, 4, and 5 is addressed in LCO 3.3.4, "Reactor Protective System (RPS) Logic and Trip Initiation."

The Applicability is modified by a Note that allows the trip to be bypassed when logarithmic power is > 1E-4%, and the bypass is automatically removed when logarithmic power is ≤ 1E-4%.

BASES

ACTIONS

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 stated in the LCO, the channel is declared inoperable immediately, and the appropriate Condition(s) must be entered immediately.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the excore logarithmic power channel or RPS bistable trip unit 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.

A.1, and A.2

Condition A applies to the failure of a single Logarithmic Power Level - High trip channel or associated instrument channel.

The Logarithmic Power Level - High coincidence logic is two-out-of-four. If one channel is inoperable, operation in MODES 3, 4, and 5 is allowed to continue, providing the inoperable channel is placed in bypass or trip in 1 hour (Required Action A.1).

The 1 hour allotted to bypass or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel while ensuring that the risk involved in operating with the failed channel is acceptable.

The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel bypassed, the coincidence logic is now in a two-out-of-three configuration. The Completion Time is based on adequate channel to channel independence, which allows a two-out-of-three channel operation since no single failure will cause or prevent a reactor trip.

BASES

ACTIONS (continued)

B.1

Condition B applies to the failure of two Logarithmic Power Level - High trip channels or associated instrument channels. Required Action B.1 provides for placing one inoperable channel in bypass and the other channel in trip within the Completion Time of 1 hour. This Completion 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.

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one RPS channel, and placing a second channel in trip will result in a reactor trip. Therefore, if one RPS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic bypass removal channel inoperable. If the bypass removal channel for the high logarithmic power level operating bypass cannot be restored to OPERABLE status within 1 hour, 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 A, and the bypass either removed or the affected automatic channel placed in trip or bypass. Both the bypass removal channel and the associated automatic trip channel must be repaired prior to entering MODE 2 following the next MODE 5 entry. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

BASES

ACTIONS (continued)

D.1 and D.2

Condition D applies to two inoperable automatic bypass removal channels. If the bypass removal channels for two operating bypasses cannot be restored to OPERABLE status within 1 hour, 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 B, and the bypass either removed or one automatic trip channel placed in bypass and the other in trip within 1 hour. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST or the plant must shut down per LCO 3.0.3, as explained in Condition B. Completion Times are consistent with Condition B.

E.1

Condition E is entered when the Required Actions and associated Completion Times of Condition A, B, C, or D are not met.

If Required Actions associated with these Conditions cannot be completed within the required Completion Time, all RTCBs must be opened, placing the plant in a condition where the logarithmic power trip channels are not required to be OPERABLE. A Completion Time of 1 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.

SURVEILLANCE REQUIREMENTS

The SRs for the Logarithmic Power Level - High trip are an extension of those listed in LCO 3.3.1, listed here because of their Applicability in these MODES.

----------REVIEWER'S NOTE----------
In order for a unit to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit (Ref. 5).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.1

SR 3.3.2.1 is the performance of a CHANNEL CHECK of each logarithmic power channel. This SR is identical to SR 3.3.1.1. Only the Applicability differs.

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally 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.

Agreement criteria are determined by the plant staff based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.2

A CHANNEL FUNCTIONAL TEST on each channel, except Loss of Load and power range neutron flux, is performed every 92 days to ensure the entire channel will perform its intended function when needed. This SR is identical to SR 3.3.1.7. Only the Applicability differs. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in the FSAR, Section [7.2] (Ref. 3). These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

Bistable Tests

A test signal is 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. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

Matrix Logic Tests

Matrix Logic Tests are addressed in LCO 3.3.4. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Trip Path Test

Trip path (Initiation Logic) tests are addressed in LCO 3.3.4. 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 Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 6). The excore 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.

SR 3.3.2.3

SR 3.3.2.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.2.2, except SR 3.3.2.3 is applicable only to bypass functions and is performed once within 92 days prior to each startup. This SR is identical to SR 3.3.1.13. Only the Applicability differs. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

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 Surveillance within 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 6). 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 3.3.2.2. Therefore, further testing of the bypass function after startup is unnecessary.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.4

SR 3.3.2.4 is the performance of a CHANNEL CALIBRATION every 18 months. This SR is identical to SR 3.3.1.10. Only the Applicability differs.

CHANNEL CALIBRATION is a complete check of the instrument channel excluding the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

Only the Allowable Values are specified for this RPS trip Function. Nominal trip setpoints are specified in the plant specific setpoint calculations. The nominal setpoint is 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 are 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. 4). A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [3].

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis and includes operating experience and consistency with the typical [18] month fuel cycle.

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 3.3.1.4).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.2.5

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 be performed in one measurement or in overlapping segments, with verification that all components are tested.

REFERENCES

1. 10 CFR 50.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. "Plant Protection System Selection of Trip Setpoint Values."
5. NRC Safety Evaluation Report.
6. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.3 Reactor Protective System (RPS) Logic and Trip Initiation (Analog)

BASES

BACKGROUND

The RPS initiates a reactor trip to protect against violating the core specified acceptable fuel design limits and reactor coolant pressure boundary integrity during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) 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 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses the RPS Logic and RTCBs, including Manual Trip capability. LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," provides a description of the role of this equipment in the RPS. This is summarized below:

RPS 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.

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.

BASES

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 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.

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 on 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.

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear, shown in Figure B 3.3.1-1, 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

BASES

BACKGROUND (continued)

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.

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 half of the control element assemblies (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 Trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two, as shown in Figure B 3.3.1-1. Depressing both push buttons in either set will result in a reactor trip.

When a Manual 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 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. FSAR, Section [7.2] (Ref. 3), explains RPS testing in more detail.

APPLICABLE SAFETY ANALYSES

Reactor Protective System (RPS) Logic

The RPS Logic provides for automatic trip initiation to maintain the SLs during AOOs and assist the ESF systems in ensuring acceptable consequences during accidents. All transients and accidents that call for a reactor trip assume the RPS Logic is functioning as designed.

BASES

APPLICABLE SAFETY ANALYSES (continued)

Reactor Trip Circuit Breakers (RTCBs)

All of the transient and accident analyses that call for a reactor trip assume that the RTCBs operate and interrupt power to the CEDMs.

Manual Trip

There are no accident analyses that take credit for the Manual Trip; however, the Manual 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.

The RPS Logic and initiation satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Reactor Protective System (RPS) Logic

Failures of individual bistable relays and their contacts are addressed in LCO 3.3.1. 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.

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.

BASES

LCO (continued)

If one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance 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, 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.

1. 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 any RTCB is closed and any CEA is capable of being withdrawn.

2. 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 any RTCB is closed and any CEA is capable of being withdrawn.

3. Reactor Trip Circuit Breakers (RTCBs)

   The LCO requires four RTCB channels to be OPERABLE in MODES 1 and 2, as well as in MODES 3, 4, and 5 when any RTCB is closed and any CEA is capable of being withdrawn.

   Each channel consists of two breakers operated in a single set by the Initiation Logic or Manual 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 actuated by the K-relay, and the contacts actuated by the Manual Trip, for each set of breakers. The K-relay actuated contacts and the upstream circuitry are considered to be RPS Logic. Manual Trip contacts and upstream circuitry are considered to be Manual Trip circuitry.

BASES

LCO (continued)

A Note associated with the ACTIONS states that if one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case, the redundant set of RTCBs will provide protection. 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. This Note is not applicable to Condition A, with one Matrix Logic channel inoperable.

4. Manual Trip

The LCO requires all four Manual Trip channels to be OPERABLE in MODES 1 and 2, and MODES 3, 4, and 5 when any RTCB is closed and any CEA is capable of being withdrawn.

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 either cause or prevent a reactor trip.

APPLICABILITY

The RPS Matrix Logic, RTCBs, and Manual Trip are required to be OPERABLE in any MODE when any CEA is capable of being withdrawn from the core (i.e., RTCBs closed and power available to the CEDMs). This ensures the reactor can be tripped when necessary, but allows for maintenance and testing when the reactor trip is not needed.

In MODES 3, 4, and 5 with all the RTCBs open, the CEAs are not capable of withdrawal and these Functions do not have to be OPERABLE. However, two [logarithmic] power level channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. This is addressed in LCO 3.3.13, "[Logarithmic] Power Monitoring Channels."

ACTIONS

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.

BASES

ACTIONS (continued)

A.1

Condition A applies if one Matrix Logic channel is inoperable or three Matrix Logic channels are inoperable due to a common power source failure de-energizing three matrix power supplies, in any applicable MODE. 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.

Failure of the matrix relays to de-energize in all three affected matrices could, when combined with trip channel bypassing of bistable relay contacts in the other matrices, result in loss of RPS function.

The channel must be restored to OPERABLE status within 48 hours. The Completion Time of 48 hours provides the operator time to take appropriate actions and still ensures 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 E is entered.

B.1

Condition B applies to one Initiation Logic channel, RTCB channel, or Manual Trip channel in MODES 1 and 2, since they have the same actions. MODES 3, 4, and 5, with the RTCBs shut, are addressed in Condition C. These Required Actions require opening the affected RTCBs. This removes the need for the affected channel by performing its associated safety function. With the 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.

Required Action B.1 provides for opening the RTCBs associated with the inoperable channel within a Completion Time of 1 hour. This Required Action is conservative, since depressing the Manual 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.

BASES

ACTIONS (continued)

C.1

Condition C applies to the failure of one Initiation Logic channel, RTCB channel, or Manual Trip channel affecting the same trip leg in MODE 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, the affected RTCBs must be opened. In some cases, this condition may effect all of the RTCBs. This removes the need for the affected channel by performing its associated safety function. With the RTCBs open, the affected functions are in a one-out-of-two logic, which meets redundancy requirements.

The Completion Time of 48 hours is consistent with that of other RPS instrumentation and should be adequate to repair most failures.

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.

D.1

Condition D applies to the failure of both Manual Trip or Initiation Logic channels affecting the same trip leg. Since this will open two channels of RTCBs, this Condition is also applicable to the two affected channels of 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 nontrip condition (e.g., due to two initiation K-relay failures). With only one Initiation Logic channel failed in a nontrip condition, there is still the redundant set of RTCBs in the trip leg. With both failed in a nontrip 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.

BASES

ACTIONS (continued)

If two Manual Trip channels are inoperable and affecting the same trip leg, the associated RTCBs must be opened immediately to ensure Manual Trip capability is maintained. With the affected RTCBs open, any one of two Manual Trip push buttons being depressed will result in a reactor trip.

If the affected RTCB(s) cannot be opened, Condition E is entered. This would only occur if there is a failure in the Manual Trip circuitry or the RTCB(s).

E.1 and E.2

Condition E is entered if Required Actions associated with Condition A, B, or D are not met within the required Completion Time or if for one or more Functions more than one Manual Trip, Matrix Logic, Initiation Logic, or RTCB channel is inoperable for reasons other than Condition A or D.

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. A Completion Time of 6 hours is reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems and to open RTCBs. All RTCBs should then be opened, placing the plant in a MODE where the LCO does not apply and ensuring no CEA withdrawal occurs.

SURVEILLANCE REQUIREMENTS

----------REVIEWER'S NOTE----------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit (Ref. 4).

SR 3.3.3.1

A CHANNEL FUNCTIONAL TEST is performed on each RTCB channel every 31 days. This verifies proper operation of each RTCB. The RTCB must then be closed prior to testing the other RTCBs, or a reactor trip may result. The Frequency of 31 days is based on the reliability analysis presented in Topical Report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," (Ref. 5).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.2

A CHANNEL FUNCTIONAL TEST on each RPS Logic channel is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 3. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. The first test, the bistable test, is addressed by SR 3.3.1.4 in LCO 3.3.1.

This SR addresses the two tests associated with the RPS Logic: Matrix Logic and Trip Path.

Matrix Logic Tests

These tests are performed one matrix at a time. They verify 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. The Matrix Logic tests 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 Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.3

A CHANNEL FUNCTIONAL TEST on the Manual Trip channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Manual Trip Function can be tested either at power or shutdown. However, the simplicity of this circuitry and the absence of drift concern makes this Frequency adequate. Additionally, operating experience has shown that these components usually pass the Surveillance when performed once within 7 days prior to each reactor startup.

[SR 3.3.3.4

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 every 18 months, a CHANNEL FUNCTIONAL TEST is performed that individually tests all four sets of undervoltage coils and all four sets of shunt trip coils. 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 Surveillance 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. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical

BASES

SURVEILLANCE REQUIREMENTS (continued)

Specifications tests at least once per refueling interval with applicable extensions. The 18 month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the Frequency of once every 18 months.

If one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance 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, 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.]

REFERENCES

1. 10 CFR 50, Appendix A.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. NRC Safety Evaluation Report, [Date].
5. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.3 Control Element Assembly Calculators (CEACs) (Digital)

BASES

BACKGROUND

The Reactor Protective System (RPS) initiates a reactor trip to protect against violating the core specified acceptable fuel design limits (SAFDLs) and breaching the reactor coolant pressure boundary (RCPB) during anticipated operational occurrences (AOOs). By tripping the reactor, the RPS also assists the Engineered Safety Features systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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 thresholds for protective system action to prevent exceeding acceptable limits during Design Basis Accidents.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) 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 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses the CEACs. LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," provides a description of this equipment in the RPS.

The excore nuclear instrumentation, the core protection calculators (CPCs), and the CEACs are considered components in the measurement channels of the Linear Power Level - High, Logarithmic Power Level - High, DNBR - Low, and Local Power Density (LPD) - High trips. The CEACs are addressed by this Specification.

All four CPCs receive control element assembly (CEA) deviation penalty factors from each CEAC and use the larger of the power factors from the two CEACs in the calculation of DNBR and LPD. CPCs are further described in the Background section of LCO 3.3.1.

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 cathode ray tube (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.

BASES

BACKGROUND (continued)

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. FSAR, Section [7.2] (Ref. 3), provides more detail on RPS testing. Process transmitter calibration is normally performed on a refueling basis.

APPLICABLE SAFETY ANALYSES

Each of the analyzed transients and accidents can be detected by one or more RPS 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 SAFDLs are approached. Each CPC also directly monitors one "target CEA" from each subgroup and uses this information to account for excessive radial peaking factors for events involving CEA groups out of sequence and subgroup deviations within a group, without the need for CEACs.

Therefore, although the CEACs do not provide a direct reactor trip Function, their input to the CPCs is taken credit for in the CEA misoperation analysis.

The CEACs satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

This 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 higher 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.

BASES

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 Engineered Safety Features Actuation System in providing acceptable consequences during accidents. 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 ensuring adequate SDM.

Because CEACs provide the inputs to the DNBR - Low and LPD - High trips, they are required to be OPERABLE in the same MODES as those trips for the same reasons.

ACTIONS

A.1 and A.2

Condition A applies to the failure of a single CEAC channel. There are only two CEACs, each providing CEA deviation input into all four CPC channels. The CEACs include complex diagnostic software, making it unlikely that a CEAC will fail without informing the CPCs of its failed status. With one failed CEAC, the CPC will receive CEA deviation penalty factors from the remaining OPERABLE CEAC. If the second CEAC should fail (Condition B), the CPC will use large preassigned penalty factors. The specific Required Actions allowed are as follows:

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 indication for display. Verification every 4 hours that each CEA is within 7 inches of the other CEAs in its group provides a check on the position of all CEAs and provides verification of the proper operation of the remaining CEAC. An OPERABLE CEAC will not generate penalty factors until deviations of > 7 inches within a subgroup 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 within this limited time frame.

As long as Required Action A.1 is accomplished as specified, the inoperable CEAC can be restored to OPERABLE status within 7 days. The Completion Time of 7 days is adequate for most repairs, while minimizing risk, considering that dropped CEAs are detectable by the redundant CEAC, and other LCOs specify Required Actions necessary to maintain DNBR and LPD margin.

BASES

ACTIONS (continued)

B.1, B.2, B.3, B.4, and B.5

Condition B applies if the Required Action and associated Completion Time of Required Action A are not met, or if both CEACs are inoperable. Actions associated with this Condition involve disabling the Control Element Drive Mechanism Control System (CEDMCS), 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 ensure 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 < 100% RTP if CPC generated reactor trips are to be avoided. The Completion Time of 4 hours is adequate to accomplish these actions while minimizing risks.

The Required Actions are as follows:

B.1

Meeting the DNBR margin requirements of LCO 3.2.5, "AXIAL SHAPE INDEX (ASI)," ensures that power level and ASI are within a conservative region of operation based on actual core conditions. In addition to the above actions, the Reactor Power Cutback (RPCB) System must be disabled. This ensures that CEA position will not be affected by RPCB operation.

B.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 group #6. This verification ensures that undesired perturbations in local fuel burnup are prevented.

B.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.

BASES

ACTIONS (continued)

B.4

The CEDMCS is placed and maintained in "OFF," except during CEA motion permitted by Required Action B.2, to prevent inadvertent motion and possible misalignment of the CEAs.

B.5

A comprehensive set of comparison checks on individual CEAs within groups must be made within 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.

C.1

Condition C applies if the CPC channel B or C 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.

If a CPC channel B or C cabinet high temperature alarm is received, it is possible for the CEAC to be affected and not be completely reliable. Therefore, a CHANNEL FUNCTIONAL TEST must be performed within 12 hours. The Completion Time of 12 hours is adequate, considering the low probability of undetected failure, the consequences of failure, and the time required to perform a CHANNEL FUNCTIONAL TEST.

D.1

Condition D applies if an OPERABLE CEAC has three or more autorestarts in a 12 hour period.

CPCs and CEACs will attempt to autorestart if they detect a fault condition such as a calculator malfunction or loss of power. A successful autorestart restores the calculator to operation; however, excessive autorestarts might be indicative of a calculator problem.

BASES

ACTIONS (continued)

If a nonbypassed CEAC has three or more autorestarts, 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 Completion Time of 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 by CPC online diagnostics.

E.1

Condition E is entered when the Required Action and associated Completion Time of Condition B, C, or D 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, for reaching the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

----------REVIEWER'S NOTE----------
In order for a plant to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that plant (Ref. 4).

SR 3.3.3.1

Performance of the CHANNEL CHECK once every 12 hours ensures that gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. 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

The CEAC autorestart count is checked every 12 hours to monitor the CPC and CEAC for normal operation. If three or more autorestarts of a nonbypassed CPC occur within a 12 hour period, the CPC may not be completely reliable. Therefore, the Required Action of Condition D must be performed. The Frequency is based on operating experience that demonstrates the rarity of more than one channel failing within the same 12 hour interval.

SR 3.3.3.3

A CHANNEL FUNCTIONAL TEST on each CEAC channel is performed every 92 days to ensure the entire channel will perform its intended function when needed. The quarterly CHANNEL FUNCTIONAL TEST is performed using test software. The Frequency of 92 days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5). A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.4

SR 3.3.3.4 is the performance of a CHANNEL CALIBRATION every [18] months.

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [5].

The 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 and includes operating experience and consistency with the typical [18] month fuel cycle.

SR 3.3.3.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the CEACs. The CHANNEL FUNCTIONAL TEST shall include the injection of a signal as close to the sensors as practicable to verify OPERABILITY, including alarm and trip Functions. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The basis for the [18] month Frequency is that the CEACs perform a continuous self monitoring function that 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 do not occur in any given [18] month interval.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.3.6

The isolation characteristics of each CEAC CEA position isolation amplifier and each optical isolator for CEAC to CPC data transfer are verified once per refueling to ensure that a fault in a CEAC or a CPC channel will not render another CEAC or CPC channel inoperable. 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.

The Frequency is based on plant operating experience with regard to channel OPERABILITY, which demonstrates the failure of a channel in any [18] month interval is rare.

REFERENCES

1. 10 CFR 50.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. NRC Safety Evaluation Report, [Date].
5. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.4 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 and the Reactor Coolant System (RCS) pressure boundary and to mitigate accidents.

The ESFAS contains devices and circuitry that 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 actuation systems is segmented into four sensor subsystems and two actuation subsystems. Each sensor subsystem includes measurement channels and bistables. The actuation subsystems include two logic subsystems for sequentially loading the diesel generators.

Each of the four sensor subsystem channels monitors redundant and independent process measurement channels. Each sensor is monitored by at least one bistable. The bistable associated with each ESFAS Function will trip when the monitored variable exceeds the trip setpoint. When tripped, the sensor subsystems provide outputs to the two actuation subsystems.

BASES

BACKGROUND (continued)

The two independent actuation subsystems compare the four sensor subsystem outputs. 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 will initiate one train of ESFAS. Each train can provide protection to the public in the case of a Design Basis Event. Actuation Logic is addressed in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip."

Each of the four sensor subsystems is mounted in a separate cabinet, excluding the sensors and field wiring.

The role of the sensor subsystem (measurement channels and bistables) is discussed below; actuation subsystems are discussed in LCO 3.3.5.

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 Protective 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. 2). 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.

BASES

BACKGROUND (continued)

In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated, and approved by the NRC staff. Plants not currently licensed as to credit four channel independence that may desire this capability must have approval of the NRC staff documented by an NRC Safety Evaluation Report (Ref. 3). 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 not demonstrating four channel independence may operate in a two-out-of-three logic configuration for 48 hours.

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 Standard 79-1971 (Ref. 4).

Bistable Trip Units

Bistable trip units receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Actuation Logic. They also provide local trip indication and remote annunciation.

There are four channels of bistables, designated A through D, for each ESF 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 CSAS, CIAS, and SIAS and a Pressurizer Pressure - Low input to the RPS and SIAS), the same bistable may be used to satisfy both Functions.

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 that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), Allowable Values specified in Table 3.3.4-1, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. A detailed description of the method used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). The actual nominal trip

BASES

BACKGROUND (continued)

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 ensure that Safety Limits of Chapter 2.0, "SAFETY LIMITS (SLs)," are not violated during anticipated operational occurrences (AOOs) and that 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.

ESFAS 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 disabling one channel input to the logic. 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 on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. At some plants 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.

ESFAS Logic is addressed in LCO 3.3.5.

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, serve as backups to Functions and are part of the NRC approved licensing basis for the plant.

ESFAS protective Functions are as follows:

BASES

APPLICABLE SAFETY ANALYSES (continued)

1. Safety Injection Actuation Signal

The SIAS ensures acceptable consequences during loss of coolant accident (LOCA) events, including steam generator tube rupture, 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 several other Functions, such as starting the emergency diesel generators.

2. Containment Spray Actuation Signal

The CSAS initiates containment spray, preventing containment overpressurization during a LOCA or MSLB. At some plants, both a high containment pressure signal and an SIAS have to actuate to provide the required protection. 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 LOCAs and MSLBs or FWLBs (inside containment). To provide protection, a high containment pressure signal will initiate CIAS at the same setpoint at which an SIAS is generated.

4. Main Steam Isolation Signal

The MSIS ensures acceptable consequences during an MSLB or FWLB by isolating both steam generators if either generator indicates a low steam generator 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.

BASES

APPLICABLE SAFETY ANALYSES (continued)

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 the 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. An RWT Level - Low signal initiates the RAS.

6. Auxiliary Feedwater Actuation Signal

An AFAS initiates feedwater flow to both steam generators if a low level is indicated in either steam generator, unless the generator is ruptured.

The AFAS maintains a steam generator heat sink during the following events:

- MSLB,
- FWLB,
- Inadvertent opening of a steam generator atmospheric dump valve, and
- Loss of feedwater.

A low steam generator water level signal will initiate auxiliary feed to the affected steam generator.

Secondary steam generator (SG) differential pressure (SG-A > SG-B) or (SG-B > SG-A) 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 MSLBs and FWLBs. This prevents containment overpressurization during these events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE.

The Bases for the LCO on ESFAS Functions are:

1. Safety Injection Actuation Signal

   a. Containment Pressure - High

      This LCO requires four channels of SIAS Containment Pressure - High to be OPERABLE in MODES 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 is not indicative of an offnormal condition. The setting is low enough to initiate the ESF Functions when an offnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

   b. Pressurizer Pressure - Low

      This LCO requires four channels of SIAS Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

      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 annunciated in the control room. This allows for a controlled depressurization of 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.

      This LCO requires four channels of the bypass permissive removal for SIAS Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

BASES

LCO (continued)

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 LCO 3.3.5.

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.

The block permissive is set low enough so as not to be enabled during normal plant operation, but high enough to allow blocking prior to reaching the trip setpoint.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. At many plants, it is also necessary to have an automatic or manual SIAS for complete actuation. 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 setpoint used in the SIAS is the same setpoint used in the CSAS. At many plants, 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.

a. Containment Pressure - High

This LCO requires four channels of CSAS Containment Pressure - High to be OPERABLE in MODES 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 is not indicative of an offnormal condition. The setting is low enough to initiate the ESF Functions when an offnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

BASES

LCO (continued)

The Containment Pressure - High setpoint is the same in the SIAS (Function 1), CSAS (Function 2), and CIAS (Function 3). However, different sensors and logic are used in each of these Functions.

3. Containment Isolation Actuation Signal

a. Containment Pressure - High

This LCO requires four channels of CIAS Containment Pressure - High to be OPERABLE in MODES 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 is not indicative of an offnormal condition. The setting is low enough to initiate the ESF Functions when an offnormal 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 CIAS (Function 3). However, different sensors and logic are used in each of these Functions.

b. Containment Radiation - High

This LCO requires four channels of CIAS Containment Radiation - High to be OPERABLE in MODES 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.

4. Main Steam Isolation Signal

The MSIS is required to be OPERABLE in MODES 1, 2, and 3 except when all associated valves are closed and de-activated.

BASES

LCO (continued)

a. Steam Generator Pressure - Low

This LCO requires four channels of MSIS Steam Generator Pressure - Low for each steam generator to be OPERABLE in MODES 1, 2, and 3.

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 steam generator pressure is reduced during controlled plant cooldowns. The block is permitted below 785 psia, and 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 steam generator 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.

This LCO requires four channels per steam generator of the bypass removal for MSIS Steam Generator Pressure - Low to be OPERABLE in MODES 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 LCO 3.3.5.

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.

The block permissive is set low enough so as not to be enabled during normal plant operation, but high enough to allow blocking prior to reaching the trip setpoint.

BASES

LCO (continued)

5. Recirculation Actuation Signal

a. Refueling Water Tank Level - Low

This LCO requires four channels of RWT Level - Low to be OPERABLE in MODES 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 injection. Premature recirculation could also damage or disable the recirculation system if recirculation begins before the sump has enough water to prevent air containment 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.

6. Auxiliary Feedwater Actuation Signal

The AFAS logic actuates auxiliary feedwater (AFW) to a steam generator 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 steam generators. The AFAS also monitors the secondary differential pressure in both steam generators and initiates an AFAS block signal to a ruptured generator, if the pressure in that generator is lower than that in the other generator by the differential pressure setpoint.

a. Steam Generator A/B Level - Low

This LCO requires four channels for each steam generator of Steam Generator Level - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value ensures adequate time exists to initiate AFW while the steam generators can function as a heat sink.

BASES

LCO (continued)

b. Steam Generator Pressure Difference - High (SG-A > SG-B) or (SG-B > SG-A)

This LCO requires four channels per steam generator of Steam Generator Pressure Difference - High to be OPERABLE in MODES 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 steam generator channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured steam generator in the event of an MSLB or FWLB, while permitting the feeding of the intact steam generator.

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:

- Close the main steam isolation valves to preclude a positive reactivity addition,
- Actuate AFW to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- 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
- 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, as addressed by LCO 3.3.5. In LCO 3.3.5, manual 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 Trip push buttons. Manual Trip of AFAS is not required in MODE 4 because AFW or shutdown cooling will already be in operation in this MODE.

BASES

APPLICABILITY (continued)

The ESFAS Actuation Logic must be OPERABLE in the same MODES as the automatic and Manual Trip. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip 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.

ACTIONS

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 performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification. If the actual trip setpoint is not within the Allowable Value in Table 3.3.4-1, the channel is inoperable and the appropriate Condition(s) are entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value in Table 3.3.4-1, or the sensor, 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 plant 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.

A Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function in Table 3.3.4-1. Completion Times for the inoperable channel of a Function will be tracked separately.

BASES

ACTIONS (continued)

[A.1

Condition A 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.]

[For those plants in which the SIAS is required for a complete CSAS actuation, Condition B for one ESFAS channel inoperable and Condition C for two ESFAS channels inoperable may be preferable to Condition A.

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.]

B.1, B.2.1, and B.2.2

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

3. Containment Isolation Actuation Signal
   Containment Pressure - High
   Containment Radiation - High

4. Main Steam Isolation Signal
   Steam Generator Pressure - Low

5. Recirculation Actuation Signal
   Refueling Water Tank Level - Low

6. Auxiliary Feedwater Actuation Signal
   Steam Generator Level - Low
   Steam Generator Pressure Difference - High

BASES

ACTIONS (continued)

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.

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 1 hour (Required Action B.1). With one channel in bypass, no additional random failure of a single channel could spuriously trip the reactor and a valid trip signal can still trip the reactor. With one channel in trip, an additional random failure of a single channel could spuriously trip the reactor. Therefore, it is preferable to place an inoperable channel in bypass rather than trip.

The Completion Time of 1 hour allotted to 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.

One failed channel is restored to OPERABLE status or is placed in trip within [48] hours (Required Action B.2.1 or B.2.2). Required Action B.2.1 restores the full capability of the function. Required Action B.2.2 places the function in 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 operating experience, which has demonstrated that a random failure of a second channel occurring during the [48] hour period is a low probability event.

C.1 and C.2

Condition C applies to the failure of two channels in any of the following ESFAS functions:

1. Safety Injection Actuation Signal
   Containment Pressure - High
   Pressurizer Pressure - Low

3. Containment Isolation Actuation Signal
   Containment Pressure - High
   Containment Radiation - High

4. Main Steam Isolation Signal
   Steam Generator Pressure - Low

BASES

ACTIONS (continued)

5. Recirculation Actuation Signal
   Refueling Water Tank Level - Low

6. Auxiliary Feedwater Actuation Signal
   Steam Generator Level - Low
   Steam Generator Pressure Difference - High

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.

One of the failed channels 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 status, 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 must be placed in trip if more than [48] hours has elapsed since the initial channel failure.

D.1, D.2.1, D.2.2.1, and D.2.2.2

Condition D applies to the failure of one 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 LCO 3.3.5.

In Condition D, it is permissible to continue operation with one bypass permissive removal channel failed, providing the bypass is disabled (Required Action D.1). 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.

BASES

ACTIONS (continued)

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.2.1, Required Action D.2.2.1, and Required Action D.2.2.2 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 bases as discussed for Condition B.

E.1, E.2.1, and E.2.2

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 nonconservative 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 LCO 3.3.5.

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.2.1 and Required Action E.2.2 are equivalent to the Required Actions for a two automatic trip channel failure (Condition C). Also similar to Condition C, after one set of inoperable channels is 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 bases as discussed for Condition C.

BASES

ACTIONS (continued)

F.1 and F.2

If the Required Actions and associated Completion Times of Condition A, B, C, D, or E are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

The SRs for any particular ESFAS Function are found in the SRs column of Table 3.3.4-1 for that Function. Most functions are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing.

----------REVIEWER'S NOTE----------
In order for a unit to take credit for topical reports as the basis for justifying Frequencies, topical reports should be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit.

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 normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. 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 of 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 indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during

BASES

SURVEILLANCE REQUIREMENTS (continued)

times when Surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Offscale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency of about once every shift is based on operating experience that demonstrates channel failure is rare. 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 3.3.4.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST tests the individual sensor subsystems using an analog test input to each bistable.

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [8].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.4.3

SR 3.3.4.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.4.2, except 3.3.4.3 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 Steam Generator Pressure - Low bypass. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass removal Functions 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 Surveillance within 92 days of startup is based upon the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 9).

SR 3.3.4.4

CHANNEL CALIBRATION is a complete check of the instrument channel, including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the extension analysis. The requirements for this review are outlined in Reference [8].

BASES

SURVEILLANCE REQUIREMENTS (continued)

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.4.5

This Surveillance ensures that the train actuation response times 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). Response time testing acceptance criteria are included in Reference 3. The test may be performed in one measurement or in overlapping segments, with verification that all components are measured.

----------REVIEWER'S NOTE----------

Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 10) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

BASES

SURVEILLANCE REQUIREMENTS (continued)

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every [18] months. 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. Surveillance 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.

REFERENCES

1. FSAR, Section [7.3].
2. 10 CFR 50, Appendix A.
3. NRC Safety Evaluation Report, [Date].
4. IEEE Standard 279-1971.
5. FSAR, Chapter [14].
6. 10 CFR 50.49.
7. "Plant Protection System Selection of Trip Setpoint Values."
8. FSAR, Section [7.2].
9. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.
10. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

B 3.3 INSTRUMENTATION

B 3.3.4 Reactor Protective System (RPS) Logic and Trip Initiation (Digital)

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). By tripping the reactor, the RPS also assists the Engineered Safety Features (ESF) systems in mitigating accidents.

The protection and monitoring systems have been designed to ensure 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.

During AOOs, which are those events expected to occur one or more times during the plant life, the acceptable limits are:

- The departure from nucleate boiling ratio shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,
- Fuel centerline melting shall not occur, and
- The Reactor Coolant System pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 1) and 10 CFR 100 (Ref. 2) 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 (Ref. 2) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event.

BASES

BACKGROUND (continued)

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and
- Reactor trip circuit breakers (RTCBs).

This LCO addresses the RPS Logic and RTCBs, including Manual Trip capability. LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating," provides a description of the role of this equipment in the RPS. This is summarized below:

RPS 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.

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 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.

BASES

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 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, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

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 on 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.

BASES

BACKGROUND (continued)

Reactor Trip Circuit Breakers (RTCBs)

The reactor trip switchgear 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.

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 half of the control element assemblies (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 Trip push button or an RPS actuated K-relay. There are four Manual Trip push buttons, arranged in two sets of two. Depressing both push buttons in either set will result in a reactor trip.

When a Manual 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 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 the individual sets of RTCBs, can be performed either at power or shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 3), explains RPS testing in more detail.

BASES

APPLICABLE SAFETY ANALYSES

Reactor Protective System (RPS) Logic

The RPS Logic provides for automatic trip initiation to maintain the SLs during AOOs and assist the ESF systems in ensuring acceptable consequences during accidents. All transients and accidents that call for a reactor trip assume the RPS Logic is functioning as designed.

Reactor Trip Circuit Breakers (RTCBs)

All of the transient and accident analyses that call for a reactor trip assume that the RTCBs operate and interrupt power to the CEDMs.

Manual Trip

There are no accident analyses that take credit for the Manual Trip; however, the Manual 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.

The RPS instrumentation satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

Reactor Protective System (RPS) Logic

The LCO on the RPS Logic channels ensures that each of the following requirements are met:

- A reactor trip will be initiated when necessary,
- The required protection system coincidence logic is maintained (minimum two-out-of-three, normal two-out-of-four), and
- Sufficient redundancy is maintained to permit a channel to be out of service for testing or maintenance.

Failures of individual bistable relays and their contacts are addressed in LCO 3.3.1. 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.

BASES

LCO (continued)

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.

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 Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance 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, 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.

1. 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 any RTCBs are closed and any CEA is capable of being withdrawn.

2. 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 any CEA is capable of being withdrawn.

BASES

LCO (continued)

3. 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 any CEA is capable of being withdrawn.

Each channel consists of two breakers operated in a single set by the Initiation Logic or Manual 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 that are actuated by the K-relay and the Manual Trip for each set of breakers. The K-relay actuated contacts and the upstream circuitry are considered to be RPS Logic. Manual Trip contacts and upstream circuitry are considered to be Manual Trip circuitry.

A Note associated with the ACTIONS states that if one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the affected set of RTCBs may be closed for up to 1 hour for Surveillance on the OPERABLE Initiation Logic, RTCB, and Manual Trip channels. In this case the redundant set of RTCBs will provide protection. 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.

4. Manual Trip

The LCO requires all four Manual Trip channels to be OPERABLE in MODES 1 and 2, and MODES 3, 4, and 5 when the RTCBs are closed and any CEA is capable of being withdrawn.

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.

BASES

LCO (continued)

Manual 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 be entered due to failure of a local Manual Trip.

APPLICABILITY

The RPS Logic, RTCBs, and Manual Trip are required to be OPERABLE in any MODE when the CEAs are capable of being withdrawn off the bottom of the core (i.e., RTCBs closed and power available to the CEDMs). This ensures that the reactor can be tripped when necessary, but allows for maintenance and testing when the reactor trip is not needed.

In MODES 3, 4, and 5 with the RTCBs open, the CEAs are not capable of withdrawal and these Functions do not have to be OPERABLE. However, two logarithmic power level channels must be OPERABLE to ensure proper indication of neutron population and to indicate a boron dilution event. This is addressed in LCO 3.3.13, "[Logarithmic] Power Monitoring Channels."

ACTIONS

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.

A.1

Condition A applies if one Matrix Logic channel is inoperable or three Matrix Logic channels are inoperable due to a common power source failure de-energizing three matrix power supplies in any applicable MODE. 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.

The channel must be restored to OPERABLE status within 48 hours. The Completion Time of 48 hours provides the operator time to take appropriate actions and still ensures 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 E is entered.

BASES

ACTIONS (continued)

B.1

Condition B applies to one Initiation Logic channel, RTCB channel, or Manual Trip channel in MODES 1 and 2, since they have the same actions. MODES 3, 4, and 5, with the RTCBs shut, are addressed in Condition C. These Required Actions require opening the affected RTCBs. This 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.

Required Action B.1 provides for opening the RTCBs associated with the inoperable channel within a Completion Time of 1 hour. This Required Action is conservative, since depressing the Manual 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 for opening the affected RTCBs while maintaining the risk of having them closed at an acceptable level.

C.1

Condition C applies to the failure of one Initiation Logic channel, RTCB channel, or Manual Trip channel affecting the same trip leg in MODE 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, the affected RTCBs must be opened. In some cases, this condition may effect all of the RTCBs. This removes the need for the affected channel by performing its associated safety function. With the RTCBs open, the affected functions are in a one-out-of-two logic, which meets redundancy requirements.

The Completion Time of 48 hours is consistent with that of other RPS instrumentation and should be adequate to repair most failures.

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.

BASES

ACTIONS (continued)

D.1

Condition D applies to the failure of both Manual Trip or Initiation Logic channels affecting the same trip leg. Since this will open two channels of RTCBs, this Condition is also applicable to 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 nontrip condition (e.g., due to two initiation K-relay failures). With only one Initiation Logic channel failed in a nontrip condition, there is still the redundant set of RTCBs in the trip leg. With both failed in a nontrip 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 two Manual Trip channels are inoperable and affecting the same trip leg, the associated RTCBs must be opened immediately to ensure Manual Trip capability is maintained. With the affected RTCBs open, any one of two Manual Trip push buttons being depressed will result in a reactor trip.

If the affected RTCB cannot be opened, Required Action E is entered. This would only occur if there is a failure in the Manual Trip circuitry or the RTCB(s).

E.1 and E.2

Condition E is entered if Required Actions associated with Condition A, B, or D are not met within the required Completion Time or, if for one or more Functions, more than one Manual Trip, Matrix Logic, Initiation Logic, or RTCB channel is inoperable for reasons other than Condition A or D.

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. A Completion Time of 6 hours is reasonable, based on operating experience, for reaching the required plant conditions from full power conditions in an orderly manner and without challenging plant systems and for opening RTCBs. All RTCBs should then be opened, placing the plant in a MODE where the LCO does not apply and ensuring no CEA withdrawal occurs.

BASES

SURVEILLANCE REQUIREMENTS

----------REVIEWER'S NOTE----------
In order for a unit to take credit for topical reports as the basis for justifying Frequencies, topical reports must be supported by an NRC staff Safety Evaluation Report that establishes the acceptability of each topical report for that unit (Ref. 4).

SR 3.3.4.1

A CHANNEL FUNCTIONAL TEST is performed on each RTCB channel every 31 days. This verifies proper operation of each RTCB. The RTCB must then be closed prior to testing the other RTCBs, or a reactor trip may result. The Frequency of 31 days is based on the reliability analysis presented in Topical Report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation," (Ref. 4).

SR 3.3.4.2

A CHANNEL FUNCTIONAL TEST on each RPS Logic channel is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

In addition to power supply tests, the RPS CHANNEL FUNCTIONAL TEST consists of three overlapping tests as described in Reference 3. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. The first test, the bistable test, is addressed by SR 3.3.1.7 in LCO 3.3.1.

This SR addresses the two tests associated with the RPS Logic: Matrix Logic and Trip Path.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Matrix Logic Tests

These tests are performed one matrix at a time. They verify 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. The Matrix Logic tests 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 Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 5).

Additionally, operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 7 days prior to each reactor startup.

SR 3.3.4.3

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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Therefore, once every [18] months, a CHANNEL FUNCTIONAL TEST is performed that individually tests all four sets of undervoltage coils and all four sets of shunt trip coils. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. During undervoltage coil testing, the shunt trip coils must remain de-energized, preventing their operation. Conversely, during shunt trip coil testing, the undervoltage coils must remain energized, preventing their operation. This Surveillance 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 is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at the Frequency of once every [18] months.

SR 3.3.4.4

A CHANNEL FUNCTIONAL TEST on the Manual Trip channels is performed prior to a reactor startup to ensure the entire channel will perform its intended function if required. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. The Manual Trip Function can only be tested at shutdown. However, the simplicity of this circuitry and the absence of drift concern make this Frequency adequate.

REFERENCES

1. 10 CFR 50, Appendix A.
2. 10 CFR 100.
3. FSAR, Section [7.2].
4. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.5 Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip (Analog)

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based upon the values of selected unit parameters, to protect against violating core design limits and the Reactor Coolant System (RCS) pressure boundary and to mitigate accidents.

The ESFAS contains devices and circuitry that 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 actuation systems is segmented into four sensor subsystems addressed by LCO 3.3.4, "Engineered Safety Features Actuation System (ESFAS) Instrumentation," and two actuation subsystems addressed by this LCO. Each sensor subsystem includes measurement channels and bistables. The SIAS actuation subsystems include two logic subsystems for sequentially loading the diesel generators.

Each of the four sensor subsystem channels monitors redundant and independent process measurement channels. Each sensor is monitored by at least one bistable. The bistable associated with each ESFAS Function will trip when the monitored variable exceeds the trip setpoint. When tripped, the sensor subsystems provide outputs to the two actuation subsystems.

BASES

BACKGROUND (continued)

The two independent actuation subsystems each compare the four associated sensor subsystem outputs. If a trip occurs in two or more sensor subsystem channels, the two-out-of-four logic in each actuation subsystem will initiate one train of ESFAS. Each has sufficient equipment to provide protection to the public in the case of a Design Basis Event. The sensor subsystem is addressed in LCO 3.3.4. This LCO addresses the actuation subsystem.

Each of the four sensor subsystems is mounted in a separate cabinet, excluding the sensors and field wiring.

The role of the sensor subsystem (measurement channels and bistables) is discussed in LCO 3.3.4. That of the actuation subsystem is discussed below.

ESFAS Logic

The two independent actuation subsystems compare the four sensor subsystem outputs. 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.

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) that 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 disabling one channel input to the logic. 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. Maintenance bypassing can be simultaneously performed on any number of parameters in any number of channels, providing each parameter is bypassed in only one channel at a time. At some plants an interlock prevents simultaneous maintenance bypassing of the same parameter in more than one channel. Maintenance bypassing is normally employed during maintenance or testing.

BASES

BACKGROUND (continued)

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 that ESFAS actuation would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent actuation caused by any single channel failure in a trip condition.

In addition to the maintenance bypasses, there are operating bypasses (blocks) on the Pressurizer Pressure - Low input to the SIAS and on the Steam Generator 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 steam generator pressure (for the 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 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 Engineered Safety Features (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:

BASES

BACKGROUND (*continued*)

- 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 (MSIVs),
- 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 secondary, or backup, actuation signal for one or more other accidents. Functions such as Manual Initiation, not specifically credited in the accident analysis, serve as backups to Functions and are part of the NRC staff approved licensing basis for the plant.

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, 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) and performs several other Functions, such as initiating control room isolation and starting the diesel generators.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Spray Actuation Signal

The CSAS initiates containment spray, preventing containment overpressurization during a LOCA or MSLB. At some plants, both a high containment pressure signal and an SIAS have to actuate to provide the required protection. 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 LOCAs and MSLBs or FWLBs (inside containment). To provide protection, a high containment pressure signal will initiate CIAS at the same setpoint at which an SIAS is initiated.

4. Main Steam Isolation Signal

The MSIS ensures acceptable consequences during an MSLB or FWLB by isolating both steam generators if either generator indicates a low steam generator 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. An RWT Level - Low signal initiates the RAS.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6. Auxiliary Feedwater Actuation Signal

An AFAS initiates feedwater flow to both steam generators if a low level is indicated in either steam generator, unless the generator is ruptured.

The AFAS maintains a steam generator heat sink during the following events:

- MSLB,
- FWLB,
- Inadvertent opening of a steam generator atmospheric dump valve, and
- Loss of feedwater.

A low steam generator water level signal will initiate auxiliary feed to the affected steam generator.

Secondary steam generator (SG) differential pressure (SG-A > SG-B) or (SG-B > SG-A) 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 MSLBs and FWLBs. This prevents containment overpressurization during these events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires that all components necessary to provide an ESFAS actuation be OPERABLE.

Actions allow maintenance bypass of individual channels. Plants are restricted to 48 hours in a maintenance 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).

The Bases for the LCO on ESFAS automatic actuation Functions are addressed in the Bases for LCO 3.3.4. Those associated with the Manual Trip or Actuation Logic are addressed below.

BASES

LCO (continued)

1. Safety Injection Actuation Signal

   a. Manual Trip

      This LCO requires two channels of SIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Actuation Logic

      This LCO requires two channels of SIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

      Failures in the actuation subsystems, including the manual bypass key switches, are Actuation Logic failures and are addressed in this LCO.

      Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

2. Containment Spray Actuation Signal

   CSAS is initiated either manually or automatically. At many plants it is also necessary to have an automatic or manual SIAS for a complete actuation. 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.

   a. Manual Trip

      This LCO requires two channels of CSAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Actuation Logic

      This LCO requires two channels of CSAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

      Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

BASES

LCO (continued)

3. Containment Isolation Actuation Signal

   a. Manual Trip

      This LCO requires two channels of CIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Actuation Logic

      This LCO requires two channels of Actuation Logic for CIAS to be OPERABLE in MODES 1, 2, 3, and 4.

      Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

4. Main Steam Isolation Signal

   a. Manual Trip

      This LCO requires two channels per steam generator of the MSIS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Actuation Logic

      This LCO requires two channels of MSIS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

      Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in the logic LCO.

5. Recirculation Actuation Signal

   a. Manual Trip

      This LCO requires two channels of RAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Actuation Logic

      This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

LCO (continued)

6. Auxiliary Feedwater Actuation Signal

A low level in either generator, as sensed by a two-out-of-four coincidence of four wide range sensors for each generator, will generate an auxiliary feedwater actuation signal (AFAS), which starts both trains of auxiliary feedwater (AFW) pumps and feeds both steam generators. The AFAS also monitors the secondary differential pressure in both steam generators 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.

a. Manual Trip

This LCO requires two channels of AFAS Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Actuation Logic

This LCO requires two channels of AFAS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

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:

- Close the MSIVs to preclude a positive reactivity addition,
- Actuate AFW to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- 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
- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

BASES

APPLICABILITY (continued)

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 Trip 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 Trip push buttons. Manual Trip of AFAS is not required in MODE 4 because AFW or shutdown cooling will already be in operation in this MODE.

The ESFAS Actuation Logic must be OPERABLE in the same MODES as the Automatic and Manual Trips. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip 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.

ACTIONS

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.

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function in Table 3.3.5-1 in the LCO. Completion Times for the inoperable channel of a Function will be tracked separately.

A.1

Condition A applies to one AFAS Manual Trip or AFAS Actuation Logic channel inoperable. It is identical to Condition C for the other ESFAS Functions, except for the shutdown track imposed by Condition D.

The channel must be restored to OPERABLE status to restore redundancy of the AFAS Function. The 48 hour Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

BASES

ACTIONS (continued)

B.1 and B.2

If two Manual Trip or Actuation Logic channels are inoperable or the Required Action and associated Completion Time of Condition A cannot be met, the reactor should be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

C.1

Condition C applies to one Manual Trip or Actuation Logic channel inoperable for those ESFAS Functions that must be OPERABLE in MODES 1, 2, 3, and 4 (all Functions except AFAS). The shutdown track imposed by Condition D 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 48 hour Completion Time is commensurate with the importance of avoiding the vulnerability of a single failure in the only remaining OPERABLE channel.

D.1 and D.2

Condition D is entered when one or more Functions have two Manual Trip or Actuation Logic channels inoperable except AFAS or the Required Action and associated Completion Time of Condition C are not met. If Required Action C.1 cannot be met within the required Completion Time, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

BASES

SURVEILLANCE REQUIREMENTS

SR 3.3.5.1

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed. Sensor subsystem tests are addressed in LCO 3.3.4. This SR addresses Actuation Logic tests. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

Actuation Logic Tests

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 requires that Actuation Logic tests include operation of initiation relays. Note 2 allows deferred at power testing of certain relays to allow for the fact that operating certain relays during power operation could cause plant transients or equipment damage. Those initiation relays that cannot be tested at power must be tested in accordance with Note 2. These include [SIAS No. 5, 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

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.

The Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 2).

SR 3.3.5.2

A CHANNEL FUNCTIONAL TEST is performed on the manual ESFAS actuation circuitry, de-energizing relays and providing Manual Trip of the Function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This Surveillance 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 Trip of the Function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

REFERENCES

1. FSAR, Section [7.3].

2. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.

B 3.3 INSTRUMENTATION

B 3.3.5 Engineered Safety Features Actuation System (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 the Reactor Coolant System (RCS) pressure boundary during anticipated operational occurrences (AOOs) and ensures acceptable consequences during accidents.

The ESFAS contains devices and circuitry that generate the following signals when monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS), Containment Cooling Actuation Signal (CCAS) (actuated by an automatic 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, 7. Emergency Feedwater Actuation Signal (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,
- Bistable trip units, and
- ESFAS Logic:
  - Matrix Logic,
  - Initiation Logic (trip paths), and
  - Actuation Logic.

BASES

BACKGROUND (continued)

This LCO addresses measurement channels and bistables. Logic is addressed in LCO 3.3.6, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip."

The role of each of these modules in the ESFAS, including the logic of LCO 3.3.6, 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 Protective 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. 2). 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.

BASES

BACKGROUND (continued)

---REVIEWER'S NOTE---

In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated and approved by the NRC staff. Plants not currently licensed to credit four channel independence that may desire this capability must have approval of the NRC staff, documented by an NRC Safety Evaluation Report (Ref. 3). 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 may operate in two-out-of-three logic configuration, with one channel removed from service, until following the next MODE 5 entry. Plants not demonstrating four channel independence can only operate for 48 hours with one channel inoperable (Ref. 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 IEEE Standard 279-1971 (Ref. 4).

Bistable Trip Units

Bistable trip units, mounted in the Plant Protection 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 for each ESFAS Function. 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).

BASES

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 that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), Allowable Values specified in Table 3.3.5-1, in the accompanying LCO, 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. 7). 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. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

Setpoints in accordance with the Allowable Value will ensure that Safety Limits of LCO Section 2.0, "Safety Limits," are not violated during 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.

Functional testing of the ESFAS, from the bistable input through the opening of initiation relay contacts in the ESFAS Actuation Logic, can be performed either at power or at shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 8), provides more detail on ESFAS testing. Process transmitter calibration is normally performed on a refueling basis. SRs for the channels are specified in the Surveillance Requirements section.

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 sense the same input parameter trip. This is called a two-out-of-four trip logic.

BASES

BACKGROUND (continued)

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 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.

Each of the two channels of Actuation Logic, mounted in the Auxiliary Relay Cabinet (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 RTCBs. This logic controls ARC mounted subgroup relays, which are normally energized. Contacts from these relays, when de-energized, actuate specific ESF equipment.

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.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

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 ARCs used to actuate the ESF Function, excluding the subgroup relays, and interconnecting wiring to the initiation relay contacts mounted in the PPS cabinet.

BASES

BACKGROUND (continued)

The subgroup relays are actuated by the ESFAS logic. Each ESFAS Function typically employs several subgroup relays, with each subgroup relay responsible for actuating one or more components in the ESFAS Function. Subgroup relays and their contacts are considered part of the actuated equipment and are addressed under the applicable LCO for this equipment. Initiation and Actuation Logic up to the subgroup relays is addressed in LCO 3.3.6.

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 on 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.

----------REVIEWER'S NOTE----------

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.

BASES

BACKGROUND (continued)

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 Trip push button opens one trip path, de-energizing one set of two initiation relays, 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 ensure that Manual Trip will not be prevented in the event of a single random failure. Each set of two push buttons is designated a single channel in LCO 3.3.6.

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 the secondary, or backup, actuation signal for one or more other accidents.

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 (ECCS) and performs several other functions such as initiating a containment cooling actuation, initiating control room isolation, and starting the diesel generators.

   CCAS mitigates containment overpressurization when required by either a manual CCAS actuation or an automatic SIAS Function. This Function is not employed by all plants.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Spray Actuation Signal

CSAS actuates containment spray, preventing containment overpressurization during large break LOCAs, small break LOCAs, and MSLBs or feedwater line breaks (FWLBs) inside containment. CSAS is initiated by 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. Main Steam Isolation Signal

MSIS ensures acceptable consequences during an MSLB or FWLB (between the steam generator and the main feedwater check valve), either inside or outside containment. MSIS isolates both steam generators 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.

5. 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 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. An RWST Level - Low signal initiates the RAS.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6, 7. Emergency Feedwater Actuation Signal

EFAS consists of two steam generator (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 a steam generator heat sink during a steam generator tube rupture event and an MSLB or FWLB event either inside or outside containment.

Low steam generator water level initiates emergency feed to the affected steam generator, providing the generator is not identified (by the circuitry) as faulted (a steam or FWLB).

EFAS logic includes steam generator specific inputs from the Steam Generator Pressure - Low bistable comparator (also used in MSIS) and the SG Pressure Difference - High (SG #1 > SG #2 or SG #2 > SG #1, 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 steam generator, even if both are below the MSIS setpoint, while preventing the ruptured generator from being fed. Not feeding a ruptured generator prevents containment overpressurization during the analyzed events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE.

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).

The Bases for the LCOs on ESFAS Functions are:

BASES

LCO (continued)

1. Safety Injection Actuation Signal

a. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

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 is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

b. Pressurizer Pressure - Low

This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1 and 2.

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 accident.

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.

BASES

LCO (continued)

When the trip setpoint has been lowered below the bypass permissive setpoint of 400 psia, the 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.

Bypass Removal

This LCO requires four channels of bypass removal for 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, 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 SDM.

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 before the Containment Pressure - High High. This ensures that a CSAS will not initiate unless required.

a. Containment Pressure - High High

This LCO requires four channels of Containment Pressure - High High to be OPERABLE in MODES 1, 2, and 3.

BASES

LCO (continued)

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.

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 and are addressed in LCO 3.3.6. Since their Applicability is also the same, they have identical Required Actions.

a. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

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 is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

b. Pressurizer Pressure - Low

This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

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 accident, the ESF systems will actuate to perform as expected, mitigating the consequences of the accidents.

BASES

LCO (continued)

The Pressurizer Pressure - Low trip setpoint, which provides an SIAS, CIAS, 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 safety 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 preparation for shutdown cooling. When RCS pressure rises above the bypass removal, the bypass is removed.

Bypass Removal

This LCO requires four channels of bypass removal for 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.

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 SDM.

BASES

LCO (continued)

4. Main Steam Isolation Signal

The LCO is applicable to the MSIS in MODES 1, 2, and 3 except when all associated valves are closed and de-activated.

a. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low to be OPERABLE in MODES 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 4) 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. An RPS trip on Steam Generator Pressure - Low is initiated simultaneously, using the same bistable. The Steam Generator Pressure - Low bistable output is also used in the EFAS logic (Function 7) to aid in determining if a steam generator is intact.

The Steam Generator Pressure - Low trip setpoint may be manually decreased as steam generator 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.

b. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3. The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

BASES

LCO (continued)

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 is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

5. Recirculation Actuation Signal

a. Refueling Water Storage Tank Level - Low

This LCO requires four channels of RWST Level - Low to be OPERABLE in MODES 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 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.

6, 7 Emergency Feedwater Actuation Signal SG #1 and SG #2 (EFAS-1 and EFAS-2)

EFAS-1 is initiated to SG #1 by either a low steam generator level coincident with no low pressure trip present on SG #1 or by a low steam generator 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.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS logic where it is used to determine if a generator is intact. The EFAS logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is less than the pressure in the other steam generator by the Steam Generator Pressure Difference (SGPD) - High setpoint.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

The following LCO description applies to both EFAS signals.

a. Steam Generator Level - Low

This LCO requires four channels of Steam Generator Level - Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Steam Generator Level - Low EFAS input is derived from the Steam Generator 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 steam generator at reactor trip. Thus, EFAS is initiated well before steam generator inventory is challenged.

b. SG Pressure Difference - High (SG #1 > SG #2) or (SG #2 > SG #1)

This LCO requires four channels of SG Pressure Difference - High to be OPERABLE for each EFAS in MODES 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 steam generator channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured steam generator in the event of an MSLB or FWLB, while permitting the feeding of the intact steam generator.

BASES

LCO (continued)

c. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Steam Generator Pressure - Low input is derived from the Steam Generator Pressure - Low RPS bistable output. This output is also used as an MSIS input.

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 4) during an excessive steam demand event. An excessive steam demand is one indicator of a potentially ruptured steam generator; thus, this EFAS input, in conjunction with the SGPD Function, prevents the feeding of a potentially ruptured steam generator.

The Steam Generator Pressure - Low trip setpoint may be manually decreased as steam generator 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.

APPLICABILITY In MODES 1, 2 and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

- Close the main steam isolation valves to preclude a positive reactivity addition,
- Actuate emergency feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- 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
- Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

BASES

APPLICABILITY (continued)

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, as addressed by LCO 3.3.6.

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

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. 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.

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 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 any related Condition 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.

A Note has been added to the ACTIONS. The Note has been added to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time for the inoperable channel of a Function will be tracked separately for each Function starting from the time the Condition was entered for that Function.

A.1 and A.2

Condition A 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

BASES

ACTIONS (continued)

2. Containment Spray Actuation Signal Containment Pressure - High High Automatic SIAS

3. Containment Isolation Actuation Signal Containment Pressure - High Pressurizer Pressure - Low

4. Main Steam Isolation Signal Steam Generator Pressure - Low Containment Pressure - High

5. Recirculation Actuation Signal Refueling Water Storage Tank Level - Low

6. Emergency Feedwater Actuation Signal SG #1 (EFAS-1) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

7. Emergency Feedwater Actuation Signal SG #2 (EFAS-2) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

ESFAS coincidence logic is normally two-out-of-four.

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 1 hour (Required Action A.1).

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.

The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel bypassed, the coincidence logic is now in a two-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip. The Completion Time of prior to entering MODE 2 following the next MODE 5 entry is based on adequate channel to channel independence, which allows a two-out-of-three channel operation, since no single failure will cause or prevent a reactor trip.

BASES

ACTIONS (continued)

B.1

Condition B applies to the failure of two channels of one or more input parameters in the following ESFAS automatic trip 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. Main Steam Isolation Signal Steam Generator Pressure - Low Containment Pressure - High
5. Recirculation Actuation Signal Refueling Water Storage Tank Level - Low
6. Emergency Feedwater Actuation Signal SG #1 (EFAS-1) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low
7. Emergency Feedwater Actuation Signal SG #2 (EFAS-2) Steam Generator Level - Low SG Pressure Difference - High Steam Generator Pressure - Low

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.

BASES

ACTIONS (continued)

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one ESFAS channel, and placing a second channel in trip will result in an ESFAS actuation. Therefore, if one ESFAS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic bypass removal channel inoperable. The only automatic bypass removal on an ESFAS is on the Pressurizer Pressure - Low signal. This bypass removal is shared with the RPS Pressurizer Pressure - Low bypass removal.

If the bypass removal channel for any operating bypass cannot be restored to OPERABLE status, the associated ESFAS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected ESFAS channel must be declared inoperable, as in Condition A, and the bypass either removed or the bypass removal channel repaired. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

D.1 and D.2

Otherwise, the affected ESFAS channels must be declared inoperable, as in Condition B, and either the bypass removed or the bypass removal channel repaired. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST or the plant must shut down per LCO 3.0.3, as explained in Condition B. Completion Times are consistent with Condition B.

BASES

ACTIONS (continued)

E.1 and E.2

If the Required Actions and associated Completion Times of Condition A, B, C, or D cannot be met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.5.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. 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 of 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 indication and readability. If a channel is outside the criteria, it may be an indication that the sensor or the signal processing equipment has drifted outside its limit. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency, about once every shift, is based on operating experience that demonstrates channel failure is rare. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.2

A CHANNEL FUNCTIONAL TEST is performed every 92 days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SR 3.3.5.2, SR 3.3.6.1, and SR 3.3.6.2, 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 3.3.5.2 and SR 3.3.6.1 are normally performed together and in conjunction with ESFAS testing. SR 3.3.6.2 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. SRs 3.3.6.1 and 3.3.6.2 are addressed in LCO 3.3.6. SR 3.3.5.2 includes bistable tests.

A test signal is 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 trip channel bypassed. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [9].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the detector and the bypass removal functions. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive surveillances. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [9].

The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

SR 3.3.5.4

This Surveillance ensures that the train actuation response times are within the maximum values assumed in the safety analyses.

Response time testing acceptance criteria are included in Reference 10.

----------REVIEWER'S NOTE----------
Applicable portions of the following TS Bases are applicable to plants adopting CEOG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A,

BASES

SURVEILLANCE REQUIREMENTS (continued)

"Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every [18] months. The [18] month Frequency is consistent with the typical industry refueling cycle and 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.

SR 3.3.5.5

SR 3.3.5.5 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.5.2, except SR 3.3.5.5 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 3.3.1.13. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

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 3.3.5.2.

The allowance to conduct this test with 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 9).

BASES

REFERENCES

1. FSAR, Section [7.3].
2. 10 CFR 50, Appendix A.
3. NRC Safety Evaluation Report.
4. IEEE Standard 279-1971.
5. FSAR, Chapter [15].
6. 10 CFR 50.49.
7. "Plant Protection System Selection of Trip Setpoint Values."
8. FSAR, Section [7.2].
9. CEN-327, May 1986, including Supplement 1, March 1989.
10. Response Time Testing Acceptance Criteria.
11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."

B 3.3 INSTRUMENTATION

B 3.3.6 Diesel Generator (DG) - Loss of Voltage Start (LOVS) (Analog)

BASES

BACKGROUND

The DGs 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 4.16 kV vital bus.

Four undervoltage relays with inverse time characteristics are provided on each 4.16 kV 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.

Trip Setpoints and Allowable Values

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 3.3.6.3 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 trip acceptance criteria, the undervoltage relay is considered OPERABLE.

Setpoints in accordance with the Allowable Values will ensure that the consequences of accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the accident and the equipment functions as designed.

BASES

BACKGROUND (continued)

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 DG starts and is available to accept loads within a 10 second time interval on the Engineered Safety Features Actuation System (ESFAS) or LOVS. Emergency power is established within the maximum time delay assumed for each event analyzed in the accident analysis (Ref. 2).

Since there are four protective channels in a two-out-of-four trip logic for each division of the 4.16 kV power supply, no single failure will cause or prevent protective system actuation. This arrangement meets IEEE Standard 279-1971 criteria (Ref. 4).

APPLICABLE SAFETY ANALYSES

The DG - LOVS is required for Engineered Safety Features (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 DG based on a loss of offsite power during a loss of coolant accident. The actual DG 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 DG supplied power following a loss of offsite power. The analysis assumes a nonmechanistic DG loading, which does not explicitly account for each individual component of the loss of power detection and subsequent actions. This delay time includes contributions from the DG start, DG loading, and Safety Injection System component actuation. The response of the DG 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.

The required channels of LOVS, in conjunction with the ESF systems powered from the DGs, 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 DG start delay and the appropriate sequencing delay, if applicable. The response times for ESFAS actuated equipment include the appropriate DG loading and sequencing delay.

The DG - LOVS channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

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 and when the associated DG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown." The LOVS supports safety systems associated with the ESFAS. In MODES 5 and 6, the four channels must be OPERABLE whenever the associated DG is required to be OPERABLE to ensure that the automatic start of the DG is available when needed.

Actions allow maintenance (trip channel) bypass of individual channels. 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 unacceptable consequences during accidents. During the loss of offsite power, which is an anticipated operational occurrence, the DG 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 are consistent with the assumptions of the plant specific setpoint calculation. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

[For this unit, the Bases for the Allowable Values and trip setpoints are as follows:]

BASES

APPLICABILITY

The DG - 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 DG must be OPERABLE, so that it can perform its function on a loss of power or degraded power to the vital bus.

ACTIONS

A LOVS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's Function. 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 actual trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

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. The required channels are specified on a per DG basis.

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 entered immediately if applicable in the current MODE of operation.

A Note has been added to the ACTIONS to clarify the application of Completion Time rules. The Conditions of this LCO may be entered independently for each Function. The Completion Time(s) of the inoperable channel(s)/train(s) of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

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

Condition A applies if one channel is inoperable for one or more Functions per DG bus.

If the channel cannot be restored to OPERABLE status, the affected channel should either be bypassed or tripped within 1 hour (Required Action A.1).

BASES

ACTIONS (continued)

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. The 1 hour Completion Time is sufficient to perform these Required Actions.

Once Required Action A.1 has been complied with, Required Action A.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. 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 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.

B.1, B.2.1, and B.2.2

Condition B applies if two channels are inoperable for one or more Functions per DG.

If the channel cannot be restored to OPERABLE status within 1 hour, the Conditions and Required Actions for the associated DG made inoperable by DG - LOVS instrumentation are required to be entered. Alternatively, one affected channel is required to be bypassed and the other is tripped, in accordance with Required Action B.2.1. 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.2.1 has been complied with, Required Action B.2.2 allows [48] hours to repair the bypassed or inoperable channel.

After one channel is restored to OPERABLE status, 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.2.2 shall be placed in trip if more than [48] hours have elapsed since the initial channel failure.

BASES

ACTIONS (continued)

C.1

Condition C applies when more than two undervoltage or Degraded Voltage channels on a single bus are inoperable.

Required Action C.1 requires all but two channels to be restored to OPERABLE status within 1 hour. With more than two channels inoperable, the logic is not capable of providing a DG - LOVS signal for valid Loss of Voltage or Degraded Voltage conditions. The 1 hour Completion Time is reasonable to evaluate and take action to correct the degraded condition in an orderly manner and takes into account the low probability of an event requiring LOVS occurring during this interval.

D.1

Condition D applies if the Required Actions and associated Completion Times are not met.

Required Action D.1 ensures that Required Actions for the affected DG inoperabilities are initiated. Depending upon plant MODE, the actions specified in LCO 3.8.1, "AC Sources - Operating," or LCO 3.8.2 are required immediately.

SURVEILLANCE REQUIREMENTS

The following SRs apply to each DG - LOVS Function.

[SR 3.3.6.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the indicated output of the potential transformers that feed the LOVS undervoltage 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

Agreement criteria are determined by the plant staff, based on a combination of the channel instrument uncertainties, including indication and readability. If the channels are within the criteria, it is an indication that the channels are OPERABLE.]

[The Frequency, about once every shift, is based upon operating experience that demonstrates channel failure is rare. 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 3.3.6.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The Frequency of [92] 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 [92] day Frequency is a rare event. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.3

SR 3.3.6.3 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.

The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

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 Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

REFERENCES

1. FSAR, Section [8.3].
2. FSAR, Chapter [15].
3. "Plant Protection System Selection of Trip Setpoint Values."
4. IEEE Standard 279-1971.
5. 10 CFR 50, Appendix A, GDC 21.
6. [ ]

B 3.3 INSTRUMENTATION

B 3.3.6 Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip (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 the Reactor Coolant System (RCS) pressure boundary during anticipated operational occurrences (AOOs) and ensures acceptable consequences during accidents.

The ESFAS contains devices and circuitry that 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 Isolation Actuation Signal (CIAS),
3. Containment Cooling Actuation Signal (CCAS),
4. Recirculation Actuation Signal (RAS),
5. Containment Spray Actuation Signal (CSAS),
6. Main Steam Isolation Signal (MSIS),
7. Emergency Feedwater Actuation Signal SG #1 (EFAS-1), and
8. Emergency Feedwater Actuation Signal SG #2 (EFAS-2).

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,
- Bistable trip units, and

BASES

BACKGROUND (continued)

- ESFAS Logic:
  - Matrix Logic,
  - Initiation Logic (trip paths), and
  - Actuation Logic.

This LCO addresses ESFAS Logic. Bistables and measurement channels are addressed in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Instrumentation."

The role of the measurement channels and bistables is described in LCO 3.3.5. The role of the ESFAS Logic is described below.

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 sense the same input parameter trip. This is called a two-out-of-four trip logic.

Bistable relay contact outputs from the four channels are configured into six Matrix Logics. Each Matrix Logic 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 Matrix Logic contains four normally energized matrix relays. When a coincidence is detected in the two channels being monitored by the Matrix Logic, 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.

Each of the two channels of Actuation Logic, mounted in the Auxiliary Relay Cabinets (ARCs), is responsible for actuating one train of ESF equipment. Each ESF Function has separate Actuation Logic in each ARC.

BASES

BACKGROUND (continued)

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 RTCBs. This logic controls ARC mounted subgroup relays, which are normally energized. Contacts from these relays, when de-energized, actuate specific ESF equipment.

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.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

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 ARCs used to actuate the ESF Function, excluding the subgroup relays, and interconnecting wiring to the initiation relay contacts mounted in the PPS cabinet.

The subgroup relays are actuated by the ESFAS Logic. Each ESFAS Function typically employs several subgroup relays, with each subgroup relay responsible for actuating one or more components in the ESFAS Function. Subgroup relays and their contacts are considered part of the actuated equipment and are addressed under the applicable LCO for this equipment.

It is possible to change the two-out-of-four ESFAS Logic to 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

BASES

BACKGROUND (continued)

simultaneously performed on 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. Trip channel bypassing is addressed in LCO 3.3.5.

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 Trip push button opens one trip path, de-energizing one set of two initiation relays, 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 ensure that Manual Trip 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.

ESFAS 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 (ECCS) and performs several other Functions, such as initiating a containment cooling actuation, initiating control room isolation, and starting the diesel generators.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Isolation Actuation Signal

CIAS ensures acceptable mitigating actions during large and small break LOCAs and during MSLBs or feedwater line breaks (FWLBs) either inside or outside containment. CIAS is initiated by low pressurizer pressure or high containment pressure.

3. Containment Cooling Actuation Signal

CCAS mitigates containment overpressurization when required by either a manual CCAS actuation or an automatic SIAS Function. This Function is not employed by all plants.

4. 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 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. An RWST Level - Low signal initiates the RAS.

5. Containment Spray Actuation Signal

CSAS actuates containment spray, preventing containment overpressurization during large break LOCAs, small break LOCAs, and MSLBs or FWLBs inside containment. CSAS is initiated by high high containment pressure and an SIAS. This configuration reduces the likelihood of inadvertent containment spray.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6. Main Steam Isolation Signal

MSIS ensures acceptable consequences during an MSLB or FWLB (between the steam generator and the main feedwater check valve) either inside or outside containment. MSIS isolates both steam generators 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.

7, 8. Emergency Feedwater Actuation Signal

EFAS consists of two steam generator (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 a steam generator heat sink during a steam generator tube rupture event and an MSLB or FWLB event either inside or outside containment.

Low steam generator water level initiates emergency feed to the affected steam generator, providing the generator is not identified (by the circuitry) as faulted (an MSLB or FWLB).

EFAS logic includes steam generator specific inputs from the Steam Generator Pressure - Low bistable comparator (also used in MSIS) and the SG Pressure Difference - High (SG #1 > SG #2 or SG #2 > SG #1, 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 steam generator even if both are below the MSIS setpoint, while preventing the ruptured generator from being fed. Not feeding a ruptured generator prevents containment overpressurization during the analyzed events.

The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

BASES

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE.

The requirements for each Function are listed below. The reasons for the applicable MODES for each Function are addressed under APPLICABILITY.

1. Safety Injection Actuation Signal

   Automatic SIAS is required to initiate CCAS and CSAS. Automatic SIAS occurs in Pressurizer Pressure - Low or Containment Pressure - High and is explained in Bases 3.3.5.

   a. Manual Trip

      This LCO requires two channels of SIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Matrix Logic

      This LCO requires six channels of SIAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

   c. Initiation Logic

      This LCO requires four channels of SIAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

   d. Actuation Logic

      This LCO requires two channels of SIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

2. 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 Trip

      This LCO requires two channels of CIAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

LCO (continued)

b. Matrix Logic

This LCO requires six channels of CIAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of CIAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

d. Actuation Logic

This LCO requires two channels of CIAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

3. Containment Cooling Actuation Signal

For plants employing a separate CCAS signal, the CCAS Function can be automatically actuated on an SIAS. It can also be manually actuated using two channels of CCAS push buttons, configured similarly to all other ESFAS Manual Trips. CCAS therefore shares the SIAS sensor channels, bistables, coincidence matrices, and matrix relays. It has separate manual channels and Actuation Logic.

a. Manual Trip

This LCO requires two channels of CCAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

b. Initiation Logic

This LCO requires four channels of CCAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

c. Actuation Logic

This LCO requires two channels of CCAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

BASES

LCO (continued)

4. Recirculation Actuation Signal

   a. Manual Trip

      This LCO requires two channels of RAS Manual Trip to be OPERABLE in MODES 1, 2, 3, and 4.

   b. Matrix Logic

      This LCO requires six channels of RAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

   c. Initiation Logic

      This LCO requires four channels of RAS Initiation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

   d. Actuation Logic

      This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

5. 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 before the Containment Pressure - High High input signal to CSAS. This ensures that a CSAS will not initiate unless required.

   a. Manual Trip

      This LCO requires two channels of CSAS Manual Trip to be OPERABLE in MODES 1, 2, and 3.

   b. 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.

BASES

LCO (continued)

c. Matrix Logic

This LCO requires six channels of CSAS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

d. Initiation Logic

This LCO requires four channels of CSAS Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

e. Actuation Logic

This LCO requires two channels of CSAS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

6. Main Steam Isolation Signal

a. Manual Trip

This LCO requires two channels of MSIS Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Matrix Logic

This LCO requires six channels of MSIS Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of MSIS Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

d. Actuation Logic

This LCO requires two channels of MSIS Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

7. Emergency Feedwater Actuation Signal SG #1 (EFAS-1)

EFAS-1 is initiated either by a low steam generator level coincident with no low pressure trip present on SG #1 or by a low steam generator level coincident with a differential pressure between the two generators with the higher pressure in SG #1.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS logic where it is used to determine if a generator is intact. The EFAS logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is less than the Steam Generator Pressure Difference (SGPD) - High setpoint pressure.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

a. Manual Trip

This LCO requires two channels of Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Matrix Logic

This LCO requires six channels of Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

d. Actuation Logic

This LCO requires one channel of Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

8. Emergency Feedwater Actuation Signal SG #2 (EFAS-2)

EFAS-2 is initiated either by a low steam generator level coincident with no low pressure trip present on SG #2 or by a low steam generator level coincident with a differential pressure between the two generators with the higher pressure in SG #2.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS Logic where it is used to determine if a generator is intact. The EFAS Logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is less than the SGPD - High setpoint pressure.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

a. Manual Trip

This LCO requires two channels of Manual Trip to be OPERABLE in MODES 1, 2, and 3.

b. Matrix Logic

This LCO requires six channels of Matrix Logic to be OPERABLE in MODES 1, 2, and 3.

c. Initiation Logic

This LCO requires four channels of Initiation Logic to be OPERABLE in MODES 1, 2, and 3.

d. Actuation Logic

This LCO requires one channel of Actuation Logic to be OPERABLE in MODES 1, 2, and 3.

APPLICABILITY In MODES 1, 2 and 3, there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

- Close the main steam isolation valves to preclude a positive reactivity addition,

BASES

APPLICABILITY (continued)

- Actuate emergency feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),
- 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
- 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 Trip 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 Trip push buttons.

CSAS, MSIS, and EFAS have relatively few components, which can be actuated individually if required in MODE 4, and the systems may be disabled or reconfigured, making system level Manual Trip impossible and unnecessary.

The ESFAS logic must be OPERABLE in the same MODES as the automatic and Manual Trip. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip 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.

ACTIONS

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 entered immediately, if applicable in the current MODE of operation.

BASES

ACTIONS (continued)

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be entered independently for each Function. The Completion Time for the inoperable channel of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1

Condition A 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.

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.

This Condition has been modified by a Note stating that for the purposes of this LCO, de-energizing up to three matrix power supplies due to a single failure, such as loss of a vital instrument bus, 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.

The channel must be restored to OPERABLE status within 48 hours. This provides the operator with time to take appropriate actions and still ensures 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 with 48 hours, Condition E is entered.

BASES

ACTIONS (continued)

B.1

Condition B applies to one Manual Trip or Initiation Logic channel inoperable.

The channel must be restored to OPERABLE status within 48 hours. Operating experience has demonstrated that the probability of a random failure in a second channel is low during any given 48 hour period.

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 relay contact is more difficult to verify, and subsequent shorting of the contact is always possible.

C.1 and C.2

Condition C applies to the failure of both Initiation Logic channels affecting the same trip leg.

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 obviates 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 ensuring 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 ensures 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 channel is low during any given 48 hour period. If the channel cannot be restored to OPERABLE status with 48 hours, Condition E is entered.

BASES

ACTIONS (continued)

Of greater concern is the failure of the initiation circuit in a nontrip 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 nontrip condition, the ESFAS Function is lost in the affected train. 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 Trip of the affected trip leg contacts may be attempted. Caution must be exercised, since depressing the wrong ESFAS push buttons may result in an ESFAS actuation.

D.1

Condition D applies to Actuation Logic.

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 Design Basis Accidents, but the single failure criterion may be violated. For this reason operation in this condition is restricted.

The channel must be restored to OPERABLE status within 48 hours. Operating experience has demonstrated that the probability of a random failure in the Actuation Logic of the second train is low during a given 48 hour period.

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 obviates the need to enter LCO 3.0.3 in the event of a vital bus, matrix, or initiation channel failure.

Required Action D.1 is modified by a Note to indicate that one channel of Actuation Logic may be bypassed for up to 1 hour for Surveillance, provided the other channel is OPERABLE.

This allows performance of a PPS CHANNEL FUNCTIONAL TEST on an OPERABLE ESFAS train without generating an ESFAS actuation in the inoperable train.

BASES

ACTIONS (continued)

E.1 and E.2

If two associated Actuation Logic channels are inoperable, or if the Required Actions and associated Completion Times of Conditions for CSAS, MSIS, or EFAS cannot be met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

F.1 and F.2

If two associated Actuation Logic channels are inoperable, or if the Required Actions and associated Completion Times for SIAS, CIAS, RAS, or CCAS are not met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE REQUIREMENTS

SR 3.3.6.1

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

BASES

SURVEILLANCE REQUIREMENTS (continued)

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SR 3.3.5.2, SR 3.3.6.1, and SR 3.3.6.2, 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 3.3.5.2 and SR 3.3.6.1 are normally performed together and in conjunction with ESFAS testing. SR 3.3.6.2 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 3.3.5.2 is addressed in LCO 3.3.5. SR 3.3.6.1 includes Matrix Logic tests and trip path (Initiation Logic) tests.

Matrix Logic Tests

These tests are performed one matrix at a time. They verify 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, preventing the matrix relay contacts from assuming their energized state. The Matrix Logic tests 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 an ESFAS actuation 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 Frequency of [92] days is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 2).

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.6.2

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 operation of each component actuated by the individual relays is thus verified without the need to actuate the entire ESFAS function.

The 184 day Frequency 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 Frequency. The actual justification is based on CEN-403, "Relaxation of Surveillance Test Interval for ESFAS Subgroup Relay Testing" (Ref. 3).

Some components cannot be tested at power since their actuation might lead to plant trip or equipment damage. Reference 1 lists those 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 the Note to this SR.

SR 3.3.6.3

A CHANNEL FUNCTIONAL TEST is performed on the manual ESFAS actuation circuitry, de-energizing relays and providing manual actuation of the function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every [18] months.

BASES

REFERENCES

1. FSAR, Section [7.3].
2. CEN-327, May 1986, including Supplement 1, March 1989.
3. CEN-403.

B 3.3 INSTRUMENTATION

B 3.3.7 Containment Purge Isolation Signal (CPIS) (Analog)

BASES

BACKGROUND

This LCO encompasses CPIS actuation, which is a plant specific instrumentation system that performs an actuation Function required for plant protection but is not otherwise included in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip," or LCO 3.3.6, "Diesel Generator (DG) - Loss of Voltage Start (LOVS)." This is a non-Nuclear Steam Supply System ESFAS Function that, because of differences in purpose, design, and operating requirements, is not included in LCOs 3.3.5 and 3.3.6. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements applicable to them.

The CPIS provides protection from radioactive contamination in the containment in the event an irradiated 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 level in containment is detected.

The CPIS includes two independent, redundant actuation subsystems. Where two isolation control valves are 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 actuates the containment air supply fan. A list of actuated valves and an additional description of the CPIS are included 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). The CIAS is addressed by LCO 3.3.4, "Engineered Safety Features Actuation System (ESFAS) Instrumentation."

BASES

BACKGROUND (continued)

Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits stated 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 3.3.7.2 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. 3). 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.

Setpoints in accordance with the Allowable Value will ensure 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.

APPLICABLE SAFETY ANALYSES

The CPIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

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 Reference 3. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

BASES

LCO (continued)

The Bases for the LCO on the CPIS are discussed below for each Function:

a. Manual Trip

The LCO on Manual Trip backs up the automatic trips and ensures operators have the capability to rapidly initiate the CPIS Function if any parameter is trending toward its setpoint. At least one channel must be OPERABLE to be consistent with the requirements of LCO 3.9.3, "Containment Penetrations."

b. Containment Radiation - High

The LCO on the radiation channels requires that all four be OPERABLE.

[For this unit, the basis for the Containment Radiation - High setpoint is as follows:]

c. Actuation Logic

One train of Actuation Logic must be OPERABLE to be consistent with the requirements of LCO 3.9.3. If one fails, it must be restored to OPERABLE status.

APPLICABILITY

In MODE 5 or 6, the CPIS isolation of containment purge valves is not required to be OPERABLE. However, during movement of [recently] irradiated fuel [(i.e., fuel that has occupied part of a critical reactor core within the previous [X] days)], there is the possibility of a fuel handling accident requiring the CPIS on high radiation in containment. Accordingly, the CPIS must be OPERABLE during movement of [recently] irradiated fuel in containment.

In MODES 1, 2, 3, and 4, the containment purge valves are sealed closed.

BASES

ACTIONS

A CPIS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's Function. 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 actual trip setpoint is not within the Allowable Value in SR 3.3.7.2, the channel is inoperable and the appropriate Conditions must be entered.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the sensor, 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 protective 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.

A.1 and A.2

Condition A applies to the failure of one Containment Radiation - High CPIS channel. The Required Action is to place the affected channel in the trip condition within 4 hours. The Completion Time accounts for the fact that three redundant channels monitoring containment radiation are still available to provide a single trip input to the CPIS logic to provide the automatic mitigation of a radiation release. Alternately, action must be taken to place the unit in a condition where the LCO does not apply. This does not preclude the movement of fuel to a safe position.

B.1 and B.2

Condition B applies to the failure of the required Manual Trip or automatic Actuation Logic train, to the failure of more than one radiation monitoring channel, or if the Required Action and associated Completion Time of Condition A are not met. Required Action B.1 is to place the containment purge and exhaust isolation valves in the closed position. The Required Action immediately performs the isolation Function of the CPIS. Required Action B.2 is to immediately enter the applicable Conditions and Required Actions for the affected isolation valves of LCO 3.9.3, "Containment Penetrations," that were made inoperable by the inoperable

BASES

ACTIONS (continued)

instrumentation of the CPIS LCO. The Required Action directs the operator to take actions that are appropriate for the containment isolation Function of the CPIS without initiating the containment air supply and exhaust fans. The Completion Time accounts for the fact that the automatic capability to isolate containment and initiate supply and exhaust fans on valid containment high radiation signals is degraded during conditions in which a fuel handling accident is possible and CPIS provides the only automatic mitigation of radiation release.

SURVEILLANCE REQUIREMENTS

SR 3.3.7.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. 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 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 indication and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limits.

The Frequency, about once every shift, is based on operating experience that demonstrates the rarity of channel failure. 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.2

A CHANNEL FUNCTIONAL TEST is performed on each containment radiation monitoring channel to ensure the entire channel will perform its intended function. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The Frequency of [92] 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 [92] day interval is a rare event.

SR 3.3.7.3

Proper operation of the initiation 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. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. A Note indicates this Surveillance includes verification of operation for each initiation relay.

The 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.4

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive calibrations to ensure that the channel remains operational between successive tests. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis.

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.7.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual CPIS actuation circuitry. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

This Surveillance 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 Trip of the Function. The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power. Operating experience has shown these components usually pass the Surveillance when performed at a Frequency of once every 18 months.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.6

This Surveillance ensures that the train actuation response times are less than or equal to the maximum times assumed in the analyses. The 18 month Frequency is based upon plant operating experience, which shows random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included. Testing of the final actuating device in one channel is included in the testing of each actuation logic channel.

REFERENCES

1. FSAR, Section [6.2].

2. FSAR, Section [7.3].

3. "Plant Protection System Selection of Trip Setpoint Values."

B 3.3 INSTRUMENTATION

B 3.3.7 Diesel Generator (DG) - Loss of Voltage Start (LOVS) (Digital)

BASES

BACKGROUND

The DGs provide a source of emergency power when offsite power is either unavailable or insufficiently stable to allow safe unit 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 4.16 kV vital bus.

Four undervoltage relays with inverse time characteristics are provided on each 4.16 kV 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 "Onsite Power Systems" (Ref. 1).

Trip Setpoints and Allowable Values

The trip setpoints and Allowable Values are based on the analytical limits presented in "Accident Analysis," 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 3.3.7.3 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 trip setpoint does not exceed the documented Surveillance acceptance criteria, the undervoltage relay is considered OPERABLE.

Setpoints in accordance with the Allowable Values will ensure that the consequences of accidents will be acceptable, providing the plant is operated from within the LCOs at the onset of the accident and the equipment functions as designed.

BASES

BACKGROUND (continued)

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 DG starts and is available to accept loads within a 10 second time interval on the Engineered Safety Features Actuation System (ESFAS) or LOVS. Emergency power is established within the maximum time delay assumed for each event analyzed in the accident analysis (Ref. 2).

Since there are four protective channels in a two-out-of-four trip logic for each division of the 4.16 kV power supply, no single failure will cause or prevent protective system actuation. This arrangement meets IEEE Standard 279-1971 criteria (Ref. 4).

APPLICABLE SAFETY ANALYSES

The DG - LOVS is required for Engineered Safety Features (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 DG based on a loss of offsite power during a loss of coolant accident. The actual DG 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 DG supplied power following a loss of offsite power. The analysis assumes a nonmechanistic DG loading, which does not explicitly account for each individual component of the loss of power detection and subsequent actions. This delay time includes contributions from the DG start, DG loading, and Safety Injection System component actuation. The response of the DG 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.

The required channels of LOVS, in conjunction with the ESF systems powered from the DGs, 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).

BASES

APPLICABLE SAFETY ANALYSES (continued)

The delay times assumed in the safety analysis for the ESF equipment include the [10] second DG start delay and the appropriate sequencing delay, if applicable. The response times for ESFAS actuated equipment in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Instrumentation," include the appropriate DG loading and sequencing delay.

The DG - LOVS channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

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 and when the associated DG is required to be OPERABLE by LCO 3.8.2, "AC Sources - Shutdown." The LOVS supports safety systems associated with the ESFAS. In MODES 5 and 6, the four channels must be OPERABLE whenever the associated DG is required to be OPERABLE to ensure that the automatic start of the DG is available when needed.

Actions allow maintenance (trip channel) bypass of individual channels. 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 units 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 unacceptable consequences during accidents. During the loss of offsite power, which is an anticipated operational occurrence, the DG 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. A channel is inoperable if its actual trip setpoint is not within its required Allowable Value.

BASES

APPLICABLE SAFETY ANALYSES (continued)

[For this unit, the Bases for the Allowable Values and trip setpoints are as follows:]

APPLICABILITY

The DG - 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 DG must be OPERABLE, so that it can perform its function on a loss of power or degraded power to the vital bus.

ACTIONS

A LOVS channel is inoperable when it does not satisfy the OPERABILITY criteria for the channel's function. 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 actual trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

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. The required channels are specified on a per DG basis.

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 entered immediately if applicable in the current MODE of operation.

A Note has been added to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each DG - LOVS Function. The Completion Time(s) of the inoperable channel(s) of a Function will be tracked separately for each Function, starting from the time the Condition was entered for that Function.

A.1 and A.2

Condition A applies if one channel is inoperable for one or more Functions per DG bus.

BASES

ACTIONS (continued)

If the channel cannot be restored to OPERABLE status, the affected channel should either be bypassed or tripped within 1 hour (Required Action A.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.1 has been complied with, Required Action A.2 allows prior to entering MODE 2 following the next MODE 5 entry to repair the inoperable channel. If the channel cannot be restored to OPERABLE status, the plant cannot enter MODE 2 following the next MODE 5 entry. 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 acceptable. The prior to entering MODE 2 following the next MODE 5 entry Completion Time is based on adequate channel independence, which allows a two-out-of-three channel operation since no single failure will cause or prevent a reactor trip.

B.1 and B.2

Condition B applies if two channels are inoperable for one or more Functions.

If the channel cannot be placed in bypass or trip within 1 hour, the Conditions and Required Actions for the associated DG made inoperable by DG - LOVS instrumentation are required to be entered. Alternatively, one affected channel is required to be bypassed and the other is tripped, in accordance with Required Action B.2. This places the Function in one-out-of-two logic. The 1 hour Completion Time is sufficient to perform the Required Actions.

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one DG - LOVS channel, and placing a second channel in trip will result in a loss of voltage diesel start signal. Therefore, if one DG - LOVS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

BASES

ACTIONS (continued)

After one channel is restored to OPERABLE status, the provisions of Condition A still apply to the remaining inoperable channel.

C.1

Condition C applies when more than two undervoltage or Degraded Voltage channels on a single bus are inoperable.

Required Action C.1 requires all but two channels to be restored to OPERABLE status within 1 hour. With more than two channels inoperable, the logic is not capable of providing the DG - LOVS signal for valid Loss of Voltage or Degraded Voltage conditions. The 1 hour Completion Time is reasonable to evaluate and take action to correct the degraded condition in an orderly manner and takes into account the low probability of an event requiring LOVS occurring during this interval.

D.1

Condition D applies if the Required Actions and associated Completion Times are not met.

Required Action D.1 ensures that Required Actions for the affected DG inoperabilities are initiated. Depending upon plant MODE, the ACTIONS specified in LCO 3.8.1, "AC Sources - Operating," or LCO 3.8.2 are required immediately.

SURVEILLANCE REQUIREMENTS

The following SRs apply to each DG - LOVS Function.

[SR 3.3.7.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the indicated output of the potential transformers that feed the LOVS undervoltage 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.]

BASES

SURVEILLANCE REQUIREMENTS (continued)

[Agreement criteria are determined by the plant staff based on a combination of channel instrument uncertainties, including indication and readability. If the channels are within the criteria, it is an indication that the channels are OPERABLE.

The Frequency, about once every shift, is based upon operating experience that demonstrates channel failure is rare. 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 3.3.7.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel will perform its intended function when needed. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The Frequency of [92] 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 [92] day Frequency is a rare event. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.7.3

SR 3.3.7.3 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. The Surveillance verifies that the channel responds to a measured parameter within the necessary range and accuracy. CHANNEL CALIBRATION leaves the channel adjusted to account for instrument drift between successive surveillances to ensure the instrument channel remains operational. CHANNEL CALIBRATIONS must be performed consistent with the plant specific setpoint analysis. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as found and as left values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [6].

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 Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

REFERENCES

1. FSAR, Section [8.3].
2. FSAR, Chapter [15].
3. "Plant Protection System Selection of Trip Setpoint Values."
4. IEEE Standard 279-1971.
5. 10 CFR 50, Appendix A, GDC 21.
6. [ ].