

## 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 CFR50.36 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. 10) and could be used to meet the requirement that they be contained in the technical specifications.

Technical specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. Operable is defined

---

## BASES

### BACKGROUND (continued)

---

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 Value 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 Safety Limit is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. If the actual setting of the device is found to have exceeded the

## BASES

---

### BACKGROUND (continued)

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. 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.

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and

## BASES

---

### BACKGROUND (continued)

- 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 ( $\Delta T$  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.

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.



## BASES

---

### BACKGROUND (continued)

Measurement channels used as an input to the RPS are never used for control functions.

When a channel monitoring a parameter exceeds a predetermined setpoint, indicating an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter de-energizes Matrix Logic, which in turn de-energizes the Initiation Logic. This causes all eight RTCBs to open, interrupting power to the control element assemblies (CEAs), allowing them to fall into the core.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in 10 CFR 50, Appendix A (Ref. 1). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic. Thus, even with a channel inoperable, no single additional failure in the RPS can either cause an inadvertent trip 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. 3).

Many of the RPS trips are generated by comparing a single measurement to a fixed bistable setpoint. Certain Functions, however, make use of more than one measurement to provide a trip. The following trips use multiple measurement channel inputs:

- Steam Generator Level - Low

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

- Steam Generator Pressure - Low

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

## BASES

---

### BACKGROUND (continued)

- Variable High Power Trip (VHPT) - High

The VHPT uses Q power as its only input. Q power is the higher of NI power and  $\Delta T$  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.

#### 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

## BASES

---

### BACKGROUND (continued)

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 4. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment errors - for those RPS channels that must function in harsh environments, as defined by 10 CFR 50.49 (Ref. 5) - Allowable Values specified in Table 3.3.1-1, 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. 6). The 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. 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.

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized,

## BASES

---

### BACKGROUND (continued)

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.

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

## BASES

---

### BACKGROUND (continued)

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.

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.

## BASES

---

### BACKGROUND (continued)

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. 7), 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 3 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 TMLP trip to protect against. The following events require VHPT protection:

- Uncontrolled CEA withdrawal event,
  - Excess load,
  - Excess feedwater heat removal event,
  - CEA ejection event, and
  - Main steam line break (MSLB) (outside containment).
-

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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  $< 1\text{E-4}\%$  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)

7a, 7b. 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:

- Excess load (inadvertent opening of a steam generator ADV),

## BASES

## APPLICABLE SAFETY ANALYSES (continued)

- 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  $T_o$ , 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 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.

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

## BASES

---

APPLICABLE SAFETY ANALYSES (continued)

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  $< 1\text{E-4}\%$  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  $< 1\text{E-4}\%$  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.

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.

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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. 6).

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

## BASES

---

### LCO (continued)

#### 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  $\Delta T$  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

## BASES

---

### LCO (continued)

setting is low enough to initiate a reactor trip to prevent containment pressure from exceeding design pressure following a DBA.

#### 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.

#### 7a, 7b. 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  $\geq$  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  $\Delta T$  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.

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

## BASES

---

### LCO (continued)

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  $\geq$  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.

---

#### 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

## BASES

### APPLICABILITY (continued)

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  $\geq$  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.

A Note has been added to the ACTIONS to clarify the application of the Completion Time rules. The Conditions of this Specification may be

## BASES

---

### ACTIONS (continued)

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.

#### B.1 and B.2

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

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even

## BASES

---

### ACTIONS (continued)

though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the [48] hours permitted is remote.

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.

#### 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

## BASES

---

### ACTIONS (continued)

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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the [48] hours permitted is remote.

#### 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 SRcolumn 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. 8).

---

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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

#### SR 3.3.1.2

A daily calibration (heat balance) is performed when THERMAL POWER is  $\geq 20\%$ . 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 " $\Delta T$  power calibrate" potentiometers are then used to null the "nuclear power -  $\Delta T$  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  $\geq 20\%$  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.

#### 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



## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

determined by the incore detectors. A Note to the Frequency indicates the Surveillance is required within 12 hours after THERMAL POWER is  $\geq$  [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 7. These tests verify that the RPS is capable of performing its intended function, from bistable input through the RTCBs. They include:

#### 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. 6). 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 9.

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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. 9).

#### 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.

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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 [9].

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.

#### 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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. 9). 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 [9].

The Frequency is based upon the assumption of an 18 month calibration interval for 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. 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).

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

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  $n \times 18$  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. {10 - analog and digital 3.3.1, analog 3.3.4/11 - digital 3.3.5} 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.

The Surveillance is modified by a Note 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

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

compensated for by performing the daily calorimetric calibration (SR 3.3.1.2) and the monthly linear subchannel gain check (SR 3.3.1.3).

---

REFERENCES

1. 10 CFR 50, Appendix A, GDC 21.
  2. 10 CFR 100.
  3. IEEE Standard 279-1971, April 5, 1972.
  4. FSAR, Chapter [14].
  5. 10 CFR 50.49.
  6. "Plant Protection System Selection of Trip Setpoint Values."
  7. FSAR, Section [7.2].
  8. NRC Safety Evaluation Report, [Date].
  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."
  11. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."
-

BASES

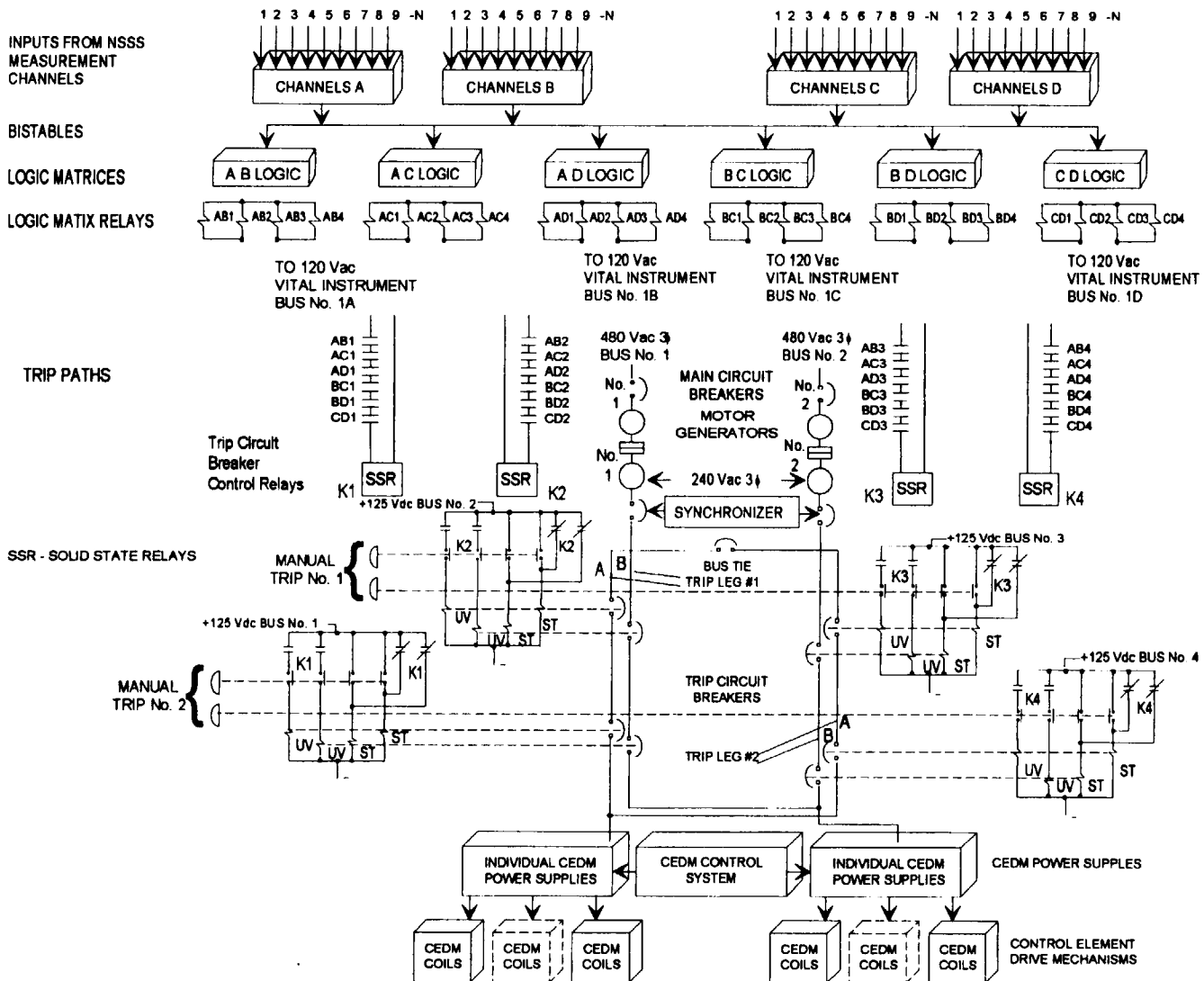


Figure B 3.3.1-1 (page 1 of 1)  
Functional Diagram of the Two-Out-of-Four Logic and RTCB Configuration

CEOG STS

B 3.3.1 - 35

Rev. 2, 04/30/01

## B 3.3 INSTRUMENTATION

### B 3.3.2 Reactor Protective System (RPS) Instrumentation - Shutdown

#### 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 excure 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  $< 1\text{E-}4\%$  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

## BASES

---

### LCO (continued)

safety analysis. Therefore, the Allowable Value specified in SR 3.3.4.2 is not derived from an analytical limit.

---

### 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.

---

BASES

---

ACTIONS (continued)

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.

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

## BASES

---

### ACTIONS (continued)

two-out-of-three logic; but with another channel failed, the RPS may be operating in a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the RPS in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, the reactor will trip.

[ The bypassed channel should be restored to OPERABLE status within 48 hours for reasons similar to those stated under Condition 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. ]

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the [48] hours permitted is remote.

#### 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

## BASES

---

### ACTIONS (continued)

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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the 48 hours permitted is remote.

#### 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, 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

#### 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

#### 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.



## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

---

### 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 3.3.3 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.

Each trip path is responsible for opening one set of two of the eight RTCBs. The RTCB control relays (K-relays), when de-energized,

## BASES

---

### BACKGROUND (continued)

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 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

## BASES

---

### BACKGROUND (continued)

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.

If one set of RTCBs has been opened in response to a single RTCB channel, Initiation Logic channel, or Manual Trip channel failure, the

## BASES

---

### LCO (continued)

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."



## BASES

---

### 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.

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

## BASES

---

### ACTIONS (continued)

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.

#### 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.

**BASES****ACTIONS (continued)**

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(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 3.3.4 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.

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

## BASES

---

### BACKGROUND (continued)

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.

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



## BASES

---

### BACKGROUND (continued)

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 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.

## BASES

### BACKGROUND (continued)

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:

##### 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

BASES

---

APPLICABLE SAFETY ANALYSES (continued)

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.

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.

## 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 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 Signala. Containment Pressure - High

This LCO requires four channels of SIAS Containment Pressure - 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 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.

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.

## BASES

---

### LCO (continued)

This LCO applies to the bypass removal feature only. If the bypass enable Function is failed so as to prevent entering a bypass condition, operation may continue.

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.

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.

BASES

---

LCO (continued)

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.

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

## BASES

---

### LCO (continued)

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

---

## BASES

---

### APPLICABILITY (continued)

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 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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed, to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the [48] hours permitted is remote.

#### 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

## BASES

---

### ACTIONS (continued)

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.

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.

## BASES

---

### ACTIONS (continued)

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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed, to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the 48 hours permitted is remote.

#### 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.

---



BASES

---

SURVEILLANCE REQUIREMENTS (continued)

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 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

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

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].

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).

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

#### 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].

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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

data, or vendor engineering specifications. Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements," Ref. {10 - analog and digital 3.3.1, analog 3.3.4/11 - digital 3.3.5} 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. This results in the interval between successive tests of a given channel of  $n \times 18$  months, where  $n$  is the number of channels in the Function. 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.

BASES

---

REFERENCES (continued)

---

10. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."
- 
-

### 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.

BASES

---

LCO (continued)

Actuation Logic consists of all circuitry housed within the actuation subsystems, including the initiating relay contacts responsible for actuating the ESF equipment.

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.

BASES

---

LCO (continued)

b. Actuation Logic

This LCO requires two channels of RAS Actuation Logic to be OPERABLE in MODES 1, 2, 3, and 4.

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

## BASES

---

### APPLICABILITY (continued)

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. 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.

## BASES

---

### ACTIONS (continued)

#### 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.

#### 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



BASES

---

ACTIONS (continued)

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 3.3.5.1

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,

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

- Letdown stop valves,
- CCW to and from the RCPs,
- MSIVs and feedwater isolation valves, and
- Instrument air containment isolation valves.

The reasons that each of the above cannot be fully tested at power are stated in Reference 1.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components.

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.

BASES

---

REFERENCES

1. FSAR, Section [7.3].
  2. CEN-327, June 2, 1986, including Supplement 1, March 3, 1989.
-

## B 3.3 INSTRUMENTATION

### B 3.3.6 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.

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

## BASES

---

### BACKGROUND (continued)

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: ]

---

### 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.

---

## BASES

---

### 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).

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.

## BASES

---

### ACTIONS (continued)

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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES, even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

Restoring at least one channel to OPERABLE status is the preferred action. 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.

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. ]

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

[ 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].

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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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 3.3.7 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."

##### 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

## BASES

### BACKGROUND (continued)

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.

The Bases for the LCO on the CPIS are discussed below for each Function:

## BASES

---

### LCO (continued)

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 [ ] 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 moving any [recently] irradiated fuel in containment.

In MODES 1, 2, 3, and 4, the containment purge valves are sealed closed.

---

### 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

## BASES

---

### ACTIONS (continued)

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 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

## BASES

---

### ACTIONS (continued)

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.

#### 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

---



## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

#### 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.

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

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.

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 3.3.8 Control Room Isolation Signal (CRIS) (Analog)

#### BASES

---

##### BACKGROUND

This LCO encompasses CRIS actuation, which is a plant specific instrumentation channel 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 LCO 3.3.5 and LCO 3.3.6. Details of this LCO are for illustration only. Individual plants shall include those Functions and LCO requirements that are applicable to them.

The CRIS terminates the normal supply of outside air to the control room and initiates actuation of the Emergency Radiation Protection System to minimize operator radiation exposure. The CRIS includes two independent, redundant subsystems, including actuation trains. Each train employs two separate sensors. One sensor detects gaseous activity. The other detects particulate and iodine activity. Since the two sensors detect different types of activity, they are not considered redundant to each other. However, since there are separate sensors in each train, the trains are redundant. If the bistable monitoring either sensor indicates an unsafe condition, that train will be actuated (one-out-of-two logic). The two trains actuate separate equipment. Actuating either train will perform the intended function. Control room isolation also occurs on a Safety Injection Actuation Signal (SIAS).

##### Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits (Ref. 1). 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 LCO 3.3.8 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. 2). 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

## BASES

---

### BACKGROUND (continued)

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 CRIS, in conjunction with the Control Room Emergency Air Cleanup System (CREACS), maintains the control room atmosphere within conditions suitable for prolonged occupancy throughout the duration of any one of the accidents discussed in Reference 1. The radiation exposure of control room personnel, through the duration of any one of the postulated accidents discussed in "Accident Analysis," FSAR, Chapter [15] (Ref. 1), does not exceed the limits set by 10 CFR 50, Appendix A, GDC 19 (Ref. 3).

The CRIS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).

---

### LCO

LCO 3.3.8 requires one channel of CRIS to be OPERABLE. The required channel consists of Actuation Logic, Manual Trip, and particulate/iodine and gaseous radiation monitors. The specific Allowable Values for the setpoints of the CRIS are listed in the SRs.

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 2. 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 CRIS 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 CRIS Function if any parameter is trending toward its setpoint. One channel must be OPERABLE. This considers that the Manual Trip capability is a backup and that other means are available to actuate the redundant train if required, including manual SIAS.

b. Airborne Radiation

Both channels of Airborne Radiation detection in the required train are required to be OPERABLE to ensure the control room isolates on either high iodine and high particulate or gaseous concentration.

[ For this unit, the basis for the Allowable Value is as follows: ]

c. Actuation Logic

One train of Actuation Logic must be OPERABLE, since there are alternate means available to actuate the redundant train, including SIAS.

---

### APPLICABILITY

The CRIS Functions must be OPERABLE in MODES 1, 2, 3, 4, [5, and 6] and during movement of [recently] irradiated fuel assemblies [(i.e., fuel that has occupied part of a critical reactor core within the previous [ ] days)] to ensure a habitable environment for the control room operators.

---

#### - REVIEWER'S NOTE -

For those plants that credit gas decay tank rupture accidents, the CRIS must also be OPERABLE in MODES 5 and 6.

---

### ACTIONS

A CRIS 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

## BASES

---

### ACTIONS (continued)

generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it within specification. If the trip setpoint is not within the Allowable Value, the channel is inoperable and the appropriate Conditions must be entered.

#### A.1, B.1, B.2, C.1, C.2.1, and C.2.2

Conditions A and C have been modified by a Note, which specifies that CREACS be placed manually in the toxic gas protection mode if the automatic transfer to the toxic gas protection mode is inoperable. [At this unit, the basis for this Note is as follows:]

Conditions A, B, and C are applicable to manual and automatic actuation of the CREACS by CRIS. Condition A applies to the failure of the CRIS Manual Trip, Actuation Logic, and required particulate/iodine and required gaseous radiation monitor channels in MODE 1, 2, 3, or 4. Entry into this Condition requires action to either restore the failed channel(s) or manually perform the CRIS safety function (Required Action A.1). The Completion Time of 1 hour is sufficient to complete the Required Actions and accounts for the fact that CRIS supplements control room isolation by other Functions (e.g., SIAS) in MODES 1, 2, 3, and 4. If the channel cannot be restored to OPERABLE status, 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 (Required Action B.1) and to MODE 5 within 36 hours (Required Action B.2). The Completion Times of 6 hours and 36 hours for reaching MODES 3 and 5 from MODE 1 are reasonable, based on operating experience and normal cooldown rates, for reaching the required MODE from full power conditions in an orderly manner and without challenging plant safety systems or operators.

Condition C applies to the failure of CRIS Manual Trip, Actuation Logic, and required particulate/iodine and required gaseous radiation monitor channels [in MODE 5 or 6] or when moving [recently] irradiated assemblies. The Required Actions are immediately taken to place one OPERABLE CREACS train in the emergency radiation protection mode or to suspend positive reactivity additions and movement of [recently] irradiated fuel assemblies. The Completion Time recognizes the fact that the radiation signals are the only Functions available to initiate control room isolation in the event of a fuel handling accident requiring control room isolation.

## BASES

---

### ACTIONS (continued)

Required Action [ ] is modified by a note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

---

### SURVEILLANCE REQUIREMENTS

#### SR 3.3.8.1

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 limit.

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.

At this unit, the following administrative controls and design features (e.g., downscale alarms) immediately alert operations to loss of function in the nonredundant channels.

[ At this unit, verification of sample system alignment and operation for gaseous, particulate, and iodine monitors is required as follows: ]

---

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.8.2

A CHANNEL FUNCTIONAL TEST is performed on the required control room 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 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 [4].

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 3.3.8.3

Proper operation of the individual 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.

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] days interval is a rare event.



BASES

---

SURVEILLANCE REQUIREMENTS (continued)

Note 1 indicates this Surveillance includes verification of operation for each initiation relay.

Note 2 indicates that relays that cannot be tested at power are excepted from the Surveillance Requirement while at power. These relays must, however, be tested during each entry into MODE 5 exceeding 24 hours unless they have been tested within the previous 6 months.

SR 3.3.8.4

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 surveillance interval extension analysis. The requirements for this review are outlined in Reference [4].

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 3.3.8.5

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual CRIS 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 test verifies that the trip push buttons are capable of opening contacts in the Actuation Logic as designed, de-energizing the initiation relays and providing Manual Trip of the function. The [18] month Frequency is based on the need to perform this Surveillance under the

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

#### [ SR 3.3.8.6

This Surveillance ensures that the train actuation response times are less than the maximum times assumed in the analyses. The [18] month Frequency is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Testing of the final actuating devices, which make up the bulk of the response time, is included in the Surveillance testing. ]

---

### REFERENCES

1. FSAR, Chapter [15].
  2. "Plant Protection System Selection of Trip Setpoint Values."
  3. 10 CFR 50, Appendix A, GDC 19.
  4. [ ].
-

## B 3.3 INSTRUMENTATION

### B 3.3.9 Chemical and Volume Control System (CVCS) Isolation Signal (Analog)

#### BASES

---

#### BACKGROUND

This LCO encompasses Chemical and Volume Control System (CVCS) Isolation Signal actuation. This is a plant specific instrumentation channel that performs an actuation Function required for plant protection and 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 that are applicable to them.

The CVCS Isolation Signal provides protection from radioactive contamination, as well as personnel and equipment protection in the event of a letdown line rupture outside containment.

Each of the two actuation subsystems will isolate a separate letdown isolation valve in response to a high pressure condition in either the West Penetration Room or Letdown Heat Exchanger Room. Two pressure detectors in each of these rooms feed the four sensor subsystems. On a two-out-of-four coincidence, both actuation subsystems will actuate.

#### Trip Setpoints and Allowable Values

Trip setpoints used in the bistables are based on the analytical limits stated in Reference 1. 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 3.3.9.2 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. 2). 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 interval. If the measured setpoint does not exceed the Allowable Value, the bistable is considered OPERABLE.

BASES

---

BACKGROUND (continued)

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 CVCS Isolation Signal is redundant to the Safety Injection Actuation Signal for letdown line breaks outside containment. In addition, an excess flow check valve is located in containment just downstream of the regenerative heat exchanger, which isolates letdown when flow exceeds 200 gpm.

[ At this unit, the provision of two sensors in each room in a two-out-of-four logic configuration satisfies the single failure criterion as follows: ]

The CVCS 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 the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 2).

CVCS isolation consists of closing the appropriate valve. This is undesirable at power, since letdown isolation will result. The absence of letdown flow will significantly decrease the charging flow temperature due to the absence of the regenerative heat exchanger preheating, causing unnecessary thermal stress to the charging nozzle. Therefore, the preferred action is to restore the valve function to OPERABLE status.

Four channels of West Penetration Room and Letdown Heat Exchanger Room pressure sensing and two Actuation Logic channels are required to be OPERABLE.

## BASES

---

### LCO (continued)

[ For this unit, the Bases for the Allowable Values are as follows: ]

[ For this unit, the Bases for the LCO requirement are as follows: ]

---

### APPLICABILITY

The CVCS Isolation Signal must be OPERABLE in MODES 1, 2, 3, and 4, since the possibility of a loss of coolant accident is greatest in these MODES. In MODE 5 or 6, the probability is greatly diminished, and there is time to manually isolate CVCS.

---

### ACTIONS

A CVCS isolation 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 trip setpoint is not consistent with the Allowable Value in SR 3.3.9.2, the channel must be declared inoperable immediately 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 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.1

Condition A applies to the failure of one CVCS Actuation Logic channel associated with the CVCS Isolation Signal. Required Action A.1 requires restoration of the inoperable channel to restore redundancy of the affected Function. The Completion Time of 48 hours is consistent with the Completion Time of other ESFAS Functions and should be adequate

---

## BASES

---

### ACTIONS (continued)

for most repairs, while minimizing the risk of operating with an inoperable channel.

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

Condition B applies if one of the four CVCS instrument channels is inoperable. The Required Actions are identical to those of ESFAS Functions employing four redundant sensors specified in LCO 3.3.4, "Engineered Safety Features Actuation System (ESFAS) Instrumentation." The channel must be placed in bypass or trip if it cannot be repaired within 1 hour (Required Action B.1). The provision of four trip channels allows one channel to be bypassed (removed from service) during operations, placing the ESFAS in two-out-of-three coincidence logic. Placing the channel in bypass is preferred, since the CVCS isolation Function will be in two-out-of-three logic. This will avoid possible inadvertent CVCS isolation if an additional channel fails. The 1 hour Completion Time to bypass or trip the channel is sufficient time to perform the Required Actions.

Once the Required Action to trip or bypass the channel has been complied with, Required Action B.2.1 and Required Action B.2.2 provide for restoring the channel to OPERABLE status or placing it in trip within 48 hours. 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 dependent channels cannot prevent CVCS isolation actuation. The Completion Time provides the operator with time to take appropriate actions and still ensures that any risk involved in operating with a failed channel is acceptable. It is improbable that a failure of a second channel will occur during any given 48 hour period.

#### C.1 and C.2

Condition C applies if two of the four CVCS West Penetration Room/Letdown Heat Exchanger Room Pressure - High channels are inoperable. The Required Actions are identical to those for other ESFAS Functions employing four redundant sensors in LCO 3.3.4.

Restoring at least one channel to OPERABLE status is the preferred Required Action. If this cannot be accomplished, one channel should be placed in bypass and the other channel in trip. The allowed Completion Time of 1 hour is sufficient time to perform the Required Actions.

## BASES

---

### ACTIONS (continued)

Once the Required Action to trip or bypass the channel has been complied with, Required Action C.2 provides for restoring one channel to OPERABLE status within 48 hours. The justification of the 48 hour Completion Time is the same as for Condition B.

After one channel is restored to OPERABLE status, the provisions of Condition C still apply to the remaining inoperable channel.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. MODE changes in this configuration are allowed to permit maintenance and testing on one of the inoperable channels. In this configuration, the protection system is in a one-out-of-two logic, and the probability of a common cause failure affecting both of the OPERABLE channels during the 48 hours permitted is remote.

#### D.1 and D.2

Condition D specifies the shutdown track to be followed if two Actuation Logic channels are inoperable or if the Required Actions and associated Completion Times of Condition A, B, or C are not met. If two Actuation Logic channels are inoperable or the Required Actions 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 Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

---

### SURVEILLANCE REQUIREMENTS

#### SR 3.3.9.1

Performance of the CHANNEL CHECK on each CVCS isolation pressure indicating channel 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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 limit.

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.

#### SR 3.3.9.2

A CHANNEL FUNCTIONAL TEST is performed on each 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 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 of 31 days is based on plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 31 day interval is a rare event.

Proper operation of the individual subgroup relays is verified by de-energizing these relays during the CHANNEL FUNCTIONAL TEST of the Actuation Logic every 31 days. This will actuate the Function,



## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

operating all associated equipment. Proper operation of the equipment actuated by each train is thus verified. Note 1 indicates this test includes verification of operation for each initiation relay. [At this unit, the verification is conducted as follows:]

Note 2 indicates that relays that cannot be tested at power are excepted from the SR while at power. These relays must, however, be tested during each entry into MODE 5 exceeding 24 hours unless they have been tested within the previous 6 months.

[ At this unit, the basis for this test exception is as follows: ]

[ At this unit, the following relays excepted by this Note are: ]

#### SR 3.3.9.3

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 [3].

Radiation detectors may be removed and calibrated in a laboratory, calibrated in place using a transfer source or replaced with an equivalent laboratory calibrated unit.

The Frequency is based upon the assumptions of an 18 month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis and includes operating experience as well as consistency with an 18 month fuel cycle.

---

### REFERENCES

1. FSAR, Section [7.3].
2. "Plant Protection System Selection of Trip Setpoint Values."

BASES

---

REFERENCES (continued)

---

3. [ ].

---

---

## B 3.3 INSTRUMENTATION

### B 3.3.10 Shield Building Filtration Actuation Signal (SBFAS) (Analog)

#### BASES

---

BACKGROUND	<p>This LCO encompasses the SBFAS, 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 that are applicable to them.</p>
APPLICABLE SAFETY ANALYSES	<p>The SBFAS is required to filter the air space between the containment and shield building during a loss of coolant accident (LOCA), as discussed in FSAR, Chapter 15 (Ref. 1).</p> <p>The SBFAS satisfies the requirements of Criterion 3 of 10 CFR 50.36(c)(2)(ii).</p>
LCO	<p>The LCO on equipment OPERABILITY ensures that the SBFAS will perform as required when called upon.</p> <p>The LCO requires two channels of SBFAS automatic and Manual Trip to be OPERABLE. Two channels are necessary to ensure the required redundancy should one channel become inoperable.</p>
APPLICABILITY	<p>The SBFAS must be OPERABLE in MODES 1, 2, 3, and 4, since the possibility of a LOCA is greatest in these MODES. In MODE 5 or 6 the probability of a LOCA is greatly diminished, and there is ample time to respond manually to a LOCA event.</p>
ACTIONS	<p>When the number of inoperable channels in a trip Function exceeds those specified in the Conditions 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.</p>

---

## BASES

---

### ACTIONS (continued)

#### A.1

Condition A applies to the failure of one SBFAS Manual Trip channel or of one Actuation Logic associated with the Chemical and Volume Control System Isolation Signal or SBFAS. Required Action A.1 requires restoration of the inoperable channel to restore redundancy of the affected Function. The Completion Time of 48 hours is consistent with the Completion Time of other ESFAS Functions employing similar logic and should be adequate for most repairs while minimizing the risk of operating with an inoperable channel for a manually actuated Function.

#### B.1 and B.2

Condition B specifies the shutdown track to be followed if the Required Action and associated Completion Time of Condition A are not met. If Required Action A.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 Completion Times are reasonable, based on operating experience, to reach the required MODE from full power conditions in an orderly manner and without challenging plant systems.

---

### SURVEILLANCE REQUIREMENTS

#### SR 3.3.10.1

The SBFAS can be initiated either on a Safety Injection Actuation Signal (SIAS) or manually. This Surveillance is a restatement of SR 3.3.5.1 on the SIAS Function. Performing SR 3.3.5.1 satisfies this Surveillance. 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 is the same as that for SR 3.3.5.1.

#### SR 3.3.10.2

Every [18] months, a CHANNEL FUNCTIONAL TEST is performed on the manual SBFAS 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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, Chapter [15].
-

## B 3.3 INSTRUMENTATION

### B 3.3.11 Post Accident Monitoring (PAM) Instrumentation (Analog)

#### BASES

---

##### BACKGROUND

The primary purpose of the post accident monitoring (PAM) instrumentation is to display plant variables that provide information required by the control room operators during accident situations. This information provides the necessary support for the operator to take the manual actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety Functions for Design Basis Events.

The OPERABILITY of the PAM instrumentation ensures that there is sufficient information available on selected plant parameters to monitor and assess plant status and behavior following an accident.

The availability of PAM instrumentation is important so that responses to corrective actions can be observed and the need for, and magnitude of, further actions can be determined. These essential instruments are identified by plant specific documents (Ref. 1) addressing the recommendations of Regulatory Guide 1.97 (Ref. 2), as required by Supplement 1 to NUREG-0737, "TMI Action Items" (Ref. 3).

Type A variables are included in this LCO because they provide the primary information required to permit the control room operator to take specific manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions for Design Basis Accidents (DBAs). Because the list of Type A variables differs widely between plants, Table 3.3.11-1, in the accompanying LCO, contains no examples of Type A variables, except for those that may also be Category I.

Category I variables are the key variables deemed risk significant because they are needed to:

- Determine whether other systems important to safety are performing their intended functions,
- Provide information to the operators that will enable them to determine the potential for causing a gross breach of the barriers to radioactivity release, and
- Provide information regarding the release of radioactive materials to allow for early indication of the need to initiate action necessary to

## BASES

### BACKGROUND (continued)

protect the public and for an estimate of the magnitude of any impending threat.

These key variables are identified by plant specific Regulatory Guide 1.97 analyses (Ref. 1). These analyses identified the plant specific Type A and Category I variables and provided justification for deviating from the NRC proposed list of Category I variables.

---

#### - REVIEWER'S NOTE -

Table 3.3.11-1, in the accompanying LCO, provides a list of variables typical of those identified by plant specific Regulatory Guide 1.97 analyses. Table 3.3.11-1 in the plant specific Technical Specifications shall list all Type A and Category I variables identified by plant specific Regulatory Guide 1.97 analyses, as amended by NRC's Safety Evaluation Report (SER) (Ref. 4). The specific instrument Functions listed in Table 3.3.11-1 are discussed in the LCO Bases.

---

#### APPLICABLE SAFETY ANALYSES

The PAM instrumentation ensures the OPERABILITY of Regulatory Guide 1.97 Type A variables, so that the control room operating staff can:

- Perform the diagnosis specified in the emergency operating procedures. These variables are restricted to preplanned actions for the primary success path of DBAs and
- Take the specified, preplanned, manually controlled actions, for which no automatic control is provided, that are required for safety systems to accomplish their safety functions.

The PAM instrumentation also ensures OPERABILITY of Category I, non-Type A variables. This ensures the control room operating staff can:

- Determine whether systems important to safety are performing their intended functions,
- Determine the potential for causing a gross breach of the barriers to radioactivity release,
- Determine if a gross breach of a barrier has occurred, and
- Initiate action necessary to protect the public as well as to obtain an estimate of the magnitude of any impending threat.

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

PAM instrumentation that satisfies the definition of Type A in Regulatory Guide 1.97 meets Criterion 3 of 10 CFR 50.36(c)(2)(ii).

Category I, non-Type A PAM instruments are retained in the Specification because they are intended to assist operators in minimizing the consequences of accidents. Therefore, these Category I variables are important in reducing public risk.

---

#### LCO

LCO 3.3.11 requires two OPERABLE channels for all but one Function to ensure no single failure prevents the operators from being presented with the information necessary to determine the status of the plant and to bring the plant to, and maintain it in, a safe condition following that accident.

Furthermore, provision of two channels allows a CHANNEL CHECK during the post accident phase to confirm the validity of displayed information.

[ More than two channels may be required at some units if the Regulatory Guide 1.97 analysis determined that failure of one PAM channel results in information ambiguity (that is, the redundant displays disagree) that could lead operators to defeat or to fail to accomplish a required safety function. ]

The exception to the two channel requirement is Containment Isolation Valve Position. In this case, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of the passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

Listed below are discussions of the specified instrument Functions listed in Table 3.3.11-1. These discussions are intended as examples of what should be provided for each Function when the plant specific list is prepared.



## BASES

---

### LCO (continued)

1. [Logarithmic] Neutron Flux

Logarithmic] Neutron Flux indication is provided to verify reactor shutdown.

[ At this unit, the [Logarithmic] Neutron Flux PAM channels consist of the following: ]

2, 3. Reactor Coolant System (RCS) Hot and Cold Leg      Temperature

RCS Hot and Cold Leg Temperatures are Category I variables provided for verification of core cooling and long term surveillance.

Reactor outlet temperature inputs to the PAM are provided by two fast response resistance elements and associated transmitters in each loop. The channels provide indication over a range of 32°F to 700°F.

4. Reactor Coolant System Pressure (wide range)

RCS wide range pressure is a Category I variable provided for verification of core cooling and RCS integrity long term surveillance.

Wide range RCS loop pressure is measured by pressure transmitters with a span of 0 psig to 3000 psig. The pressure transmitters are located outside the containment. Redundant monitoring capability is provided by two trains of instrumentation. Control room indications are provided through the inadequate core cooling (ICC) plasma display. The ICC plasma display is the primary indication used by the operator during an accident. Therefore, the PAM instrumentation LCO deals specifically with this portion of the instrument channel.

In some plants, RCS pressure is a Type A variable because the operator uses this indication to monitor the cooldown of the RCS following a steam generator tube rupture or small break loss of coolant accident (LOCA). Operator actions to maintain a controlled cooldown, such as adjusting steam generator pressure or level, would use this indication. Furthermore, RCS pressure is one factor that may be used in decisions to terminate reactor coolant pump operation.

## BASES

---

### LCO (continued)

#### 5. Reactor Vessel Water Level

Reactor Vessel Water Level is provided for verification and long term surveillance of core cooling.

The Reactor Vessel Water Level monitoring system provides a direct measurement of the collapsed liquid level above the fuel alignment plate. The collapsed level represents the amount of liquid mass that is in the reactor vessel above the core. Measurement of the collapsed water level is selected because it is a direct indication of the water inventory. The collapsed level is obtained over the same temperature and pressure range as the saturation measurements, thereby encompassing all operating and accident conditions where it must function. Also, it functions during the recovery interval. Therefore, it is designed to survive the high steam temperature that may occur during the preceding core recovery interval.

The level range extends from the top of the vessel down to the top of the fuel alignment plate. The response time is short enough to track the level during small break LOCA events. The resolution is sufficient to show the initial level drop, the key locations near the hot leg elevation, and the lowest levels just above the alignment plate. This provides the operator with adequate indication to track the progression of the accident and to detect the consequences of its mitigating actions or the functionality of automatic equipment.

#### 6. Containment Sump Water Level (wide range)

Containment Sump Water Level is provided for verification and long term surveillance of RCS integrity.

[ For this unit, Containment Sump Water Level instrumentation consists of the following: ]

#### 7. Containment Pressure (wide range)

Containment Pressure is provided for verification of RCS and containment OPERABILITY.

[ For this unit, Containment Pressure instrumentation consists of the following: ]

BASES

---

LCO (continued)

8. Containment Isolation Valve Position

Containment Isolation Valve Position is provided for verification of containment OPERABILITY.

PCIV position is provided for verification of containment integrity. In the case of PCIV position, the important information is the isolation status of the containment penetration. The LCO requires one channel of valve position indication in the control room to be OPERABLE for each active PCIV in a containment penetration flow path, i.e., two total channels of PCIV position indication for a penetration flow path with two active valves. For containment penetrations with only one active PCIV having control room indication, Note (b) requires a single channel of valve position indication to be OPERABLE. This is sufficient to redundantly verify the isolation status of each isolable penetration via indicated status of the active valve, as applicable, and prior knowledge of passive valve or system boundary status. If a penetration flow path is isolated, position indication for the PCIV(s) in the associated penetration flow path is not needed to determine status. Therefore, the position indication for valves in an isolated penetration flow path is not required to be OPERABLE. Each penetration is treated separately and each penetration flow path is considered a separate function. Therefore, separate Condition entry is allowed for each inoperable penetration flow path.

[ For this unit, the PCIV position PAM instrumentation consists of the following: ]

9. Containment Area Radiation (high range)

Containment Area Radiation is provided to monitor for the potential of significant radiation releases and to provide release assessment for use by operators in determining the need to invoke site emergency plans.

[ For this unit, Containment Area Radiation instrumentation consists of the following: ]

10. Containment Hydrogen Monitors

Containment Hydrogen Monitors are provided to detect high hydrogen concentration conditions that represent a potential for

BASES

---

LCO (continued)

containment breach. This variable is also important in verifying the adequacy of mitigating actions.

[ For this unit, Containment Hydrogen instrumentation consists of the following: ]

11. Pressurizer Level

Pressurizer Level is used to determine whether to terminate safety injection (SI), if still in progress, or to reinitiate SI if it has been stopped. Knowledge of pressurizer water level is also used to verify the plant conditions necessary to establish natural circulation in the RCS and to verify that the plant is maintained in a safe shutdown condition.

[ For this unit, Pressurizer Level instrumentation consists of the following: ]

12. Steam Generator Water Level

Steam Generator Water Level is provided to monitor operation of decay heat removal via the steam generators. The Category I indication of steam generator level is the extended startup range level instrumentation. The extended startup range level covers a span of 6 inches to 394 inches above the lower tubesheet. The measured differential pressure is displayed in inches of water at 68°F. Temperature compensation of this indication is performed manually by the operator. Redundant monitoring capability is provided by two trains of instrumentation. The uncompensated level signal is input to the plant computer, a control room indicator, and the [Auxiliary Feedwater (AFW)] Control System.

At some plants, operator action is based on the control room indication of Steam Generator Water Level. The RCS response during a design basis small break LOCA is dependent on the break size. For a certain range of break sizes, the boiler condenser mode of heat transfer is necessary to remove decay heat. At these plants, extended startup range level is a Type A variable because the operator must manually raise and control the steam generator level to establish boiler condenser heat transfer. Operator action is initiated on a loss of subcooled margin. Feedwater flow is increased until the indicated extended startup range level reaches the boiler condenser setpoint.

BASES

---

LCO (continued)

13. Condensate Storage Tank (CST) Level

CST Level is provided to ensure water supply for [AFW]. The CST provides the ensured safety grade water supply for the [AFW] System. The CST consists of two identical tanks connected by a common outlet header. Inventory is monitored by a 0 to 144 inch level indication for each tank. CST Level is displayed on a control room indicator, strip chart recorder, and plant computer. In addition, a control room annunciator alarms on low level.

At some plants, CST Level is considered a Type A variable because the control room meter and annunciator are considered the primary indication used by the operator. The DBAs that require [AFW] are the loss of electric power, steam line break (SLB), and small break LOCA. The CST is the initial source of water for the [AFW] System. However, as the CST is depleted, manual operator action is necessary to replenish the CST or align suction to the [AFW] pumps from the hotwell.

14, 15, 16, 17. Core Exit Temperature

Core Exit Temperature is provided for verification and long term surveillance of core cooling.

An evaluation was made of the minimum number of valid core exit thermocouples necessary for inadequate core cooling detection. The evaluation determined the reduced complement of core exit thermocouples necessary to detect initial core uncover and trend the ensuing core heatup. The evaluations account for core nonuniformities including incore effects of the radial decay power distribution and excore effects of condensate runback in the hot legs and nonuniform inlet temperatures. Based on these evaluations, adequate or inadequate core cooling detection is ensured with two valid core exit thermocouples per quadrant.

The design of the Incore Instrumentation System includes a Type K (chromel alumel) thermocouple within each of the 56 incore instrument detector assemblies.

The junction of each thermocouple is located a few inches above the fuel assembly, inside a structure that supports and shields the incore instrument detector assembly string from flow forces in the outlet

## BASES

---

### LCO (continued)

plenum region. These core exit thermocouples monitor the temperature of the reactor coolant as it exits the fuel assemblies.

The core exit thermocouples have a usable temperature range from 32°F to 2300°F, although accuracy is reduced at temperatures above 1800°F.

#### 18. [Auxiliary Feedwater (AFW)] Flow

[AFW] Flow is provided to monitor operation of decay heat removal via the steam generators.

The [AFW] Flow to each steam generator is determined from a differential pressure measurement calibrated to a span of 0 gpm to 1200 gpm. Redundant monitoring capability is provided by two independent trains of instrumentation for each steam generator. Each differential pressure transmitter provides an input to a control room indicator and the plant computer. Since the primary indication used by the operator during an accident is the control room indicator, the PAM instrumentation Specification deals specifically with this portion of the instrument channel.

At some plants [AFW] Flow is a Type A variable because operator action is required to throttle flow during an SLB accident in order to prevent the [AFW] pumps from operating in runout conditions. [AFW] Flow is also used by the operator to verify that the [AFW] System is delivering the correct flow to each steam generator. However, the primary indication used by the operator to ensure an adequate inventory is steam generator level.

Two channels are required to be OPERABLE for all but one Function. Two OPERABLE channels ensure that no single failure, within either the PAM instrumentation or its auxiliary supporting features or power sources (concurrent with the failures that are a condition of or result from a specific accident), prevents the operators from being presented the information necessary for them to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident.

In Table 3.3.11-1 the exception to the two channel requirement is Containment Isolation Valve Position.

## BASES

---

### LCO (continued)

Two OPERABLE channels of core exit thermocouples are required for each channel in each quadrant to provide indication of radial distribution of the coolant temperature rise across representative regions of the core. Power distribution symmetry was considered in determining the specific number and locations provided for diagnosis of local core problems. Therefore, two randomly selected thermocouples may not be sufficient to meet the two thermocouples per channel requirement in any quadrant. The two thermocouples in each channel must meet the additional requirement that one be located near the center of the core and the other near the core perimeter, such that the pair of core exit thermocouples indicate the radial temperature gradient across their core quadrant. Plant specific evaluations in response to Item II.F.2 of NUREG-0737 should have identified the thermocouple pairings that satisfy these requirements. Two sets of two thermocouples in each quadrant ensure a single failure will not disable the ability to determine the radial temperature gradient.

For loop and steam generator related variables, the required information is individual loop temperature and individual steam generator level. In these cases two channels are required to be OPERABLE for each loop of steam generator to redundantly provide the necessary information.

In the case of Containment Isolation Valve Position, the important information is the status of the containment penetrations. The LCO requires one position indicator for each active containment isolation valve. This is sufficient to redundantly verify the isolation status of each isolable penetration either via indicated status of the active valve and prior knowledge of the passive valve or via system boundary status. If a normally active containment isolation valve is known to be closed and deactivated, position indication is not needed to determine status. Therefore, the position indication for valves in this state is not required to be OPERABLE.

---

### APPLICABILITY

The PAM instrumentation LCO is applicable in MODES 1, 2, and 3. These variables are related to the diagnosis and preplanned actions required to mitigate DBAs. The applicable DBAs are assumed to occur in MODES 1, 2, and 3. In MODES 4, 5, and 6, plant conditions are such that the likelihood of an event occurring that would require PAM instrumentation is low; therefore, PAM instrumentation is not required to be OPERABLE in these MODES.

## BASES

---

### ACTIONS

Note 1 has been added in the ACTIONS to exclude the MODE change restriction of LCO 3.0.4. This exception allows entry into the applicable MODE while relying on the ACTIONS, even though the ACTIONS may eventually require plant shutdown. This exception is acceptable due to the passive function of the instruments, the operator's ability to monitor an accident using alternate instruments and methods, and the low probability of an event requiring these instruments.

Note 2 has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification may be entered independently for each Function listed in Table 3.3.11-1. 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

When one or more Functions have one required channel that is inoperable, the required inoperable channel must be restored to OPERABLE status within 30 days. The 30 day Completion Time is based on operating experience and takes into account the remaining OPERABLE channel (or in the case of a Function that has only one required channel, other non-Regulatory Guide 1.97 instrument channels to monitor the Function), the passive nature of the instrument (no critical automatic action is assumed to occur from these instruments), and the low probability of an event requiring PAM instrumentation during this interval.

#### B.1

This Required Action specifies initiation of actions in accordance with Specification 5.6.7, which requires a written report to be submitted to the Nuclear Regulatory Commission. This report discusses the results of the root cause evaluation of the inoperability and identifies proposed restorative Required Actions. This Required Action is appropriate in lieu of a shutdown requirement, given the likelihood of plant conditions that would require information provided by this instrumentation. Also, alternative Required Actions are identified before a loss of functional capability condition occurs.

#### C.1

When one or more Functions have two required channels inoperable (i.e., two channels inoperable in the same Function), one channel in the Function should be restored to OPERABLE status within 7 days. The



## BASES

---

### ACTIONS (continued)

Completion Time of 7 days is based on the relatively low probability of an event requiring PAM instrumentation operation and the availability of alternate means to obtain the required information. Continuous operation with two required channels inoperable in a Function is not acceptable because the alternate indications may not fully meet all performance qualification requirements applied to the PAM instrumentation. Therefore, requiring restoration of one inoperable channel of the Function limits the risk that the PAM Function will be in a degraded condition should an accident occur.

#### D.1

When two required hydrogen monitor channels are inoperable, Required Action D.1 requires one channel to be restored to OPERABLE status. This Required Action restores the monitoring capability of the hydrogen monitor. The 72 hour Completion Time is based on the relatively low probability of an event requiring hydrogen monitoring and the availability of alternative means to obtain the required information. Continuous operation with two required channels inoperable is not acceptable because alternate indications are not available.

#### E.1

This Required Action directs entry into the appropriate Condition referenced in Table 3.3.11-1. The applicable Condition referenced in the Table is Function dependent. Each time Required Action C.1 or D.1 is not met, and the associated Completion Time has expired, Condition E is entered for that channel and provides for transfer to the appropriate subsequent Condition.

#### F.1 and F.2

If the Required Action and associated Completion Time of Condition C are not met, and Table 3.3.11-1 directs entry into Condition F, the plant must be brought to a MODE in which the requirements of this LCO do 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.

BASES

---

ACTIONS (continued)

G.1

[ At this plant, alternate means of monitoring Reactor Vessel Water Level and Containment Area Radiation have been developed and tested. These alternate means may be temporarily installed if the normal PAM channel cannot be restored to OPERABLE status within the allotted time. If these alternate means are used, the Required Action is not to shut down the plant, but rather to follow the directions of Specification 5.6.7. The report provided to the NRC should discuss the alternate means used, describe the degree to which the alternate means are equivalent to the installed PAM channels, justify the areas in which they are not equivalent, and provide a schedule for restoring the normal PAM channels. ]

---

SURVEILLANCE  
REQUIREMENTS

A Note at the beginning of the Surveillance Requirements specifies that the following SRs apply to each PAM instrumentation Function in Table 3.3.11-1.

SR 3.3.11.1

Performance of the CHANNEL CHECK once every 31 days 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. A 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 times when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

The Frequency of 31 days is based upon plant operating experience with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given Function in any 31 day interval is a rare event. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel during normal operational use of the displays associated with this LCO's required channels.

#### SR 3.3.11.2

A CHANNEL CALIBRATION is performed every [18] months or approximately every refueling. CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies the channel responds to the measured parameter within the necessary range and accuracy. A Note allows exclusion of neutron detectors from the CHANNEL CALIBRATION.

[ At this unit, CHANNEL CALIBRATION shall find measurement errors are within the following acceptance criteria: ]

For the Containment Area Radiation instrumentation, a CHANNEL CALIBRATION may consist of an electronic calibration of the channel, not including the detector, for range decades above 10 R/hr, and a one point calibration check of the detector below 10 R/hr with a gamma source.

Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the resistance temperature detectors (RTD) sensors is accomplished by an in-place cross calibration that compares the other sensing elements with the recently installed sensing element.

Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the Core Exit thermocouple sensors is accomplished by an in-place cross calibration that compares the other sensing elements with the recently installed sensing element.

The Frequency is based upon operating experience and consistency with the typical industry refueling cycle and is justified by an [18] month calibration interval for the determination of the magnitude of equipment drift.

**BASES**

---

**REFERENCES**

1. Plant specific document (e.g., FSAR, NRC Regulatory Guide 1.97, SER letter).
  2. Regulatory Guide 1.97.
  3. NUREG-0737, Supplement 1.
  4. NRC Safety Evaluation Report (SER).
- 
-

### B 3.3 INSTRUMENTATION

#### B 3.3.12 Remote Shutdown System (Analog)

##### BASES

---

##### BACKGROUND

The Remote Shutdown System provides the control room operator with sufficient instrumentation and controls to place and maintain the unit in a safe shutdown condition from a location other than the control room. This capability is necessary to protect against the possibility that the control room becomes inaccessible. A safe shutdown condition is defined as MODE 3. With the unit in MODE 3, the [Auxiliary Feedwater (AFW) System] and the steam generator safety valves or the steam generator atmospheric dump valves can be used to remove core decay heat and meet all safety requirements. The long term supply of water for the [AFW System] and the ability to borate the Reactor Coolant System (RCS) from outside the control room allow extended operation in MODE 3.

In the event that the control room becomes inaccessible, the operators can establish control at the remote shutdown panel and place and maintain the unit in MODE 3. Not all controls and necessary transfer switches are located at the remote shutdown panel. Some controls and transfer switches will be operated locally at the switchgear, motor control panels, or other local stations. The unit automatically reaches MODE 3 following a unit shutdown and can be maintained safely in MODE 3 for an extended period of time.

The OPERABILITY of the Remote Shutdown System control and instrumentation Functions ensures that there is sufficient information available on selected plant parameters to place and maintain the plant in MODE 3, should the control room become inaccessible.

---

##### APPLICABLE SAFETY ANALYSES

The Remote Shutdown System is required to provide equipment at appropriate locations outside the control room with a capability to promptly shut down and maintain the plant in a safe condition in MODE 3.

The criteria governing the design and the specific system requirements of the Remote Shutdown System are located in 10 CFR 50, Appendix A, GDC 19, and Appendix R (Ref. 1).

The Remote Shutdown System satisfies Criterion 4 of 10 CFR 50.36(c)(2)(ii).

## BASES

---

### LCO

The Remote Shutdown System LCO provides the requirements for the OPERABILITY of the instrumentation and controls necessary to place and maintain the unit in MODE 3 from a location other than the control room. The instrumentation and controls required are listed in Table B 3.3.12-1.

The controls, instrumentation, and transfer switches are those required for:

- Core Reactivity Control (initial and long term),
- RCS Pressure Control,
- Decay Heat Removal via the [AFW System] and the safety valves or steam generator ADVs,
- RCS Inventory Control via charging flow, and
- Safety support systems for the above Functions, as well as service water, component cooling water, and onsite power including the diesel generators.

A Function of a Remote Shutdown System is OPERABLE if all instrument and control channels needed to support the remote shutdown Functions are OPERABLE. In some cases, Table B 3.3.12-1 may indicate that the required information or control capability is available from several alternate sources. In these cases, the Function is OPERABLE as long as one channel of any of the alternate information or control sources for each Function is OPERABLE.

The Remote Shutdown System instrumentation and control circuits covered by this LCO do not need to be energized to be considered OPERABLE. This LCO is intended to ensure that the instrument and control circuits will be OPERABLE if plant conditions require that the Remote Shutdown System be placed in operation.

---

### APPLICABILITY

The Remote Shutdown System LCO is applicable in MODES 1, 2, and 3. This is required so that the unit can be placed and maintained in MODE 3 for an extended period of time from a location other than the control room.

This LCO is not applicable in MODE 4, 5, or 6. In these MODES, the unit is already subcritical and in the condition of reduced RCS energy. Under these conditions, considerable time is available to restore necessary

BASES

---

APPLICABILITY (continued)

instrument control Functions if control room instruments or control become unavailable.

---

ACTIONS

A Note has been included that excludes the MODE change restrictions of LCO 3.0.4. This exception allows entry into an applicable MODE while relying on the ACTIONS, even though the ACTIONS may eventually require a plant shutdown. This is acceptable due to the low probability of an event requiring this system. The Remote Shutdown System equipment can generally be repaired during operation without significant risk of spurious trip.

A Remote Shutdown System division is inoperable when each Function is not accomplished by at least one designated Remote Shutdown System channel that satisfies the OPERABILITY criteria for the channel's Function. These criteria are outlined in the LCO section of the Bases.

Note 2 has been added in the ACTIONS to clarify the application of Completion Time rules. The Conditions of this Specification 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

Condition A addresses the situation where one or more channels of the Remote Shutdown System are inoperable. This includes the control and transfer switches for any required Function .

The Required Action is to restore the divisions to OPERABLE status within 30 days. The Completion Time is based on operating experience and the low probability of an event that would require evacuation of the control room.

B.1 and B.2

If the Required Action and associated Completion Time of Condition A 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 MODE from full power conditions in an orderly manner and without challenging plant systems.

---

## BASES

---

### SURVEILLANCE REQUIREMENTS [ SR 3.3.12.1

Performance of the CHANNEL CHECK once every 31 days 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 instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. A 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 limit. As specified in the Surveillance, a CHANNEL CHECK is only required for those channels that are normally energized. If the channels are within the criteria, it is an indication that the channels are OPERABLE. If the channels are normally off scale during times when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency is based on plant operating experience that demonstrates channel failure is rare. ]

### SR 3.3.12.2

SR 3.3.12.2 verifies that each required Remote Shutdown System transfer switch and control circuit performs its intended function. This verification is performed from the reactor shutdown panel and locally, as appropriate. Operation of the equipment from the remote shutdown panel is not necessary. The Surveillance can be satisfied by performance of a continuity check. This will ensure that if the control room becomes inaccessible, the plant can be placed and maintained in MODE 3 from the reactor shutdown panel and the local control stations. 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 demonstrates that Remote Shutdown System control channels seldom fail to pass the Surveillance when performed at a Frequency of once every [18] months.



BASES

---

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.12.3

CHANNEL CALIBRATION is a complete check of the instrument channel including the sensor. The Surveillance verifies that the channel responds to the measured parameter within the necessary range and accuracy. Whenever a sensing element is replaced, the next required CHANNEL CALIBRATION of the resistance temperature detectors (RTD) sensors is accomplished by an in-place cross calibration that compares the other sensing elements with the recently installed sensing element.

The 18 month Frequency is based upon 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.

The SR is modified by a Note, which excludes neutron detectors from the CHANNEL CALIBRATION.

[ SR 3.3.12.4

SR 3.3.12.4 is the performance of a CHANNEL FUNCTIONAL TEST every 18 months. 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 should verify the OPERABILITY of the reactor trip circuit breaker (RTCB) open/closed indication on the remote shutdown panels by actuating the RTCBs. The Frequency of 18 months was chosen because the RTCBs cannot be exercised while the unit is at power. Operating experience has shown that these components usually pass the Surveillance when performed at a Frequency of once every 18 months. Therefore, the Frequency was concluded to be acceptable from a reliability standpoint. ]

---

REFERENCES

1. 10 CFR 50, Appendix A, GDC 19, and Appendix R.
  2. NRC Safety Evaluation Report (SER).
-

Table B 3.3.12-1 (page 1 of 1)  
Remote Shutdown System Instrumentation and Controls

- NOTE -

This Table is for illustration purposes only. It does not attempt to encompass every Function used at every unit, but does contain the types of Functions commonly found.

FUNCTION/INSTRUMENT OR CONTROL PARAMETER	REQUIRED NUMBER OF DIVISIONS
1. Reactivity Control	
a. Log Power Neutron Flux	[1]
b. Source Range Neutron Flux	[1]
c. Reactor Trip Circuit Breaker Position	[1 per trip breaker]
d. Manual Reactor Trip	[2]
2. Reactor Coolant System Pressure Control	
a. Pressurizer Pressure or RCS Wide Range Pressure	[1]
b. Pressurizer Power Operated Relief Valve Control and Block Valve Control	[1, controls must be for power operated relief valve and block valves on same line]
3. Decay Heat Removal via Steam Generators	
a. Reactor Coolant\ Hot Leg Temperature	[1 per loop]
b. Reactor Coolant Cold Leg Temperature	[1 per loop]
c. Auxiliary Feedwater Controls	[1]
d. Steam Generator Pressure	[1 per steam generator]
e. Steam Generator Level or Auxiliary Feedwater Flow	[1 per steam generator]
f. Condensate Storage Tank Level	[1]
4. Reactor Coolant System Inventory Control	
a. Pressurizer Level	[1]
b. Reactor Coolant Charging Pump Controls	[1]

- REVIEWER'S NOTE -

The number of channels that fulfill GDC 19 requirements for the number of OPERABLE channels required depends upon the plant's licensing basis as described in the NRC plant specific Safety Evaluation Report (SER) (Ref. 2). Generally, two divisions are required to be OPERABLE. However, only one channel is required if the plant has justified such a design and the NRC's SER accepted the justification.

## B 3.3 INSTRUMENTATION

### B 3.3.13 [Logarithmic] Power Monitoring Channels (Analog)

#### BASES

---

**BACKGROUND** The [logarithmic] power monitoring channels provide neutron flux power indication from < 1E-7% RTP to > 100% RTP. They also provide reactor protection when the reactor trip circuit breakers (RTCBs) are shut, in the form of a Power Rate of Change - High trip (analog plants) or a [Logarithmic] Power Level - High trip (digital plants).

This LCO addresses MODES 3, 4, and 5 with the RTCBs open. When the RTCBs are shut, the [logarithmic] power monitoring channels are addressed by LCO 3.3.2, "Reactor Protective System (RPS) Instrumentation - Shutdown."

When the RTCBs are open, two of the four wide range power channels must be available to monitor neutron flux power. In this application, the RPS channels need not be OPERABLE since the reactor trip Function is not required. By monitoring neutron flux power when the RTCBs are open, loss of SDM caused by boron dilution can be detected as an increase in flux. Alarms are also provided when power increases above the fixed bistable setpoints. For plants employing separate post accident, [logarithmic] nuclear instrumentation channels with adequate range, these can be substituted for the [logarithmic] power range channels. Two channels must be OPERABLE to provide single failure protection and to facilitate detection of channel failure by providing CHANNEL CHECK capability.

---

**APPLICABLE SAFETY ANALYSES** The [logarithmic] power monitoring channels are necessary to monitor core reactivity changes. They are the primary means for detecting and triggering operator actions to respond to reactivity transients initiated from conditions in which the RPS is not required to be OPERABLE. They also trigger operator actions to anticipate RPS actuation in the event of reactivity transients starting from shutdown or low power conditions. The [logarithmic] power monitoring channel's LCO requirements support compliance with 10 CFR 50, Appendix A, GDC 13 (Ref. 1). The FSAR, Chapters [7] and [15] (Refs. 2 and 3, respectively), describes the specific [logarithmic] power monitoring channel features that are critical to comply with the GDC.

The OPERABILITY of [logarithmic] power monitoring channels is necessary to meet the assumptions of the safety analyses and provide for the mitigation of accident and transient conditions.

---

BASES

---

APPLICABLE SAFETY ANALYSES (continued)

The [logarithmic] power monitoring channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

---

LCO

The LCO on the [logarithmic] power monitoring channels ensures that adequate information is available to verify core reactivity conditions while shut down.

A minimum of two [logarithmic] power monitoring channels are required to be OPERABLE. Some plants may have either four or six channels capable of performing this function. In these cases, multiple failures may be tolerated while the plants are still complying with LCO requirements.

---

APPLICABILITY

In MODES 3, 4, and 5, with RTCBs open or the Control Element Assembly (CEA) Drive System not capable of CEA withdrawal, [logarithmic] power monitoring channels must be OPERABLE to monitor core power for reactivity changes. In MODES 1 and 2, and in MODES 3, 4, and 5 with the RTCBs shut and the CEAs capable of withdrawal, the [logarithmic] power monitoring channels are addressed as part of the RPS in LCO 3.3.1, "Reactor Protective System (RPS) Instrumentation - Operating."

The requirements for source range neutron flux monitoring in MODE 6 are addressed in LCO 3.9.2, "Nuclear Instrumentation." The source range nuclear instrumentation channels provide neutron flux coverage extending an additional one to two decades below the [logarithmic] channels for use during refueling, when neutron flux may be extremely low. They are built into the [logarithmic] neutron flux channels in the analog plants and in many of the post accident channels used in both the digital and analog plants.

---

ACTIONS

A.1 and A.2

With one required channel inoperable, it may not be possible to perform a CHANNEL CHECK to verify that the other required channel is OPERABLE. Therefore, with one or more required channels inoperable, the [logarithmic] power monitoring Function cannot be reliably performed. Consequently, the Required Actions are the same for one required channel inoperable or more than one required channel inoperable. The absence of reliable neutron flux indication makes it difficult to ensure SDM is maintained. Required Action [ ] is modified by a note to indicate that normal plant control operations that individually add limited positive reactivity (e.g., temperature or boron fluctuations associated with RCS

---

## BASES

---

### ACTIONS (continued)

inventory management or temperature control) are not precluded by this Action, provided they are accounted for in the calculated SDM.

SDM must be verified periodically to ensure that it is being maintained. Both required channels must be restored as soon as possible. The initial Completion Time of 4 hours and once every 12 hours thereafter to perform SDM verification takes into consideration that Required Action A.1 eliminates many of the means by which SDM can be reduced. These Completion Times are also based on operating experience in performing the Required Actions and the fact that plant conditions will change slowly.

---

### SURVEILLANCE REQUIREMENTS

#### SR 3.3.13.1

SR 3.3.13.1 is the performance of a CHANNEL CHECK on each required channel every 12 hours. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based upon the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or 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 and should be based on a combination of the channel instrument uncertainties including control 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. 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 the rarity of channel failure. Since the probability of two random failures in redundant channels in any 12 hour period is extremely low, CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.13.2

A CHANNEL FUNCTIONAL TEST is performed every [92] days to ensure that the entire channel is capable of properly indicating neutron flux. 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. Internal test circuitry is used to feed preadjusted test signals into the preamplifier to verify channel alignment. It is not necessary to test the detector, because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This Frequency is the same as that employed for the same channels in the other applicable MODES. [At this unit, the channel trip Functions tested by the CHANNEL FUNCTIONAL TEST are as follows:]

SR 3.3.13.3

SR 3.3.13.3 is the performance of a CHANNEL CALIBRATION. A CHANNEL CALIBRATION is performed every [18] months. The Surveillance is a complete check and readjustment of the [logarithmic] power channel from the preamplifier input through to the remote indicators. 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.

This SR is modified by a Note to indicate that it is not necessary to test the detector because generating a meaningful test signal is difficult; the detectors are of simple construction, and any failures in the detectors will be apparent as change in channel output. This Frequency is the same as that employed for the same channels in the other applicable MODES.

---

REFERENCES

1. 10 CFR 50, Appendix A, GDC 13.
2. FSAR, Chapter [7].

BASES

---

REFERENCES (continued)

---

3. FSAR, Chapter [15].

---

---

## 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 CFR50.36 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. 11) and could be used to meet the requirement that they be contained in the technical specifications.

Technical specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. Operable is defined

---



## BASES

---

### BACKGROUND (continued)

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 Value 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 Safety Limit is not exceeded at any given point of time as long as the device has 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

## BASES

---

### BACKGROUND (continued)

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. 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.

The RPS is segmented into four interconnected modules. These modules are:

- Measurement channels,
- Bistable trip units,
- RPS Logic, and

## BASES

---

### BACKGROUND (continued)

- 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.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of 10 CFR 50, Appendix A, GDC 21

## BASES

---

### BACKGROUND (continued)

(Ref. 1). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic. Thus, even with a channel inoperable, no single additional failure in the RPS can either cause an inadvertent trip 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. 3).

---

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. 4).

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,
- Excore neutron flux levels,

## BASES

---

### BACKGROUND (continued)

- 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  $\Delta T$  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. 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 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. 7). The nominal trip setpoint entered into the bistable is normally still more conservative than

## BASES

---

### BACKGROUND (continued)

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. 8), 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.

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

## BASES

---

### BACKGROUND (continued)

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 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)

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.

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

## BASES

---

### BACKGROUND (continued)

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. 8), 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.

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

---

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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 Steam Generator #1 Level - High, Steam Generator #2 Level - High, and the Loss of Load. These trips are purely equipment protective, and their 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.

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  $< 1\text{E-4}\%$ . 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."

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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.

#### 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.

BASES

---

APPLICABLE SAFETY ANALYSES (continued)

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. Steam Generator Level - High

The Steam Generator #1 Level - High and Steam Generator #2 Level - High trips are provided to protect the turbine from excessive moisture carryover in case of a steam generator overfill event.

12, 13. 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.

14. 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

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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.

#### 15. 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.

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.

BASES

---

APPLICABLE SAFETY ANALYSES (continued)

16. 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,
- CEA Misoperation; Part Length CEA Subgroup Drop,
- Primary Sample or Instrument Line Break, and

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

- 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).

---

## 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

---



## BASES

---

### LCO (continued)

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. 7).

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.

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

## BASES

---

### LCO (continued)

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.

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

## BASES

---

### LCO (continued)

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.

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

## BASES

---

### LCO (continued)

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 and the Steam Generator (#1 and #2) Level - High trip may be manually bypassed simultaneously when cold leg temperature is below the specified limit to allow for CEA withdrawal during testing. The bypass is automatically removed when cold leg temperature reaches 200°F.

#### 10, 11. Steam Generator Level - High

This LCO requires four channels of Steam Generator #1 Level - High and Steam Generator #2 Level - High to be OPERABLE in MODES 1 and 2.

The Allowable Value is high enough to allow for normal plant operation and transients without causing a reactor trip. It is set low enough to ensure a reactor trip occurs before the level reaches the steam dryers. Having steam generator water level at the trip value is indicative of the plant not being operated in a controlled manner.

This trip and the Steam Generator Level - Low trip may be manually bypassed simultaneously when cold leg temperature is below the specified limit to allow for CEA withdrawal during testing with the steam generators in wet layup. The bypass is automatically removed when cold leg temperature reaches 200°F. Below 200°F the plant is in shutdown cooling; therefore, the steam generators are not required for heat removal.

## BASES

---

### LCO (continued)

#### 12, 13. 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.

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.

#### 14. 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  $\leq 55\%$  RTP. Therefore, the Loss of Load trip may be bypassed when reactor power is  $\leq 55\%$  RTP, as sensed by the power range nuclear instrumentation. Both the bypass and bypass removal, when above 55% power, are automatically performed.

BASES

---

LCO (continued)

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.

15. 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.

16. 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.

## BASES

---

### LCO (continued)

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.

#### 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	<p>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:</p> <ul style="list-style-type: none"><li>• 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.</li></ul> <p>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.</p>
ACTIONS	<p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>



## BASES

---

### ACTIONS (continued)

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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES, even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

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

## BASES

---

### ACTIONS (continued)

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 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)

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

#### 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.

BASES

---

ACTIONS (continued)

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.

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.

## 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.

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  $\geq 70\%$  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  $\geq 20\%$ . The Linear Power Level signal and the CPC addressable constant multipliers are adjusted to make the CPC  $\Delta T$  power and nuclear power calculations agree with the calorimetric calculation if the absolute difference is  $\geq 2\%$ . 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

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  $\geq 70\%$  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.

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

The 31 day Frequency is adequate because the demonstrated long term drift of the instrument channels is minimal.

#### 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 8. 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 [9].

#### 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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 3.3.4. 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. 9).

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. 9). 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 [9]. 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 [9].

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  $\leq 70\%$  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 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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. 9). 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  $n \times 18$  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. {10 - analog and digital 3.3.1, analog 3.3.4/11 -

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

digital 3.3.5} 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. 10 CFR 50, Appendix A, GDC 21.
  2. 10 CFR 100.
  3. NRC Safety Evaluation Report.
  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. 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."
  11. Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."
-

### 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 Steam Generator Water Level - High and the Loss of Load. The Steam Generator Water Level - High and the Loss of Load trips are

BASES

---

APPLICABLE SAFETY ANALYSES (continued)

purely equipment protective, and their use minimizes the potential for equipment damage.

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  $1\text{E-}4\%$  to allow the reactor to be brought to power during a reactor startup. This bypass is automatically removed when logarithmic power decreases below  $1\text{E-}4\%$ . Above  $1\text{E-}4\%$ , 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  $> 1\text{E-}4\%$ , and the bypass is automatically removed when logarithmic power is  $\leq 1\text{E-}4\%$ .

## 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 .

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.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

#### 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

---

### ACTIONS (continued)

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. Completion Times are consistent with Condition B.

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

#### 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.

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

---

**- 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).

---

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



## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

compensated for by performing the daily calorimetric calibration (SR 3.3.1.4).

#### 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  $n \times 18$  months, where  $n$  is the number of channels in the Function. The [18] month Frequency is based upon operating experience, which has shown that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences. Also, response times cannot be determined at power, since equipment operation is required. Testing may be performed in one measurement or in overlapping segments, with verification that all components are tested.

---

#### 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 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.

## BASES

---

### BACKGROUND (continued)

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,
- 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

## BASES

---

### BACKGROUND (continued)

the two reed switch position transmitters on each CEA, so that the position of all CEAs is independently monitored by both CEACs.

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.

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

## BASES

---

### ACTIONS (continued)

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.

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.



## 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 3.3.3.2

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.

#### 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.

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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.

#### 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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 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.

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

## 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.

---

#### **- 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

## BASES

---

### BACKGROUND (continued)

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).

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



## BASES

---

### BACKGROUND (continued)

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.

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.

## BASES

---

### BACKGROUND (continued)

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.

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.

## BASES

---

### BACKGROUND (continued)

It is possible to change the two-out-of-four ESFAS logic to a two-out-of-three logic for a given input parameter in one channel at a time by trip channel bypassing select portions of the Matrix Logic. Trip channel bypassing a bistable effectively shorts the bistable relay contacts in the three matrices associated with that channel. Thus, the bistables will function normally, producing normal trip indication and annunciation, but ESFAS actuation will not occur since the bypassed channel is effectively removed from the coincidence logic. Trip channel bypassing can be simultaneously performed 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.

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

## BASES

---

### BACKGROUND (continued)

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.

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

---

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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.

#### 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).

## BASES

---

### APPLICABLE SAFETY ANALYSES (continued)

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:

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

---

## BASES

---

### LCO (continued)

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.

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.

## BASES

---

### LCO (continued)

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.

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



## BASES

---

### LCO (continued)

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. 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.

## BASES

---

### LCO (continued)

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.

#### 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.

## BASES

---

### LCO (continued)

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).

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.

BASES

---

LCO (continued)

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.

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

## BASES

---

### LCO (continued)

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.

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

## BASES

---

### LCO (continued)

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.

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.

---

## 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. 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
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

BASES

---

ACTIONS (continued)

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.

B.1

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

Condition B applies to the failure of two channels of one or more input parameters in the following ESFAS automatic trip Functions:



BASES

---

ACTIONS (continued)

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.

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.

## BASES

---

### ACTIONS (continued)

#### 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

The Required Action is modified by a Note stating that LCO 3.0.4 is not applicable. The Note was added to allow the changing of MODES even though two channels are inoperable, with one channel bypassed and one tripped. In this configuration, the protection system is in a one-out-of-two logic, which is adequate to ensure that no random failure will prevent protection system operation.

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, the associated ESFAS channel may be considered OPERABLE only if the bypass is not in effect. 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.

#### 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

## BASES

---

### ACTIONS (continued)

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.

#### 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

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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].

#### 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].

## BASES

---

### SURVEILLANCE REQUIREMENTS (continued)

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, "Elimination of Pressure Sensor Response Time Testing Requirements," Ref. {10 - analog and digital 3.3.1, analog 3.3.4/11 - digital 3.3.5} 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.

BASES

---

SURVEILLANCE REQUIREMENTS (continued)

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).

---

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].

**BASES**

---

**REFERENCES (continued)**

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."
-