

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. This is achieved by specifying limiting safety system settings (LSSS) in terms of parameters directly monitored by the ESFAS, as well as LCOs on other system parameters and equipment performance. The subset of LSSS that directly protect against violating the Reactor Core Safety Limits or the Reactor Coolant System (RCS) pressure boundary Safety Limits during anticipated operational occurrences (AOOs) are referred to as Safety Limit LSSS (SL-LSSS).

10 CFR 50.36(c)(1)(ii)(A) requires that TSs include LSSSs for variables that have significant safety functions. For variables on which a SL has been placed, the LSSS must be chosen to initiate automatic protective action to correct abnormal situations before the SL is exceeded. ~~Technical Specifications are required by 10 CFR 50.36 to contain LSSS defined by the regulation as "...settings for automatic protective devices...so chosen that automatic protective actions will correct the abnormal situation before a Safety Limit (SL) is exceeded."~~ The Analytical Limit is the limit of the process variable at which a safety action is initiated, as established by the safety analysis, to ensure that an SL is not exceeded. Any automatic protection action that occurs on reaching the Analytical 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 Analytical Limit to account for instrument loop uncertainties related to the setting at which the automatic protective action would actually occur.

----- REVIEWER'S NOTE -----
The term "Limiting Trip Setpoint (LTSP)" is generic terminology for the setpoint value calculated by means of the plant-specific setpoint methodology documented in a document controlled under 10 CFR 50.59. The term Limiting Trip Setpoint indicates that no additional margin has been added between the Analytical Limit and the calculated trip setting. Where margin is added between the Analytical Limit and trip setpoint, the term Nominal Trip Setpoint (NTSP) is preferred. The trip setpoint (field setting) may be more conservative than the Limiting or Nominal Trip Setpoint. Where the [LTSP] is not included in Table 3.3.5-1 for the purpose of compliance with 10 CFR 50.36, the plant-specific term for the Limiting or Nominal Trip Setpoint must be cited in Note c of Table 3.3.5-1. The brackets indicate plant-specific terms may apply, as reviewed and

approved by the NRC. The as-found and as-left tolerances will apply to the actual setpoint implemented in the Surveillance procedures to confirm channel performance.

Licensees are to insert the name of the document(s) controlled under 10 CFR 50.59 that contain the [LTSP] and the methodology for calculating the as-left and as-found tolerances, for the phrase "[a document controlled under 10 CFR 50.59]" in the specifications.

The [Limiting Trip Setpoint (LTSP)] is a predetermined setting for a protective device chosen to ensure automatic actuation prior to the process variable reaching the Analytical Limit and thus ensuring that the SL would not be exceeded. As such, the [LTSP] 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 [LTSP] ensures that SLs are not exceeded. As such, the [LTSP] meets the definition of an SL-LSSS

BASES

BACKGROUND (continued)

Technical Specifications contain values related to the OPERABILITY of equipment required for safe operation of the facility. OPERABLE is defined in Technical Specifications as "...being capable of performing its safety function(s)." However, use of the [LTSP] to define OPERABILITY in Technical Specifications 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 [LTSP] 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 [LTSP] 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 [LTSP] to account for further drift during the next surveillance interval.

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. The Allowable Value specified in Table 3.3.5-1 is the least

conservative value of the as-found setpoint that a channel can have during testing such that a channel is OPERABLE if the trip setpoint is found conservative with respect to the Allowable Value during the CHANNEL FUNCTIONAL TEST (CFT). As such, the Allowable Value differs from the [LTSP] by an amount [greater than or] equal to the expected instrument channel uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will ensure that an SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance

BASES

BACKGROUND (continued)

interval. Note that, although the channel is OPERABLE under these circumstances, the setpoint must be left adjusted to a value within the established as-left tolerance, in accordance with uncertainty assumptions (as-left criteria), and confirmed to be operating within the statistical allowances of the uncertainty terms assigned (as-found criteria).

If the actual setting of the device is found to be conservative with respect to the Allowable Value but is beyond the as-found tolerance band, then this condition indicates that the instrument is degraded and is not performing in accordance with the setpoint methodology assumptions. This condition must be entered into the plant corrective action program, the trip setpoint must be left adjusted to a value within the as-left tolerance band, and an immediate determination of operability decision must be made.

If the actual setting of the device is found to be non-conservative with respect to the Allowable Value, the ~~device~~ channel 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.

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

The departure from nucleate boiling ratio (DNBR) shall be maintained above the Safety Limit (SL) value to prevent departure from nucleate boiling,

Fuel centerline melting shall not occur, and

The Reactor Coolant System (RCS) pressure SL of 2750 psia shall not be exceeded.

Maintaining the parameters within the above values ensures that the offsite dose will be within the 10 CFR 50 (Ref. 2) and ~~10 CFR 100~~do (Ref. 3) criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 3) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event. However, the acceptable dose limit for an accident category ~~these values and their~~ associated [LTSPs] are not considered to be LSSS as defined in 10 CFR 50.36.

The ESFAS contains devices and circuitry that generate the following signals when monitored variables reach levels that are indicative of conditions requiring protective action:

1. Safety Injection Actuation Signal (SIAS), Containment Cooling Actuation Signal (CCAS) (actuated by an automatic SIAS),
2. Containment Spray Actuation Signal (CSAS),
3. Containment Isolation Actuation Signal (CIAS),
4. Main Steam Isolation Signal (MSIS),
5. Recirculation Actuation Signal (RAS), and
- 6, 7. Emergency Feedwater Actuation Signal (EFAS).

Equipment actuated by each of the above signals is identified in the FSAR (Ref. 1).

Each of the above ESFAS instrumentation systems is segmented into three interconnected modules. These modules are:

Measurement channels,

Bistable trip units, and

ESFAS Logic:

- Matrix Logic,
- Initiation Logic (trip paths), and
- Actuation Logic.

BASES

BACKGROUND (continued)

This LCO addresses measurement channels and bistables. Logic is addressed in LCO 3.3.6, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip."

The role of each of these modules in the ESFAS, including the logic of LCO 3.3.6, is discussed below.

Measurement Channels

Measurement channels, consisting of field transmitters or process sensors and associated instrumentation, provide a measurable electronic signal based upon the physical characteristics of the parameter being measured.

Four identical measurement channels with electrical and physical separation are provided for each parameter used in the generation of trip signals. These channels are designated A through D. Measurement channels provide input to ESFAS bistables within the same ESFAS channel. In addition, some measurement channels are used as inputs to Reactor Protective System (RPS) bistables, and most provide indication in the control room. Measurement channels used as an input to the RPS or ESFAS are not used for control Functions.

When a channel monitoring a parameter indicates an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter will de-energize Matrix Logic, which in turn de-energizes the Initiation Logic. This causes both channels of Actuation Logic to de-energize. Each channel of Actuation Logic controls one train of the associated Engineered Safety Features (ESF) equipment.

Three of the four measurement and bistable channels are necessary to meet the redundancy and testability of GDC 21 in Appendix A to 10 CFR 50 (Ref. 2). The fourth channel provides additional flexibility by allowing one channel to be removed from service (trip channel bypass) for maintenance or testing while still maintaining a minimum two-out-of-three logic.

BASES

BACKGROUND (continued)

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

In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated and approved by the NRC staff. Plants not currently licensed to credit four channel

independence that may desire this capability must have approval of the NRC staff, documented by an NRC Safety Evaluation Report (Ref. 3). Adequate channel to channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants that have demonstrated adequate channel to channel independence may operate in two-out-of-three logic configuration, with one channel removed from service, until following the next MODE 5 entry. Plants not demonstrating four channel independence can only operate for 48 hours with one channel inoperable (Ref. 3).

Since no single failure will either cause or prevent a protective system actuation, and no protective channel feeds a control channel, this arrangement meets the requirements of IEEE Standard 279-1971 (Ref. 4).

Bistable Trip Units

Bistable trip units, mounted in the Plant Protection System (PPS) cabinet, receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Matrix Logic for each ESFAS Function. They also provide local trip indication and remote annunciation.

There are four channels of bistables, designated A through D, for each ESFAS Function, one for each measurement channel. In cases where two ESF Functions share the same input and trip setpoint (e.g., containment pressure input to CIAS and SIAS), the same bistable may be used to satisfy both Functions. Similarly, bistables may be shared between the RPS and ESFAS (e.g., Pressurizer Pressure - Low input to the RPS and SIAS). Bistable output relays de-energize when a trip occurs, in turn de-energizing bistable relays mounted in the PPS relay card racks.

The contacts from these bistable relays are arranged into six coincidence matrices, comprising the Matrix Logic. If bistables monitoring the same parameter in at least two channels trip, the Matrix Logic will generate an ESF actuation (two-out-of-four logic).

BASES

BACKGROUND (continued)

The trip setpoints and Allowable Values used in the bistables are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment effects, for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), Allowable

Values specified in Table 3.3.5-1, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. A detailed description of the methodology used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). The actual nominal trip setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. A channel is inoperable if its actual trip setpoint is non-~~not~~ ~~within~~ conservative with respect to its ~~required~~ Allowable Value.

~~Setpoints~~[LTSPs] in accordance with the Allowable Value will ensure that Safety Limits of LCO Section 2.0, "Safety Limits," are not violated during AOOs and the consequences of Design Basis Accidents (DBAs) will be acceptable, providing the plant is operated from within the LCOs at the onset of the AOO or DBA and the equipment functions as designed.

Functional testing of the ESFAS, from the bistable input through the opening of initiation relay contacts in the ESFAS Actuation Logic, can be performed either at power or at shutdown and is normally performed on a quarterly basis. FSAR, Section [7.2] (Ref. 8), provides more detail on ESFAS testing. Process transmitter calibration is normally performed on a refueling basis. SRs for the channels are specified in the Surveillance Requirements section.

ESFAS Logic

The ESFAS Logic, consisting of Matrix, Initiation and Actuation Logic, employs a scheme that provides an ESF actuation of both trains when bistables in any two of the four channels sense the same input parameter trip. This is called a two-out-of-four trip logic.

BASES

BACKGROUND (continued)

Bistable relay contact outputs from the four channels are configured into six logic matrices. Each logic matrix checks for a coincident trip in the same parameter in two bistable channels. The matrices are designated the AB, AC, AD, BC, BD, and CD matrices to reflect the bistable channels being monitored. Each logic matrix contains four normally energized matrix relays. When a coincidence is detected in the two channels being monitored by the logic matrix, all four matrix relays de-energize.

The matrix relay contacts are arranged into trip paths, with one relay contact from each matrix relay in each of the four trip paths. Each trip path controls two initiation relays. Each of the two initiation relays in each trip path controls contacts in the Actuation Logic for one train of ESF.

Each of the two channels of Actuation Logic, mounted in the Auxiliary Relay Cabinet (ARCs), is responsible for actuating one train of ESF

equipment. Each ESF Function has separate Actuation Logic in each ARC.

The contacts from the Initiation Logic are configured in a selective two-out-of-four logic in the Actuation Logic, similar to the configuration employed by the RPS in the RTCBs. This logic controls ARC mounted subgroup relays, which are normally energized. Contacts from these relays, when de-energized, actuate specific ESF equipment.

When a coincidence occurs in two ESFAS channels, all four matrix relays in the affected matrix will de-energize. This in turn will de-energize all eight initiation relays, four used in each Actuation Logic.

Matrix Logic refers to the matrix power supplies, trip channel bypass contacts, and interconnecting matrix wiring between bistable relay cards, up to but not including the matrix relays. Matrix contacts on the bistable relay cards are excluded from the Matrix Logic definition, since they are addressed as part of the measurement channel.

Initiation Logic consists of the trip path power source, matrix relays and their associated contacts, all interconnecting wiring, and the initiation relays.

Actuation Logic consists of all circuitry housed within the ARCs used to actuate the ESF Function, excluding the subgroup relays, and interconnecting wiring to the initiation relay contacts mounted in the PPS cabinet.

BASES

BACKGROUND (continued)

The subgroup relays are actuated by the ESFAS logic. Each ESFAS Function typically employs several subgroup relays, with each subgroup relay responsible for actuating one or more components in the ESFAS Function. Subgroup relays and their contacts are considered part of the actuated equipment and are addressed under the applicable LCO for this equipment. Initiation and Actuation Logic up to the subgroup relays is addressed in LCO 3.3.6.

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

same parameter in more than one channel. Trip channel bypassing is normally employed during maintenance or testing.

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

For plants that have demonstrated sufficient channel to channel independence, two-out-of-three logic is the minimum that is required to provide adequate plant protection, since a failure of one channel still ensures ESFAS actuation would be generated by the two remaining OPERABLE channels. Two-out-of-three logic also prevents inadvertent actuations caused by any single channel failure in a trip condition.

In addition to the trip channel bypasses, there are also operating bypasses on select ESFAS actuation trips. These bypasses are enabled manually in all four channels when plant conditions do not warrant the specific trip protection. All operating bypasses are automatically removed when enabling bypass conditions are no longer satisfied. Operating bypasses normally are implemented in the bistable, so that normal trip indication is also disabled. The Pressurizer Pressure - Low input to the SIAS shares an operating bypass with the Pressurizer Pressure - Low reactor trip.

BASES

BACKGROUND (continued)

Manual ESFAS initiation capability is provided to permit the operator to manually actuate an ESF System when necessary.

Two sets of two push buttons (located in the control room) for each ESF Function are provided, and each set actuates both trains. Each Manual Trip push button opens one trip path, de-energizing one set of two initiation relays, one affecting each train of ESF. Initiation relay contacts are arranged in a selective two-out-of-four configuration in the Actuation Logic. By arranging the push buttons in two sets of two, such that both push buttons in a set must be depressed, it is possible to ensure that Manual Trip will not be prevented in the event of a single random failure. Each set of two push buttons is designated a single channel in LCO 3.3.6.

| | |
|----------------------------------|--|
| APPLICABLE SAFETY ANALYSES | Each of the analyzed accidents can be detected by one or more ESFAS Functions. One of the ESFAS Functions is the primary actuation signal for that accident. An ESFAS Function may be the primary actuation signal for more than one type of accident. An ESFAS Function may also be the secondary, or backup, actuation signal for one or more other accidents. |
|----------------------------------|--|

~~Trip Setpoints that directly protect against violating the Reactor Core Safety Limits or the Reactor Coolant System (RCS) Pressure boundary Safety Limits during anticipated operational occurrences (AOOs) are Safety Limit-Limiting Safety System Settings (SL-LSSS). Permissive and interlock setpoints allow bypass of trips when they are not required by the Safety Analysis. These permissives and interlocks ensure that the starting conditions are consistent with the safety analysis, before preventative or mitigating actions occur. Because these permissives or~~

interlocks are only one of multiple conservative starting assumptions for the accident analysis, they are generally considered as nominal values without regard to measurement accuracy, (i.e. the value indicated is sufficiently close to the necessary value to ensure proper operation of the safety systems to turn the AOO). Therefore permissives and interlocks are not considered to be SL-LSSS.

ESFAS protective Functions are as follows:

1. Safety Injection Actuation Signal

SIAS ensures acceptable consequences during large break loss of coolant accidents (LOCAs), small break LOCAs, control element assembly ejection accidents, and main steam line breaks (MSLBs) inside containment. To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS) and performs several other functions such as initiating a containment cooling actuation, initiating control room isolation, and starting the diesel generators.

CCAS mitigates containment overpressurization when required by either a manual CCAS actuation or an automatic SIAS Function. This Function is not employed by all plants.

BASES

APPLICABLE SAFETY ANALYSES (continued)

2. Containment Spray Actuation Signal

CSAS actuates containment spray, preventing containment overpressurization during large break LOCAs, small break LOCAs, and MSLBs or feedwater line breaks (FWLBs) inside containment. CSAS is initiated by high containment pressure and an SIAS. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

CIAS ensures acceptable mitigating actions during large and small break LOCAs, and MSLBs or FWLBs either inside or outside containment. CIAS is initiated by low pressurizer pressure or high containment pressure.

4. Main Steam Isolation Signal

MSIS ensures acceptable consequences during an MSLB or FWLB (between the steam generator and the main feedwater check valve), either inside or outside containment. MSIS isolates both steam generators if either generator indicates a low pressure condition or if

a high containment pressure condition exists. This prevents an excessive rate of heat extraction and subsequent cooldown of the RCS during these events.

5. Recirculation Actuation Signal

At the end of the injection phase of a LOCA, the refueling water storage tank (RWST) will be nearly empty. Continued cooling must be provided by the ECCS to remove decay heat. The source of water for the ECCS pumps is automatically switched to the containment recirculation sump. Switchover from RWST to containment sump must occur before the RWST empties to prevent damage to the ECCS pumps and a loss of core cooling capability. For similar reasons, switchover must not occur before there is sufficient water in the containment sump to support pump suction. Furthermore, early switchover must not occur to ensure sufficient borated water is injected from the RWST to ensure the reactor remains shut down in the recirculation mode. An RWST Level - Low signal initiates the RAS.

BASES

APPLICABLE SAFETY ANALYSES (continued)

6, 7. Emergency Feedwater Actuation Signal

EFAS consists of two steam generator (SG) specific signals (EFAS-1 and EFAS-2). EFAS-1 initiates emergency feed to SG #1, and EFAS-2 initiates emergency feed to SG #2.

EFAS maintains a steam generator heat sink during a steam generator tube rupture event and an MSLB or FWLB event either inside or outside containment.

Low steam generator water level initiates emergency feed to the affected steam generator, providing the generator is not identified (by the circuitry) as faulted (a steam or FWLB).

EFAS logic includes steam generator specific inputs from the Steam Generator Pressure - Low bistable comparator (also used in MSIS) and the SG Pressure Difference - High (SG #1 > SG #2 or SG #2 > SG #1, bistable comparators) to determine if a rupture in either generator has occurred.

Rupture is assumed if the affected generator has a low pressure condition, unless that generator is significantly higher in pressure than the other generator.

This latter feature allows feeding the intact steam generator, even if both are below the MSIS setpoint, while preventing the ruptured

generator from being fed. Not feeding a ruptured generator prevents containment overpressurization during the analyzed events.
The ESFAS satisfies Criterion 3 of 10 CFR 50.36(c)(2)(ii).

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE. 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.

Only the Allowable Values are specified for each ESFAS Function in the LCO. The [LTSP] and the methodologies for calculation of the as-left and as-found tolerances are described in [a document controlled under 10 CFR 50.59]. The [LTSPs] 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. The Allowable Value specified in Table 3.3.5-1 is the least conservative value of the as-found setpoint that the channel can have when tested, such that a channel is OPERABLE if the as-found setpoint is conservative with respect to the Allowable Value during the CHANNEL FUNCTIONAL TEST (CFT). Each Allowable Value specified is more conservative than instrument uncertainties appropriate to the trip Function. These uncertainties are defined in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). As such, the Allowable Value differs from the [LTSP] by an amount [greater than or] equal to the expected instrument channel uncertainties, such as drift, during the surveillance interval. In this manner, the actual setting of the device will ensure that a SL is not exceeded at any given point of time as long as the device has not drifted beyond that expected during the surveillance interval. Note that, although the channel is OPERABLE under these circumstances, the trip setpoint must be left adjusted to a value within the as-left tolerance, 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 (as-found criteria). If the actual setting of the device is found to be conservative with respect to the Allowable Value but is beyond the as-found tolerance band, then this condition indicates that the instrument is degraded and is not performing in accordance with the setpoint methodology assumptions. This condition must be entered into the plant corrective action program, the trip setpoint must be left adjusted to a value within the as-left tolerance band, and an immediate determination of operability decision must be made. If the actual setting of the device is found to be non-conservative with respect to the Allowable Value, the device—device would be considered inoperable. This requires corrective action including those actions required by 10 CFR 50.36 when automatic protective devices do not function as required.

Plants are restricted to 48 hours in a trip channel bypass condition before restoring the Function to four channel operation (two-out-of-four logic) or placing the channel in trip (two-out-of-three logic).

The Bases for the LCOs on ESFAS Functions are:
BASES

LCO (continued)

1. Safety Injection Actuation Signal

a. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

b. Pressurizer Pressure - Low

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

The Allowable Value for this trip is set low enough to prevent actuating the ESF Functions (SIAS and CIAS) during normal plant operation and pressurizer pressure transients. The setting is high enough that, with the specified accidents, the ESF systems will actuate to perform as expected, mitigating the consequences of the accident. The Pressurizer Pressure - Low trip setpoint, which provides SIAS, CIAS, and RPS trip, may be manually decreased to a floor value of 300 psia to allow for a controlled cooldown and depressurization of the RCS without causing a reactor trip, CIAS, or SIAS. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value (400 psia) to ensure a reactor trip, CIAS, and SIAS will occur if required during RCS cooldown and depressurization.

From this reduced setting, the trip setpoint will increase automatically as pressurizer pressure increases, tracking actual RCS pressure until the trip setpoint is reached.

BASES

LCO (continued)

When the trip setpoint has been lowered below the bypass permissive setpoint of 400 psia, the Pressurizer Pressure - Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When RCS pressure rises above the bypass removal setpoint, the bypass is removed.

Bypass Removal

This LCO requires four channels of bypass removal for Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

Each of the four channels enables and disables the bypass capability for a single channel. Therefore, this LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Because the trip setpoint has a floor value of 300 psia, a channel trip will result if pressure is decreased below this setpoint without bypassing.

The bypass removal Allowable Value was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated for by required SDM.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. For an automatic actuation, it is necessary to have a Containment Pressure - High High signal, coincident with an SIAS. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure - High signal used in the SIAS will initiate before the Containment Pressure - High High. This ensures that a CSAS will not initiate unless required.

a. Containment Pressure - High High

This LCO requires four channels of Containment Pressure - High High to be OPERABLE in MODES 1, 2, and 3.

BASES

LCO (continued)

The Allowable Value for this trip is set high enough to allow for first response ESF systems (containment cooling systems) to attempt to mitigate the consequences of an accident before resorting to spraying borated water onto containment equipment. The setting is low enough to initiate CSAS in time to prevent containment pressure from exceeding design.

3. Containment Isolation Actuation Signal

For plants where the SIAS and CIAS are actuated on Pressurizer Pressure - Low or Containment Pressure - High, the SIAS and CIAS share the same input channels, bistables, and matrices and matrix relays. The remainder of the initiation channels, the manual channels, and the Actuation Logic are separate and are addressed in LCO 3.3.6. Since their Applicability is also the same, they have identical Required Actions.

a. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3.

The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

b. Pressurizer Pressure - Low

This LCO requires four channels of Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is set low enough to prevent actuating the ESF Functions (SIAS and CIAS) during normal plant operation and pressurizer pressure transients. The setting is high enough that, with the specified accident, the ESF systems will actuate to perform as expected, mitigating the consequences of the accidents.

BASES

LCO (continued)

The Pressurizer Pressure - Low trip setpoint, which provides an SIAS, CIAS, and RPS trip, may be manually decreased to a floor Allowable Value of 300 psia to allow for a controlled cooldown and depressurization of the RCS without causing a reactor trip, CIAS or SIAS. The safety margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value (400 psi) to ensure a reactor trip, CIAS, and SIAS will occur if required during RCS cooldown and depressurization.

From this reduced setting, the trip setpoint will increase automatically as pressurizer pressure increases, tracking actual RCS pressure until the trip setpoint is reached. When the trip setpoint has been lowered below the bypass removal setpoint of 400 psia, the Pressurizer Pressure - Low reactor trip, CIAS, and SIAS actuation may be manually bypassed in preparation for shutdown cooling. When RCS pressure rises above the bypass removal, the bypass is removed.

Bypass Removal

This LCO requires four channels of bypass removal for Pressurizer Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

Each of the four channels enables and disables the bypass capability for a single channel. Therefore all four bypass removal channels must be OPERABLE to ensure that none of the four channels are inadvertently bypassed.

This LCO applies to the bypass removal feature only. If the bypass enable function is failed so as to prevent entering a bypass condition, operation may continue. Because the trip setpoint has a floor value of 300 psia, a channel trip will result if pressure is decreased below this setpoint without bypassing.

The bypass removal Allowable Value was chosen because MSLB events originating from below this setpoint add less positive reactivity than that which can be compensated for by required SDM.

BASES

LCO (continued)

4. Main Steam Isolation Signal

The LCO is applicable to the MSIS in MODES 1, 2, and 3 except when all associated valves are closed and de-activated.

a. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The Allowable Value for this trip is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide an MSIS (Function 4) during an excessive steam demand event. An excessive steam demand event causes the RCS to cool down, resulting in a positive reactivity addition to the core.

MSIS limits this cooldown by isolating both steam generators if the pressure in either drops below the trip setpoint. An RPS trip on Steam Generator Pressure - Low is initiated simultaneously, using the same bistable. The Steam Generator Pressure - Low bistable output is also used in the EFAS logic (Function 7) to aid in determining if a steam generator is intact.

The Steam Generator Pressure - Low trip setpoint may be manually decreased as steam generator pressure is reduced. This prevents an RPS trip or MSIS actuation during controlled plant cooldown. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value of 200 psia to ensure a reactor trip and MSIS will occur when required.

b. Containment Pressure - High

This LCO requires four channels of Containment Pressure - High to be OPERABLE in MODES 1, 2, and 3. The Containment Pressure - High signal is shared among the SIAS (Function 1), CIAS (Function 3), and MSIS (Function 4).

BASES

LCO (continued)

The Allowable Value for this trip is set high enough to allow for small pressure increases in containment expected during normal operation (i.e., plant heatup) and is not indicative of an abnormal condition. The setting is low enough to initiate the ESF Functions when an abnormal condition is indicated. This allows the ESF systems to perform as expected in the accident analyses to mitigate the consequences of the analyzed accidents.

5. Recirculation Actuation Signal

a. Refueling Water Storage Tank Level - Low

This LCO requires four channels of RWST Level - Low to be OPERABLE in MODES 1, 2, and 3.

The upper limit on the Allowable Value for this trip is set low enough to ensure RAS does not initiate before sufficient water is transferred to the containment sump. Premature recirculation could impair the reactivity control function of safety injection by limiting the amount of boron injection. Premature recirculation could also damage or disable the recirculation system if recirculation begins before the sump has enough water to prevent air entrainment in the suction. The lower limit on the RWST Level - Low trip Allowable Value is high enough to transfer suction to the containment sump prior to emptying the RWST.

6, 7 Emergency Feedwater Actuation Signal SG #1 and SG #2 (EFAS-1 and EFAS-2)

EFAS-1 is initiated to SG #1 by either a low steam generator level coincident with no low pressure trip present on SG #1 or by a low steam generator level coincident with a differential pressure between the two generators with the higher pressure in SG #1. EFAS-2 is similarly configured to feed SG #2.

BASES

LCO (continued)

The steam generator secondary differential pressure is used, in conjunction with a Steam Generator Pressure - Low input from each steam generator, as an input of the EFAS logic where it is used to determine if a generator is intact. The EFAS logic inhibits feeding a steam generator if a Steam Generator Pressure - Low condition exists in that generator and the pressure in that steam generator is

less than the pressure in the other steam generator by the Steam Generator Pressure Difference (SGPD) - High setpoint.

The SGPD logic thus enables the feeding of a steam generator in the event that a plant cooldown causes a Steam Generator Pressure - Low condition, while inhibiting feeding the other (lower pressure) steam generator, which may be ruptured. The setpoint is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation.

The following LCO description applies to both EFAS signals.

a. Steam Generator Level - Low

This LCO requires four channels of Steam Generator Level - Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Steam Generator Level - Low EFAS input is derived from the Steam Generator Level - Low RPS bistable output. EFAS is thus initiated simultaneously with a reactor trip. The setpoint ensures at least a 20 minute inventory of water remains in the affected steam generator at reactor trip. Thus, EFAS is initiated well before steam generator inventory is challenged.

b. SG Pressure Difference - High (SG #1 > SG #2) or (SG #2 > SG #1)

This LCO requires four channels of SG Pressure Difference - High to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Allowable Value for this trip is high enough to allow for small pressure differences and normal instrumentation errors between the steam generator channels during normal operation without an actuation. The setting is low enough to detect and inhibit feeding of a ruptured steam generator in the event of an MSLB or FWLB, while permitting the feeding of the intact steam generator.

BASES

LCO (continued)

c. Steam Generator Pressure - Low

This LCO requires four channels of Steam Generator Pressure - Low to be OPERABLE for each EFAS in MODES 1, 2, and 3.

The Steam Generator Pressure - Low input is derived from the Steam Generator Pressure - Low RPS bistable output. This output is also used as an MSIS input.

The Allowable Value for this trip is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide an MSIS (Function 4) during an excessive steam demand event. An excessive steam demand is one indicator of a potentially ruptured steam generator; thus, this EFAS input, in conjunction with the SGPD Function, prevents the feeding of a potentially ruptured steam generator.

The Steam Generator Pressure - Low trip setpoint may be manually decreased as steam generator pressure is reduced. This prevents an RPS trip or MSIS actuation during controlled plant cooldown. The margin between actual pressurizer pressure and the trip setpoint must be maintained less than or equal to the specified value of 200 psi to ensure that a reactor trip and MSIS will occur when required.

APPLICABILITY In MODES 1, 2 and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

Close the main steam isolation valves to preclude a positive reactivity addition,

Actuate emergency feedwater to preclude the loss of the steam generators as a heat sink (in the event the normal feedwater system is not available),

Actuate ESF systems to prevent or limit the release of fission product radioactivity to the environment by isolating containment and limiting the containment pressure from exceeding the containment design pressure during a design basis LOCA or MSLB, and

Actuate ESF systems to ensure sufficient borated inventory to permit adequate core cooling and reactivity control during a design basis LOCA or MSLB accident.

BASES

APPLICABILITY (continued)

In MODES 4, 5, and 6, automatic actuation of these Functions is not required because adequate time is available to evaluate plant conditions and respond by manually operating the ESF components if required, as addressed by LCO 3.3.6.

Several trips have operating bypasses, discussed in the preceding LCO section. The interlocks that allow these bypasses shall be OPERABLE whenever the RPS Function they support is OPERABLE.

ACTIONS

The most common causes of channel inoperability are outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis. Typically, the drift is found to be small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within specification.

In the event a channel's trip setpoint is found nonconservative with respect to the Allowable Value, or the transmitter, instrument loop, signal processing electronics, or ESFAS bistable is found inoperable, then all affected Functions provided by that channel must be declared inoperable and the LCO Condition entered for the particular protection Function affected.

When the number of inoperable channels in a trip Function exceeds those specified in any related Condition associated with the same trip Function, then the plant is outside the safety analysis. Therefore, LCO 3.0.3 should be entered immediately, if applicable in the current MODE of operation.

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

A.1 and A.2

Condition A applies to the failure of a single channel of one or more input parameters in the following ESFAS Functions:

1. Safety Injection Actuation Signal Containment Pressure - High
Pressurizer Pressure - Low

BASES

ACTIONS (continued)

2. Containment Spray Actuation Signal Containment Pressure - High
High Automatic SIAS
3. Containment Isolation Actuation Signal Containment Pressure - High
Pressurizer Pressure - Low
4. Main Steam Isolation Signal Steam Generator Pressure - Low
Containment Pressure - High
5. Recirculation Actuation Signal Refueling Water Storage Tank Level -
Low
6. Emergency Feedwater Actuation Signal SG #1 (EFAS-1) Steam
Generator Level - Low SG Pressure Difference - High Steam
Generator Pressure - Low
7. Emergency Feedwater Actuation Signal SG #2 (EFAS-2) Steam
Generator Level - Low SG Pressure Difference - High Steam
Generator Pressure - Low

ESFAS coincidence logic is normally two-out-of-four.

If one ESFAS channel is inoperable, startup or power operation is allowed to continue, providing the inoperable channel is placed in bypass or trip within 1 hour (Required Action A.1).

The Completion Time of 1 hour allotted to restore, bypass, or trip the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.

The failed channel must be restored to OPERABLE status prior to entering MODE 2 following the next MODE 5 entry. With a channel bypassed, the coincidence logic is now in a two-out-of-three configuration. In this configuration, common cause failure of dependent channels cannot prevent trip. The Completion Time of prior to entering MODE 2 following the next MODE 5 entry is based on adequate channel to channel independence, which allows a two-out-of-three channel operation, since no single failure will cause or prevent a reactor trip.

BASES

ACTIONS (continued)

B.1

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

1. Safety Injection Actuation Signal Containment Pressure - High
Pressurizer Pressure - Low
2. Containment Spray Actuation Signal Containment Pressure - High
High Automatic SIAS
3. Containment Isolation Actuation Signal Containment Pressure - High
Pressurizer Pressure - Low
4. Main Steam Isolation Signal Steam Generator Pressure - Low
Containment Pressure - High
5. Recirculation Actuation Signal Refueling Water Storage Tank Level -
Low
6. Emergency Feedwater Actuation Signal SG #1 (EFAS-1) Steam
Generator Level - Low SG Pressure Difference - High Steam
Generator Pressure - Low
7. Emergency Feedwater Actuation Signal SG #2 (EFAS-2) Steam
Generator Level - Low SG Pressure Difference - High Steam
Generator Pressure - Low

With two inoperable channels, power operation may continue, provided one inoperable channel is placed in bypass and the other channel is placed in trip within 1 hour. With one channel of protective instrumentation bypassed, the ESFAS Function is in two-out-of-three logic in the bypassed input parameter, but with another channel failed, the ESFAS may be operating with a two-out-of-two logic. This is outside the assumptions made in the analyses and should be corrected. To correct the problem, the second channel is placed in trip. This places the ESFAS Function in a one-out-of-two logic. If any of the other OPERABLE channels receives a trip signal, ESFAS actuation will occur. BASES

ACTIONS (continued)

One of the two inoperable channels will need to be restored to OPERABLE status prior to the next required CHANNEL FUNCTIONAL TEST because channel surveillance testing on an OPERABLE channel requires that the OPERABLE channel be placed in bypass. However, it is not possible to bypass more than one ESFAS channel, and placing a second channel in trip will result in an ESFAS actuation. Therefore, if one ESFAS channel is in trip and a second channel is in bypass, a third inoperable channel would place the unit in LCO 3.0.3.

C.1, C.2.1, and C.2.2

Condition C applies to one automatic bypass removal channel inoperable. The only automatic bypass removal on an ESFAS is on the Pressurizer Pressure - Low signal. This bypass removal is shared with the RPS Pressurizer Pressure - Low bypass removal.

If the bypass removal channel for any operating bypass cannot be restored to OPERABLE status, the associated ESFAS channel may be considered OPERABLE only if the bypass is not in effect. Otherwise, the affected ESFAS channel must be declared inoperable, as in Condition A, and the bypass either removed or the bypass removal channel repaired. The Bases for the Required Actions and required Completion Times are consistent with Condition A.

D.1 and D.2

Otherwise, the affected ESFAS channels must be declared inoperable, as in Condition B, and either the bypass removed or the bypass removal channel repaired. The restoration of one affected bypassed automatic trip channel must be completed prior to the next CHANNEL FUNCTIONAL TEST or the plant must shut down per LCO 3.0.3, as explained in Condition B. Completion Times are consistent with Condition B.

BASES

ACTIONS (continued)

E.1 and E.2

If the Required Actions and associated Completion Times of Condition A, B, C, or D cannot be met, the plant must be brought to a MODE in which the LCO does not apply. To achieve this status, the plant must be brought to at least MODE 3 within 6 hours and to MODE 4 within [12] hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

SURVEILLANCE ~~SR 3.3.5.1~~ REQUIREMENTS

----- REVIEWER'S NOTE -----
The Notes in Table 3.3.5-1 requiring reset of the channel to a predefined as-left tolerance and the verification of the as-found tolerance are only associated with SL-LSSS values. Therefore, the Notes are applied to specific SRs for the associated functions in the SR column only. The Notes may be placed at the top of the Allowable Value column in the Table and applied to all Functions with allowable values in the table.

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

Notes 1 and 2 are applied to the setpoint verification Surveillances for all SL-LSSS Functions unless one or more of the following exclusions apply:

1. Notes 1 and 2 are not applied to SL-LSSS Functions which utilize mechanical components to sense the trip setpoint or to manual initiation circuits (the latter are not explicitly modeled in the accident analysis). Examples of mechanical components are limit switches, float switches, proximity detectors, manual actuation switches, and other such devices that are normally only checked on a "go/no go" basis. Note 1 requires a comparison of the periodic surveillance requirement results to provide an indication of channel (or individual device) performance. This comparison is not valid for most mechanical components. While it is possible to verify that a limit switch functions at a point of travel, a change in the surveillance result probably indicates that the switch has moved, not that the input/output relationship has changed. Therefore, a comparison of surveillance requirement results would not provide an indication of the channel or component performance.
2. Notes 1 and 2 are not applied to Technical Specifications associated with mechanically operated safety relief valves. The performance of these components is already controlled (i.e., trended with as-left and as-found limits) under the ASME Section XI testing program.
3. Notes 1 and 2 are may not applied to SL-LSSS Functions and Surveillances which test only digital components. For purely digital components, such as actuation logic circuits and associated relays, there is no expected change in result between surveillance performances other than measurement and test errors (M&TE) and, therefore, justification is needed to confirm that comparison of Surveillance results does not provide an indication of channel or component performance.

An evaluation of the potential SL-LSSS Functions resulted in Notes 1 and 2 being applied to the Functions shown in the TS markups. Each licensee proposing to fully adopt this TSTF must review the the potential SL-LSSS Functions to identify which of the identified functions are SL-LSSS according to the definition of SL-LSSS and their plant specific safety analysis. The two TSTF Notes are not required to be applied to any of the listed Functions which meet any of the exclusion criteria or are not SL-LSSS based on the plant specific design and analysis.

SR 3.3.5.1

Performance of the CHANNEL CHECK once every 12 hours ensures that a gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a

similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; thus, it is key to verifying the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

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

The Frequency, about once every shift, is based on operating experience that demonstrates channel failure is rare. Since the probability of two random failures in redundant channels in any 12 hour period is low, the CHANNEL CHECK minimizes the chance of loss of protective function due to failure of redundant channels. The CHANNEL CHECK supplements less formal, but more frequent, checks of channel OPERABILITY during normal operational use of displays associated with the LCO required channels.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.2

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

The CHANNEL FUNCTIONAL TEST is part of an overlapping test sequence similar to that employed in the RPS. This sequence, consisting of SR 3.3.5.2, SR 3.3.6.1, and SR 3.3.6.2, tests the entire ESFAS from the bistable input through the actuation of the individual subgroup relays. These overlapping tests are described in Reference 1. SR 3.3.5.2 and SR 3.3.6.1 are normally performed together and in conjunction with ESFAS testing. SR 3.3.6.2 verifies that the subgroup relays are capable of actuating their respective ESF components when de-energized.

These tests verify that the ESFAS is capable of performing its intended function, from bistable input through the actuated components. SRs 3.3.6.1 and 3.3.6.2 are addressed in LCO 3.3.6. SR 3.3.5.2 includes bistable tests.

A test signal is superimposed on the input in one channel at a time to verify that the bistable trips within the specified tolerance around the setpoint. This is done with the affected RPS trip channel bypassed. Any setpoint adjustment shall be consistent with the assumptions of the current plant specific setpoint analysis.

The as-found [and as-left] values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [9].

SL-LSSS functions are modified by two Notes as identified in Table 3.3.5-1. The first Note requires evaluation of channel performance for the condition where the as-found setting for the channel setpoint is outside its as-found tolerance but conservative with respect to the Allowable Value. Evaluation of instrument performance will verify that the instrument will continue to behave in accordance with safety analysis setpoint methodology assumptions. The purpose of the assessment is to ensure confidence in the instrument performance prior to returning the instrument to service. These channels will also be identified in the Corrective Action Program. Entry into the Corrective Action Program will ensure required review and documentation of the condition for continued OPERABILITY. The second Note requires that the as-left setting for the instrument be returned to within the as-left tolerance of the [LTSP]. Where a setpoint more conservative than the [LTSP] is used in the plant surveillance procedures, the as-left and as-found tolerances, as applicable, will be applied to the surveillance procedure setpoint. This will ensure that sufficient margin to the Safety Limit and/or Analytical Limit is maintained. If the as-left instrument setting cannot be returned to a setting within the as-left tolerance of the [LTSP], then the instrument channel shall be declared inoperable.

The second Note also requires that [LTSP] and the methodologies for calculating the as-left and the as-found tolerances be in [a document controlled under 10 CFR 50.59].

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.3

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

The as-found [and as-left] values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [9].

The [18] month Frequency is based on the need to perform this Surveillance under the conditions that apply during a plant outage and the potential for an unplanned transient if the Surveillance were performed with the reactor at power.

SR 3.3.5.3 for SL-LSSS functions are modified by two Notes as identified in Table 3.3.5-1. The first Note requires evaluation of channel performance for the condition where the as-found setting for the channel setpoint is outside its as-found tolerance but conservative with respect to the Allowable Value. Evaluation of instrument performance will verify that the instrument will continue to behave in accordance with safety analysis setpoint methodology assumptions. The purpose of the assessment is to ensure confidence in the instrument performance prior to returning the instrument to service. These channels will also be identified in the Corrective Action Program. Entry into the Corrective Action Program will ensure required review and documentation of the condition for continued OPERABILITY. The second Note requires that the as-left setting for the instrument be returned to within the as-left tolerance of the [LTSP]. Where a setpoint more conservative than the [LTSP] is used in the plant surveillance procedures, the as-left and as-found tolerances, as applicable, will be applied to the surveillance procedure setpoint. This will ensure that sufficient margin to the Safety Limit and/or Analytical Limit is maintained. If the as-left instrument setting cannot be returned to a setting within the as-left tolerance of the [LTSP], then the instrument channel shall be declared inoperable.

The second Note also requires that [LTSP] and the methodologies for calculating the as-left and the as-found tolerances be in [a document controlled under 10 CFR 50.59].

SR 3.3.5.4

This Surveillance ensures that the train actuation response times are within the maximum values assumed in the safety analyses.

Response time testing acceptance criteria are included in Reference 10.

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

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

Response time may be verified by any series of sequential, overlapping or total channel measurements, including allocated sensor response time, such that the response time is verified. Allocations for sensor response times may be obtained from records of test results, vendor test data, or vendor engineering specifications. Topical Report CE NPSD-1167-A,

BASES

SURVEILLANCE REQUIREMENTS (continued)

"Elimination of Pressure Sensor Response Time Testing Requirements," (Ref. 11) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every [18] months. The [18] month Frequency is consistent with the typical industry refueling cycle and is based upon plant operating experience, which shows that random failures of instrumentation components causing serious response time degradation, but not channel failure, are infrequent occurrences.

SR 3.3.5.5

SR 3.3.5.5 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.5.2, except SR 3.3.5.5 is performed within 92 days prior to startup and is only applicable to bypass functions. Since the Pressurizer Pressure - Low bypass is identical for both the RPS and ESFAS, this is the same Surveillance performed for the RPS in SR 3.3.1.13. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

The CHANNEL FUNCTIONAL TEST for proper operation of the bypass permissives is critical during plant heatups because the bypasses may be in place prior to entering MODE 3 but must be removed at the appropriate points during plant startup to enable the ESFAS Function. Consequently, just prior to startup is the appropriate time to verify bypass function OPERABILITY. Once the bypasses are removed, the bypasses must not fail in such a way that the associated ESFAS Function is inappropriately bypassed. This feature is verified by SR 3.3.5.2.

The allowance to conduct this test with 92 days of startup is based on the reliability analysis presented in topical report CEN-327, "RPS/ESFAS Extended Test Interval Evaluation" (Ref. 9).

BASES

REFERENCES

1. FSAR, Section [7.3].
 2. 10 CFR 50, Appendix A.
 3. NRC Safety Evaluation Report.
 4. IEEE Standard 279-1971.
 5. FSAR, Chapter [15].
 6. 10 CFR 50.49.
 7. "Plant Protection System Selection of Trip Setpoint Values."
 8. FSAR, Section [7.2].
 9. CEN-327, May 1986, including Supplement 1, March 1989.
 10. Response Time Testing Acceptance Criteria.
 11. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."
-