

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. This is achieved by specifying limiting safety system settings (LSSS), where they exist, in terms of parameters directly monitored by the ESFAS as well as LCOs on other reactor 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 3.3.4-1 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 b of Table 3.3.4-1. 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 3.3.4-1 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~~ a SL is not exceeded at any given point of time as long as the device has

BASES

BACKGROUND (continued)

not drifted beyond that expected during the surveillance interval. 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 channel ~~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.

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

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

Fuel centerline melting shall not occur, and

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

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

Accidents are events that are analyzed even though they are not expected to occur during the plant life. The acceptable limit during accidents is that the offsite dose shall be maintained within an acceptable fraction of 10 CFR 100 (Ref. 3) limits. Different accident categories allow a different fraction of these limits based on probability of occurrence. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event. However, the acceptable accident 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 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 [LTSP]. When tripped, the sensor subsystems provide outputs to the two actuation subsystems.

BACKGROUND (continued)

The two independent actuation subsystems compare the four sensor subsystem outputs. If a trip occurs in the same parameter in two or more sensor subsystem channels, the two-out-of-four logic in each actuation subsystem will initiate one train of ESFAS. Each train can provide protection to the public in the case of a Design Basis Event. Actuation Logic is addressed in LCO 3.3.5, "Engineered Safety Features Actuation System (ESFAS) Logic and Manual Trip."

Each of the four sensor subsystems is mounted in a separate cabinet, excluding the sensors and field wiring.

The role of the sensor subsystem (measurement channels and bistables) is discussed below; actuation subsystems are discussed in LCO 3.3.5.

Measurement Channels

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

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

When a channel monitoring a parameter indicates an unsafe condition, the bistable monitoring the parameter in that channel will trip. Tripping two or more channels of bistables monitoring the same parameter will de-energize both channels of Actuation Logic of the associated Engineered Safety Features (ESF) equipment.

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

BASES

BACKGROUND (continued)

In order to take full advantage of the four channel design, adequate channel to channel independence must be demonstrated, and approved by the NRC staff. Plants not currently licensed as to credit four channel independence that may desire this capability must have approval of the

NRC staff documented by an NRC Safety Evaluation Report (Ref. 3). Adequate channel to channel independence includes physical and electrical independence of each channel from the others. Furthermore, each channel must be energized from separate inverters and station batteries. Plants not demonstrating four channel independence may operate in a two-out-of-three logic configuration for 48 hours.

Since no single failure will either cause or prevent a protective system actuation and no protective channel feeds a control channel, this arrangement meets the requirements of IEEE Standard 79-1971 (Ref. 4).

Bistable Trip Units

Bistable trip units receive an analog input from the measurement channels, compare the analog input to trip setpoints, and provide contact output to the Actuation Logic. They also provide local trip indication and remote annunciation.

There are four channels of bistables, designated A through D, for each ESF Function, one for each measurement channel. In cases where two ESF Functions share the same input and trip setpoint (e.g., containment pressure input to CSAS, CIAS, and SIAS and a Pressurizer Pressure - Low input to the RPS and SIAS), the same bistable may be used to satisfy both Functions.

The trip setpoints and Allowable Values used in the bistables are based on the analytical limits stated in Reference 5. The selection of these trip setpoints is such that adequate protection is provided when all sensor and processing time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment effects, for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 6), Allowable Values specified in Table 3.3.4-1, in the accompanying LCO, are conservatively adjusted with respect to the analytical limits. A detailed description of the method used to calculate the trip setpoints, including their explicit uncertainties, is provided in the "Plant Protection System Selection of Trip Setpoint Values" (Ref. 7). The actual nominal trip

BASES

BACKGROUND (continued)

setpoint entered into the bistable is normally still more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. If the measured setpoint ~~does not exceed~~ is conservative with respect to the Allowable Value, the bistable is considered OPERABLE.

Setpoints [LTSPs] 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.

~~Trip Setpoints [LTSPs] 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:

APPLICABLE SAFETY ANALYSES (continued)

1. Safety Injection Actuation Signal

The SIAS ensures acceptable consequences during loss of coolant accident (LOCA) events, including steam generator tube rupture, and main steam line breaks (MSLBs) or feedwater line breaks (FWLBs) (inside containment). To provide the required protection, either a high containment pressure or a low pressurizer pressure signal will initiate SIAS. SIAS initiates the Emergency Core Cooling Systems (ECCS), control room isolation, and several other Functions, such as starting the emergency diesel generators.

2. Containment Spray Actuation Signal

The CSAS initiates containment spray, preventing containment overpressurization during a LOCA or MSLB. At some plants, both a high containment pressure signal and an SIAS have to actuate to provide the required protection. This configuration reduces the likelihood of inadvertent containment spray.

3. Containment Isolation Actuation Signal

The CIAS actuates the Containment Isolation System, ensuring acceptable consequences during LOCAs and MSLBs or FWLBs (inside containment). To provide protection, a high containment pressure signal will initiate CIAS at the same setpoint at which an SIAS is generated.

4. Main Steam Isolation Signal

The MSIS ensures acceptable consequences during an MSLB or FWLB by isolating both steam generators if either generator indicates a low steam generator pressure. The MSIS, concurrent with or following a reactor trip, minimizes the rate of heat extraction and subsequent cooldown of the RCS during these events.

BASES

APPLICABLE SAFETY ANALYSES (continued)

5. Recirculation Actuation Signal

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

to ensure the reactor remains shut down in the recirculation mode.
An RWT Level - Low signal initiates the RAS.

6. Auxiliary Feedwater Actuation Signal

An AFAS initiates feedwater flow to both steam generators if a low level is indicated in either steam generator, unless the generator is ruptured.

The AFAS maintains a steam generator heat sink during the following events:

MSLB,

FWLB,

Inadvertent opening of a steam generator atmospheric dump valve, and

Loss of feedwater.

A low steam generator water level signal will initiate auxiliary feed to the affected steam generator.

Secondary steam generator (SG) differential pressure (SG-A > SG-B) or (SG-B > SG-A) inhibits auxiliary feed to a generator identified as being ruptured. This input to the AFAS logic prevents loss of the intact generator while preventing feeding a ruptured generator during MSLBs and FWLBs. This prevents containment overpressurization during these events.

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

BASES

LCO

The LCO requires all channel components necessary to provide an ESFAS actuation to be OPERABLE. 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 3.3.4-1 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 channel 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.

The Bases for the LCO on ESFAS Functions are:

1. Safety Injection Actuation Signal

a. Containment Pressure - High

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

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

b. Pressurizer Pressure - Low

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

The Allowable Value for this trip is set low enough to prevent actuating the SIAS during normal plant operation and pressurizer pressure transients. The setting is high enough that with a LOCA or MSLB it will actuate to perform as expected, mitigating the consequences of the accidents.

The Pressurizer Pressure - Low trip may be blocked when pressurizer pressure is reduced during controlled plant

shutdowns. This block is permitted below 1800 psia, and block permissive responses are annunciated in the control room. This allows for a controlled depressurization of the RCS, while maintaining administrative control of ESF protection. From a blocked condition, the block will be automatically removed as pressurizer pressure increases above 1800 psia, as sensed by two of the four sensor subsystems, in accordance with the bypass philosophy of removing bypasses when the enabling conditions are no longer satisfied.

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

LCO (continued)

The bypass permissive channels consist of four sensor subsystems and two actuation subsystems. This LCO applies to failures in the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

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

The block permissive is set low enough so as not to be enabled during normal plant operation, but high enough to allow blocking prior to reaching the trip setpoint.

2. Containment Spray Actuation Signal

CSAS is initiated either manually or automatically. At many plants, it is also necessary to have an automatic or manual SIAS for complete actuation. The SIAS opens the containment spray valves, whereas the CSAS actuates other required components. The SIAS requirement should always be satisfied on a legitimate CSAS, since the Containment Pressure - High signal setpoint used in the SIAS is the same setpoint used in the CSAS. At many plants, the transmitters used to initiate CSAS are independent of those used in the SIAS to prevent inadvertent containment spray due to failures in two sensor channels.

a. Containment Pressure - High

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

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

LCO (continued)

The Containment Pressure - High setpoint is the same in the SIAS (Function 1), CSAS (Function 2), and CIAS (Function 3). However, different sensors and logic are used in each of these Functions.

3. Containment Isolation Actuation Signala. 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.

LCO (continued)

a. Steam Generator Pressure - Low

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

The Allowable Value is set below the full load operating value for steam pressure so as not to interfere with normal plant operation. However, the setting is high enough to provide the required protection for excessive steam demand. An excessive steam demand causes the RCS to cool down, resulting in a positive reactivity addition to the core. An MSIS is required to prevent the excessive cooldown.

This Function may be manually blocked when steam generator pressure is reduced during controlled plant cooldowns. The block is permitted below 785 psia, and block permissive responses are annunciated in the control room. This allows a controlled depressurization of the secondary system, while maintaining administrative control of ESF protection. From a blocked condition, the block will be removed automatically as steam generator pressure increases above 785 psia, as sensed by two of the four sensor subsystems, in accordance with the bypass philosophy of removing bypasses when the enabling conditions are no longer satisfied.

This LCO requires four channels per steam generator of the bypass removal for MSIS Steam Generator Pressure - Low to be OPERABLE in MODES 1, 2, and 3.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This LCO applies to failures in the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

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

The block permissive is set low enough so as not to be enabled during normal plant operation, but high enough to allow blocking prior to reaching the trip setpoint.

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.

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.

The ESFAS channels satisfy Criterion 3 of 10 CFR 50.36(c)(2)(ii).

APPLICABILITY All ESFAS Functions are required to be OPERABLE in MODES 1, 2, and 3. In MODES 1, 2, and 3 there is sufficient energy in the primary and secondary systems to warrant automatic ESF System responses to:

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

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

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

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

In MODES 4, 5, and 6, automatic actuation of ESFAS Functions is not required because adequate time is available for plant operators to evaluate plant conditions and respond by manually operating the ESF components, if required, as addressed by LCO 3.3.5. In LCO 3.3.5, manual capability is required for Functions other than AFAS in MODE 4, even though automatic actuation is not required. Because of the large number of components actuated on each ESFAS, actuation is simplified by the use of the Manual Trip push buttons. Manual Trip of AFAS is not required in MODE 4 because AFW or shutdown cooling will already be in operation in this MODE.

APPLICABILITY (continued)

The ESFAS Actuation Logic must be OPERABLE in the same MODES as the automatic and Manual Trip. In MODE 4, only the portion of the ESFAS logic responsible for the required Manual Trip must be OPERABLE.

In MODES 5 and 6, ESFAS initiated systems are either reconfigured or disabled for shutdown cooling operation. Accidents in these MODES are slow to develop and would be mitigated by manual operation of individual components.

ACTIONS

The most common cause of channel inoperability is outright failure or drift of the bistable or process module sufficient to exceed the tolerance allowed by the plant specific setpoint analysis.

Typically, the drift is small and results in a delay of actuation rather than a total loss of function. Determination of setpoint drift is generally made during the performance of a CHANNEL FUNCTIONAL TEST when the process instrument is set up for adjustment to bring it to within **specification. If the actual trip setpoint is not within conservative with** respect to 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.

ACTIONS (continued)

[A.1

Condition A applies to one CSAS Containment Pressure - High channel inoperable. CSAS logic is identical to that of the other ESFAS Functions; however, the inadvertent actuation of a CSAS is undesirable, since it may damage equipment inside containment. For this reason, placing the inoperable channel in trip is not an option as it is in Conditions B and C.]

[For those plants in which the SIAS is required for a complete CSAS actuation, Condition B for one ESFAS channel inoperable and Condition C for two ESFAS channels inoperable may be preferable to Condition A.

If one CSAS channel is inoperable, operation is allowed to continue, providing the inoperable channel is placed in bypass within 1 hour. The Completion Time of 1 hour allotted to bypass the channel is sufficient to allow the operator to take all appropriate actions for the failed channel and still ensures that the risk involved in operating with the failed channel is acceptable.]

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

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

1. Safety Injection Actuation Signal
Containment Pressure - High
Pressurizer Pressure - Low
3. Containment Isolation Actuation Signal
Containment Pressure - High
Containment Radiation - High
4. Main Steam Isolation Signal
Steam Generator Pressure - Low
5. Recirculation Actuation Signal
Refueling Water Tank Level - Low
6. Auxiliary Feedwater Actuation Signal
Steam Generator Level - Low
Steam Generator Pressure Difference - High

BASES

ACTIONS (continued)

ESFAS coincidence logic is normally two-out-of-four. If one ESFAS channel is inoperable, startup or power operation is allowed to continue as long as action is taken to restore the design level of redundancy.

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

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

One failed channel is restored to OPERABLE status or is placed in trip within [48] hours (Required Action B.2.1 or B.2.2). Required Action B.2.1 restores the full capability of the function. Required Action B.2.2 places the function in a one-out-of-three configuration. In this configuration, common cause failure of the dependent channel cannot prevent ESFAS actuation. The [48] hour Completion Time is based upon operating experience, which has demonstrated that a random failure of a second channel occurring during the [48] hour period is a low probability event.

C.1 and C.2

Condition C applies to the failure of two channels in any of the following ESFAS functions:

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

3. Containment Isolation Actuation Signal
Containment Pressure - High
Containment Radiation - High

4. Main Steam Isolation Signal
Steam Generator Pressure - Low

BASES

ACTIONS (continued)

5. Recirculation Actuation Signal
Refueling Water Tank Level - Low

6. Auxiliary Feedwater Actuation Signal
Steam Generator Level - Low
Steam Generator Pressure Difference - High

With two inoperable channels, one channel should be placed in bypass, and the other channel should be placed in trip within the 1 hour Completion Time. With one channel of protective instrumentation bypassed, the ESFAS Function is in two-out-of-three logic, but with

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

One of the failed channels should be restored to OPERABLE status within [48] hours, for reasons similar to those stated under Condition B. After one channel is restored to OPERABLE status, the provisions of Condition B still apply to the remaining inoperable channel. Therefore, the channel that is still inoperable after completion of Required Action C.2 must be placed in trip if more than [48] hours has elapsed since the initial channel failure.

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

Condition D applies to the failure of one bypass removal channel.

The bypass removal channels consist of four sensor subsystems and two actuation subsystems. Condition D applies to failures in one of the four sensor subsystems, including sensors, bistables, and associated equipment. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

In Condition D, it is permissible to continue operation with one bypass permissive removal channel failed, providing the bypass is disabled (Required Action D.1). This can be accomplished by removing the bypass with the manual bypass key switch, which disables the bypass in both trains. Since the bypass Function must be manually enabled, the bypass permissive Function will not by itself cause an undesired bypass insertion.

BASES

ACTIONS (continued)

Alternatively, the bypass may be disabled by defeating the bypass permissive input in one of the four channels to the two-out-of-four bypass removal logic, placing the bypass removal feature in one-out-of-three logic. Thus, any of the remaining three channels is capable of removing the bypass feature when the bypass enable conditions are no longer valid.

If the bypass removal feature in the inoperable channel cannot be defeated, actions to address the inoperability of the affected automatic trip channel must be taken. Required Action D.2.1, Required Action D.2.2.1, and Required Action D.2.2.2 are equivalent to the Required Actions for a single automatic trip channel failure (Condition B). The 1 hour and [48] hour Completion Times have the same bases as discussed for Condition B.

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

Condition E applies to two inoperable bypass removal channels. The bypass removal channels consist of four sensor subsystems and two actuation subsystems. This Condition applies to failures in two of the four sensor subsystems. With two of the four sensor subsystems failed in a nonconservative direction (enabling the bypass Function), the bypass removal feature is in two-out-of-two logic. Failures in the actuation subsystems, including the manual bypass key switches, are considered Actuation Logic failures and are addressed in LCO 3.3.5.

In Condition E, it is permissible to continue operation with two bypass permissive channels failed, providing the bypasses are disabled in a similar manner as discussed for Condition D.

If the failed bypasses cannot be disabled, actions to address the inoperability of the affected automatic trip channels must be taken. Required Action E.2.1 and Required Action E.2.2 are equivalent to the Required Actions for a two automatic trip channel failure (Condition C). Also similar to Condition C, after one set of inoperable channels is restored, the provisions of Condition D still apply to the remaining inoperable channel, with the Completion Time measured from the point of the initial bypass channel failure. The 1 hour and [48] hour Completion Times have the same bases as discussed for Condition C.

BASES

ACTIONS (continued)

F.1 and F.2

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

SURVEILLANCE 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.

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

The Notes in Table 3.3.4-1 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 3.3.4.1

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

SURVEILLANCE REQUIREMENTS (continued)

times when Surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Offscale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

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

SR 3.3.4.2

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

The CHANNEL FUNCTIONAL TEST tests the individual sensor subsystems using an analog test input to each bistable.

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

The as-found [and as-left] values must also be recorded and reviewed for consistency with the assumptions of the surveillance interval extension analysis. The requirements for this review are outlined in Reference [8].

SR 3.3.4.2 for SL-LSSS functions is modified by two Notes as identified in Table 3.3.4-1. 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].

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.4.3

SR 3.3.4.3 is a CHANNEL FUNCTIONAL TEST similar to SR 3.3.4.2, except 3.3.4.3 is performed within 92 days prior to startup and is only applicable to bypass Functions. These include the Pressurizer Pressure - Low bypass and the MSIS Steam Generator Pressure - Low bypass. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions.

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

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

SR 3.3.4.4

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

The as-found [and as-left] values must also be recorded and reviewed for consistency with the assumptions of the -extension analysis. The requirements for this review are outlined in Reference [8].

SURVEILLANCE REQUIREMENTS (continued)

The Frequency is based upon the assumption of an [18] month calibration interval for the determination of the magnitude of equipment drift in the setpoint analysis.

SR 3.3.4.4 for SL-LSSS functions is modified by two Notes as identified in Table 3.3.4-1. 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 3.3.4.5

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 CEQG Topical Report CE NPSD-1167-1, "Elimination of Pressure Sensor Response Time Testing Requirements."

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

(Ref. 10) provides the basis and methodology for using allocated sensor response times in the overall verification of the channel response time for specific sensors identified in the Topical Report. Response time verification for other sensor types must be demonstrated by test. The allocation of sensor response times must be verified prior to placing a new component in operation and reverified after maintenance that may adversely affect the sensor response time.

BASES

SURVEILLANCE REQUIREMENTS (continued)

ESF RESPONSE TIME tests are conducted on a STAGGERED TEST BASIS of once every [18] months. This results in the interval between successive tests of a given channel of $n \times 18$ 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.
 10. CEOG Topical Report CE NPSD-1167-A, "Elimination of Pressure Sensor Response Time Testing Requirements."
-