B 3.3 INSTRUMENTATION

B 3.3.5 Engineered Safety Feature Actuation System (ESFAS) Instrumentation

BASES

BACKGROUND

The ESFAS initiates necessary safety systems, based on the values of selected unit Parameters, to protect against violating core design limits and reactor coolant pressure boundary and to mitigate 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 R~~r~~eactor C~~c~~ore Safety Limitis or ~~and~~ the Reactor Coolant System (RCS) P~~p~~ressure S~~boundary s~~afety ~~l~~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~~a 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 b 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~~a SL-LSSS (Ref. 1).

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)." 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 because 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 because 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) or CHANNEL CALIBRATION.

BASES

BACKGROUND (continued)

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 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 established [LTSP] 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 unit's life, the acceptable limits are:

a. The departure from nucleate boiling ratio (DNBR) shall be maintained above the SL value,

b. Fuel centerline melt shall not occur, and

c. The 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 20 and 10 CFR 100 criteria during AOOs.

Accidents are events that are analyzed even though they are not expected to occur during the unit's life. The acceptable limit during

accidents is that the offsite dose shall be maintained within 10 CFR 100 limits. Meeting the acceptable dose limit for an accident category is considered having acceptable consequences for that event. However, ~~these values~~ the acceptable dose limit for an accident category ~~dose limit~~ and their associated trip setpoints are not considered to be SL-LSSS as defined in 10 CFR 50.36.

ESFAS actuates the following systems:

High pressure injection (HPI) Actuation,

Low pressure injection (LPI) Actuation,

Reactor building (RB) Cooling,

RB Spray,

RB Isolation, and

Emergency diesel generator (EDG) Start.

ESFAS also provides a signal to the Emergency Feedwater Isolation and Control (EFIC) System. This signal initiates emergency feedwater (EFW) when HPI is initiated.

The ESFAS operates in a distributed manner to initiate the appropriate systems. The ESFAS does this by determining the need for actuation in each of three channels monitoring each actuation Parameter. Once the need for actuation is determined, the condition is transmitted to automatic actuation logics, which perform the two-out-of-three logic to determine the actuation of each end device. Each end device has its own automatic actuation logic, although all automatic actuation logics take their signals from the same point in each channel for each Parameter.

Four Parameters are used for actuation:

Low Reactor Coolant System (RCS) Pressure,

Low Low RCS Pressure,

BASES

BACKGROUND (continued)

High RB Pressure, and

High High RB Pressure.

LCO 3.3.5 covers only the instrumentation channels that measure these Parameters. These channels include all intervening equipment necessary to produce actuation before the measured process Parameter exceeds the limits assumed by the accident analysis. This includes sensors, bistable devices, operational bypass circuitry, block timers, and output relays. LCO 3.3.6, "Engineered Safety Feature Actuation System (ESFAS) Manual Initiation," and LCO 3.3.7, "Engineered Safety Feature Actuation System (ESFAS) Automatic Actuation Logic," provide requirements on the manual initiation and automatic actuation logic Functions.

The ESFAS consists of three protection channels. Each channel provides input to logics that initiate equipment with a two-out-of-three logic on each component. Each protection channel includes bistable inputs from one instrumentation channel of Low RB Pressure, Low Low RCS Pressure, High RB Pressure, and High High RB Pressure. Automatic actuation logics combine the three protection channel trips in each train to actuate the individual Engineered Safety Feature (ESF) components needed to initiate each ESF System. Figure [ ] , FSAR, Chapter [7] (Ref. 1), illustrates how instrumentation channel trips combine to cause protection channel trips.

The RCS pressure sensors are common to both trains. Isolation is provided via separate bistables for each train. Separate RB pressure sensors are used for the high and high high pressure Functions in each train, and separate sensors are used for each train.

The following matrix identifies the measurement channels and the Function actuated by each.

BASES

BACKGROUND (continued)

PARAMETER	LOW RCS PRESSURE	LOW LOW RCS PRESSURE	HIGH RB PRESSURE	HIGH HIGH RB PRESSURE
HPI	X	X	X	
LPI		X		X
RB Cooling	X	X	X	(b)
RB Spray	(b)			
RB Isolation[(a)]	X	X	X	
EDG Start	X	X	X	
Control Room Isolation			X	

(a) Only isolates systems not required for RB or RCS heat removal.
(b) Actuates on High High RB Pressure coincident with HPI actuation.

Engineered safeguards bus undervoltage will also sequence on the HPI loads started by the HPI block timers. However, HPI will not occur unless the ESFAS HPI signal is also present. LCO 3.3.8, "Emergency Diesel Generator (EDG) Loss of Power Start (LOPS)," contains the requirements for the undervoltage channels.

BASES

BACKGROUND (continued)

The ESF equipment is divided between the two redundant actuation trains A and B. The division of the equipment between the two actuation trains is based on the equipment redundancy and function and is accomplished in such a manner that the failure of one of the actuation channels and the related safeguards equipment will not inhibit the overall ESF Functions. Where a motor operated or a solenoid operated valve is driven by either of two matrices, one is from actuation channel A and one from actuation channel B. Redundant ESF pumps are controlled from separate and independent actuation channels.

The actuation of ESF equipment is also available by manual actuation switches located on the control room console.

The ESFAS, in conjunction with the actuated equipment, provides protective functions necessary to mitigate Design Basis Accidents (DBAs), specifically the loss of coolant accident (LOCA) and steam line break (SLB) events. The ESFAS relies on the OPERABILITY of the automatic actuation logic for each component to perform the actuation of the selected systems of LCO 3.3.7.

Engineered Safety Feature Actuation System Bypasses

No provisions are made for maintenance bypass of ESFAS instrumentation channels. Operational bypass of certain channels is necessary to allow accident recovery actions to continue and, for some channels, to allow reactor shutdown without spurious ESFAS actuation.

The ESFAS RCS pressure instrumentation channels include permissive bistables that allow manual bypass when reactor pressure is below the point at which the low and low low pressure trips are required to be OPERABLE. Once permissive conditions are sensed, the RCS pressure trips may be manually bypassed. Bypasses are automatically removed when bypass permissive conditions are exceeded.

Each High RB Pressure channel may be manually bypassed after the other two channels in the Parameter have tripped. The manual bypass allows operators to take manual control of ESF Functions after initiation to allow recovery actions. The bypass may be manually removed and is automatically removed when RB pressure returns to below the trip setpoint.

BASES

BACKGROUND (continued)

Reactor Coolant System Pressure

The RCS pressure is monitored by three independent pressure transmitters located in the RB. These transmitters are separate from the transmitters that feed the Reactor Protection System (RPS). Each of the pressure signals generated by these transmitters is monitored by four bistables to provide two trip signals, at 1500 psig and 500 psig, and two bypass permissive signals, at 1700 psig and 900 psig.

The outputs of the three bistables, associated with the low RCS pressure, 1500 psig, trip drive relays in two sets (actuation channels A and B) of identical and independent channels. These two sets of HPI channels each use three logic channels used in two-out-of-three coincidence networks for HPI Actuation. The outputs of the three bistables associated with the Low Low RCS Pressure [500 psig] trip drive relays in two sets (actuation channels A and B) of identical and independent channels. These two sets of LPI channels each use three logic channels used in two-out-of-three coincidence networks for LPI Actuation. The outputs of the three Low Low RCS Pressure bistables also trip the drive relays in the corresponding HPI Actuation channel as previously described.

Reactor Building Pressure

RB pressure inputs to the ESFAS are provided by 12 pressure switches. Six pressure switches are used for the High RB Pressure Parameter, and six pressure switches are used for the High High Pressure Parameter.

The output contacts of six High RB Pressure switches are used in two sets of identical and independent actuation trains. These two trains each use three logic channels. The outputs of these channels are used in two-out-of-three coincidence networks. The output contacts of the six RB pressure switches also trip the drive relays in the corresponding HPI and LPI Actuation channels as previously described.

The output contacts of six High High RB Pressure switches are used in two sets of identical and independent actuation trains. These two trains each use three logic channels (RB4, RB5, and RB6). The outputs of these channels are used in two-out-of-three coincident networks for RB Spray Actuation. Each high high pressure train actuates one RB Spray train when the High High RB signal and the HPI signal are coincident in that train.

BASES

BACKGROUND (continued)

[Limiting Trip Setpoints] and Allowable Values

Trip setpoints are the nominal value at which the bistables are set. Any bistable is considered to be properly adjusted when the "as-left" value is within the band for CHANNEL CALIBRATION accuracy (i.e., ± [rack calibration + comparator setting accuracy]).

The trip setpoints used in the bistables are based on the analytical limits stated in Figure [ ]-, FSAR, Chapter [7] (Ref. 1). The selection of these ~~trip setpoints~~[LTSPs] is such that adequate protection is provided when all sensor and processing uncertainties and time delays are taken into account. To allow for calibration tolerances, instrumentation uncertainties, instrument drift, and severe environment induced errors for those ESFAS channels that must function in harsh environments as defined by 10 CFR 50.49 (Ref. 2), the 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~~[LTSPs], as-left tolerances, and as-found tolerances, including their explicit uncertainties, is provided in the "Unit Specific Setpoint Methodology" (Ref. 3). The actual nominal trip setpoint entered into the bistable is more conservative than that specified by the Allowable Value to account for changes in random measurement errors detectable by a CHANNEL FUNCTIONAL TEST. One example of such a change in measurement error is drift during the surveillance interval. A channel is inoperable if its actual trip setpoint is ~~not within~~ non-conservative with respect to its required Allowable Value.

[Limiting Trip Setpoints], in accordance with the Allowable Values, ensure that the consequences of DBAs will be acceptable, providing the unit is operated from within the LCOs at the onset of the DBA and the equipment functions as designed. Note that in LCO 3.3.5 the Allowable Values listed in Table 3.3.5-1 are the least conservative value of the as-found setpoint that a channel can have during a periodic CHANNEL CALIBRATION or CHANNEL FUNCTIONAL TEST.

Each channel can be tested online to verify that the signal and setpoint accuracy is within the specified allowance requirements of Reference 3. Once a designated channel is taken out of service for testing, a simulated signal is injected in place of the field instrument signal. The process equipment for the channel in test is then tested, verified, and calibrated.

BASES

BACKGROUND (continued)

The Allowable Values listed in Table 3.3.5-1 are based on the methodology described in FSAR, Chapter [14] (Ref. 4), which incorporates all of the known uncertainties applicable for each channel. The magnitudes of these uncertainties are factored into the determination of each ~~trip setpoint.~~[LTSP]. All field sensors and signal processing equipment for these channels are assumed to operate within the allowances of these uncertainty magnitudes.

----------REVIEWER'S NOTE----------
The ESFAS LCOs in the BWOG Standard Technical Specifications are based on a system representative of the Crystal River Unit 3 design.----------
----------As discussed earlier, this arrangement involves measurement channels shared among all actuation functions, with separate actuation logic channels for each actuated component. In this arrangement, multiple components are affected by each instrumentation channel failure, but a single automatic actuation logic failure affects only one component. The organization of BWOG STS ESFAS LCOs reflects the described logic arrangement by identifying instrumentation requirements on an instrumentation channel rather than on a protective function basis. This greatly simplifies delineation of ESFAS LCOs. Furthermore, the LCO requirements on instrumentation channels, automatic actuation logics, and manual initiation are specified separately to reflect the different impact each has on ESFAS OPERABILITY.

APPLICABLE SAFETY ANALYSES

The following ESFAS Functions have been assumed within the accident analyses.

[LTSPs] ~~Trip Setpoints~~ that ~~directly~~ protect against violating the ~~r~~Reactor ~~c~~Core Safety Limits or Reactor Coolant System (RCS) ~~p~~Pressure ~~boundary~~ Safety Limit~~s~~ 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.

High Pressure Injection

The ESFAS actuation of HPI has been assumed for core cooling in the LOCA analysis and is credited with boron addition in the SLB analysis.

Low Pressure Injection

The ESFAS actuation of LPI has been assumed for large break LOCAs.

BASES
APPLICABLE SAFETY ANALYSES (continued)

Reactor Building Spray, Reactor Building Cooling, and Reactor Building Isolation

The ESFAS actuation of the RB coolers and RB Spray have been credited in RB analysis for LOCAs, both for RB performance and equipment environmental qualification pressure and temperature envelope definition. Accident dose calculations have credited RB Isolation and RB Spray.

Emergency Diesel Generator Start

The ESFAS initiated EDG Start has been assumed in the LOCA analysis to ensure that emergency power is available throughout the limiting LOCA scenarios.

The small and large break LOCA analyses assume a conservative 35 second delay time for the actuation of HPI and LPI in FSAR, Chapter [14] (Ref. 4). This delay time includes allowances for EDG starting, EDG loading, Emergency Core Cooling Systems (ECCS) pump starts, and valve openings. Similarly, the RB Cooling, RB Isolation, and RB Spray have been analyzed with delays appropriate for the entire system analyzed. Typical values used in the analysis are 35 seconds for RB Cooling, 60 seconds for RB Isolation, and 56 seconds for RB Spray.

Accident analyses rely on automatic ESFAS actuation for protection of the core temperature and containment pressure limits and for limiting off site dose levels following an accident. These include LOCA, SLB, and feedwater line break events that result in RCS inventory reduction or severe loss of RCS cooling.

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

LCO

The LCO requires three channels of ESFAS instrumentation for each Parameter in Table 3.3.5-1 to be OPERABLE in each ESFAS train. Failure of any instrument renders the affected channel(s) inoperable and reduces the reliability of the affected Functions.

BASES
LCO (continued)

Only the Allowable Values are specified for each RPS trip 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 "[Unit Specific Setpoint Methodology]" (Ref. 3). 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. ~~Only the Allowable Value is specified for each ESFAS Function in the LCO. Nominal trip setpoints are specified in the unit specific setpoint calculations.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 nominal trip setpoints are selected to ensure the setpoints measured by CHANNEL FUNCTIONAL TESTS do not exceed the Allowable Value if the bistable is performing as required. Operation with a trip setpoint less conservative than the nominal trip setpoint[LTSP], but within conservative with respect its Allowable Value, is acceptable provided that operation and testing are consistent with the assumptions of the unit specific setpoint calculations. and that the trip setpoint is within the as-found tolerance. Each Allowable Value specified is more conservative than the analytical limit assumed in the safety analysis to account for instrument uncertainties appropriate to the trip Parameter. These uncertainties are defined in the "Unit Specific Setpoint Methodology" (Ref. 3).~~

The Allowable Values for bypass removal functions are stated in the Applicable MODES or Other Specified Condition column of Table 3.3.5-1.

Three ESFAS instrumentation channels shall be OPERABLE in each ESFAS train to ensure that a single failure in one channel will not result in loss of the ability to automatically actuate the required safety systems.

The bases for the LCO on ESFAS Parameters include the following.

Reactor Coolant System Pressure

Three channels each of RCS Pressure - Low and RCS Pressure - Low Low are required OPERABLE in each train. Each channel includes a sensor, trip bistable, bypass bistable, bypass relays, output relays, and block timers. The analog portion of each pressure channel is common to both trains of both RCS Pressure Parameters. Therefore, failure of one analog channel renders one channel of the low pressure and low low pressure Functions in each train inoperable. The bistable portions of the channels are Function and train specific. Therefore, a bistable failure renders only one Function in one train inoperable. Failure of a bypass bistable or bypass circuitry, such that a trip channel cannot be bypassed, does not render the channel inoperable. Output relays and block timer relays are train specific but may be shared among Parameters. Therefore, output or block timer relay failure renders all affected Functions in one train inoperable.

BASES
LCO (continued)

1. Reactor Coolant System Pressure - Low Setpoint

   The RCS Pressure - Low Setpoint is based on HPI actuation for small break LOCAs. The setpoint ensures that the HPI will be actuated at a pressure greater than or equal to the value assumed in accident analyses plus the instrument uncertainties. The maximum value assumed for the setpoint of the RCS Pressure - Low trip of HPI in safety analyses is 1480 psig. The setpoint for the low RCS and Allowable Value of $\geq$ [1600] psig for the low pressure Parameter is selected to ensure actuation occurs when actual RCS pressure is above 1480 psig. The RCS Pressure instrumentation must function while subject to the severe environment created by a LOCA. Therefore, the ~~trip setpoint~~[LTSP] and Allowable Value accounts for severe environment induced errors.

   To ensure the RCS Pressure - Low trip is not bypassed when required to be OPERABLE by the safety analysis, each channel's bypass removal bistable must be set with an Allowable Value of $\leq$ [1800] psig. The bypass removal does not need to function for accidents initiated from RCS Pressures below the bypass removal setpoint. Therefore, the bypass removal setpoint Allowable Value need not account for severe environment induced errors.

2. Reactor Coolant System Pressure - Low Low Setpoint

   The RCS Pressure - Low Low Setpoint LPI actuation occurs in sufficient time to ensure LPI flow prior to the emptying of the core flood tanks during a large break LOCA. The Allowable Value of $\geq$ [400] psig ensures sufficient overlap of the core flood tank flow and

the LPI flow to keep the reactor vessel downcomer full during a large break LOCA. The RCS Pressure instrumentation must function while subject to the severe environment created by a LOCA. Therefore, the [LTSP] and ~~trip setpoint~~ Allowable Value accounts for severe environment induced errors.

To ensure the RCS Pressure - Low Low trip is not bypassed when assumed OPERABLE by the safety analysis, each channel's bypass removal bistable must be set with an Allowable Value of $\leq$ [900] psig. The bypass removal does not need to function for accidents initiated by RCS Pressure below the bypass removal setpoint. Therefore, the bypass removal setpoint Allowable Value need not account for severe environment induced errors.

BASES

LCO (continued)

Reactor Building Pressure

Three channels each of RCS Pressure - Low and RB Pressure - High are required to be OPERABLE in each train. Each channel includes a pressure switch, bypass relays, and output relays. The high pressure channels also include block timers. Each pressure switch is Function and train specific, so there are 12 pressure switches total. Therefore, a pressure switch renders only one Function in one train inoperable. Output relays and block timer relays are train specific but may be shared among Parameters. Therefore, output or block timer relay failure renders all affected Functions in one train inoperable.

The RB Pressure switches may be subjected to high radiation conditions during the accidents that they are intended to mitigate. The sensor portion of the switches is also exposed to the steam environment present in the RB following a LOCA or high energy line break. Therefore, the trip setpoint Allowable Value accounts for measurement errors induced by these environments.

1. Reactor Building Pressure - High Setpoint

   The RB Pressure - High Setpoint Allowable Value $\leq$ [5] psig was selected to be low enough to detect a rise in RB Pressure that would occur due to a small break LOCA, thus ensuring that the RB high pressure actuation of the safety systems will occur for a wide spectrum of break sizes. The trip setpoint also causes the RB coolers to shift to emergency mode to prevent damage to the cooler fans due to the increase in the density of the air steam mixture present in the containment following a LOCA.

2. Reactor Building Pressure - High High Setpoint

   The RB Pressure - High High Setpoint Allowable Value $\leq$ [30] psig was chosen to be high enough to avoid actuation during ~~an SL~~a SLB, but also low enough to ensure a timely actuation during a large break LOCA.

BASES

APPLICABILITY Three channels of ESFAS instrumentation for each Parameter listed next shall be OPERABLE in each ESFAS train.

1. Reactor Coolant System Pressure - Low Setpoint

   The RCS Pressure - Low Setpoint actuation Parameter shall be OPERABLE during operation above 1800 psig. This requirement ensures the capability to automatically actuate safety systems and components during conditions indicative of a LOCA or secondary unit overcooling. Below 1800 psig, the low RCS Pressure actuation Parameter can be bypassed to avoid actuation during normal unit cooldowns when safety systems actuations are not required.

   The allowance for the bypass is consistent with the transition of the unit to a lower energy state, providing greater margins to safety limits. The unit response to any event, given that the reactor is already tripped, will be less severe and allows sufficient time for operator action to provide manual safety system actuations. This is even more appropriate during unit heatups when the primary system and core energy content is low, prior to power operation.

   In MODES 5 and 6, there is adequate time for the operator to evaluate unit conditions and respond by manually starting individual systems, pumps, and other equipment to mitigate the consequences of an abnormal condition or accident. Plant pressure and temperature are very low, and many ESF components are administratively locked out or otherwise prevented from actuating to prevent inadvertent overpressurization of unit systems.

2. Reactor Coolant System Pressure - Low Low Setpoint

   The RCS Pressure - Low Low Setpoint actuation Parameter shall be OPERABLE during operation above [900] psig. This requirement ensures the capability to automatically actuate safety systems and components during conditions indicative of a LOCA or secondary unit overcooling. Below [900] psig, the low low RCS Pressure actuation Parameter can be bypassed to avoid actuation during normal unit cooldowns when safety system actuations are not required.

   The allowance for the bypass is consistent with the transition of the unit to a lower energy state, providing greater margins to safety limits. The unit response to any event, given that the reactor is already tripped, will be less severe and allows sufficient time for operator action to provide manual safety system actuations. This is even more appropriate during unit heatups when the primary system and core energy content is low, prior to power operation.

BASES
APPLICABILITY (continued)

In MODES 5 and 6, there is adequate time for the operator to evaluate unit conditions and respond by manually starting individual systems, pumps, and other equipment to mitigate the consequences of an abnormal condition or accident. Plant pressure and temperature are very low, and many ESF components are administratively locked out or otherwise prevented from actuating to prevent inadvertent overpressurization of unit systems.

3. 4. Reactor Building Pressure - High and Reactor Building Pressure – High High Setpoints

The RB Pressure - High and RB Pressure - High High actuation Functions of ESFAS shall be OPERABLE in MODES 1, 2, 3, and 4 when the potential for a HELB exists. In MODES 5 and 6, the unit conditions are such that there is insufficient energy in the primary and secondary systems to raise the containment pressure to either the RB Pressure - High or RB Pressure - High High Setpoints. Furthermore, in MODES 5 and 6, there is adequate time for the operator to evaluate unit conditions and respond by manually starting individual systems, pumps, and other equipment to mitigate the consequences of an abnormal condition or accident. Plant pressure and temperature are very low and many ESF components are administratively locked out or otherwise prevented from actuating to prevent inadvertent overpressurization of unit systems.

ACTIONS Required Actions A and B apply to all ESFAS instrumentation Parameters listed in Table 3.3.5-1.

A Note has been added to the ACTIONS indicating separate Condition entry is allowed for each Parameter.
If a channel's trip setpoint is found non-conservative with respect to the Allowable Value, or the transmitter, instrument loop, signal processing electronics, or ESFAS bistable is found inoperable, then all affected functions provided by that channel should be declared inoperable and the unit must enter the Conditions for the particular protection Parameter affected.

When the number of inoperable channels in a trip Parameter exceeds those specified, then the unit is outside the safety analysis. Therefore, LCO 3.0.3 shall be immediately entered if applicable in the current MODE of operation.

BASES
ACTIONS (continued)

A.1

Condition A applies when one channel becomes inoperable in one or more Parameters. If one ESFAS channel is inoperable, placing it in a tripped condition leaves the system in a one-out-of-two condition for actuation. Thus, if another channel were to fail, the ESFAS instrumentation could still perform its actuation functions. This action is completed when all of the affected output relays and block timers are tripped. This can normally be accomplished by tripping the affected bistables or tripping the individual output relays and block timers. [At this unit, the specific output relays associated with each ESFAS instrumentation channel are listed in the following document:]

The 1 hour Completion Time is sufficient time to perform the Required Action.

B.1, B.2.1, B.2.2, and B.2.3

Condition B applies when Required Action A.1 is not met within the required Completion Time or when one or more parameters have more than one inoperable channel. If Condition B applies, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 6 hours and, for the RCS Pressure - Low Setpoint, to < [1800] psig, for the RCS Pressure - Low Low Setpoint, to < [900] psig, and for the RB Pressure High Setpoint and High High Setpoint, to MODE 5 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required unit conditions from full power conditions in an orderly manner and without challenging unit systems.

SURVEILLANCE REQUIREMENTS

All ESFAS Parameters listed in Table 3.3.5-1 are subject to CHANNEL CHECK, CHANNEL FUNCTIONAL TEST, CHANNEL CALIBRATION, and response time testing. The operational bypasses associated with each ESFAS instrumentation channel are also subject to these SRs to ensure OPERABILITY of the ESFAS instrumentation channel.

---------- 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 may ~~are~~ not apply ~~ied~~ 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.

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.3.5.1

Performance of the CHANNEL CHECK every 12 hours ensures that a

gross failure of instrumentation has not occurred. A CHANNEL CHECK is normally a comparison of the parameter indicated on one channel to a similar parameter on other channels. It is based on the assumption that instrument channels monitoring the same parameter should read approximately the same value. Significant deviations between the two instrument channels could be an indication of excessive instrument drift in one of the channels or of something even more serious. CHANNEL CHECK will detect gross channel failure; therefore, it is key in verifying that the instrumentation continues to operate properly between each CHANNEL CALIBRATION.

Agreement criteria are determined by the unit staff, based on a combination of the channel instrument uncertainties, including isolation, indication, and readability. If a channel is outside the criteria, it may be an indication that the transmitter or the signal processing equipment has drifted outside its limit. If the channels are normally off scale during times when surveillance is required, the CHANNEL CHECK will only verify that they are off scale in the same direction. Off scale low current loop channels are verified to be reading at the bottom of the range and not failed downscale.

The Frequency, 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 the displays associated with the LCO's required channels.

SR 3.3.5.2

A Note defines a channel as being OPERABLE for up to 8 hours while bypassed for Surveillance testing provided the remaining two ESFAS channels are OPERABLE or tripped. The Note allows channel bypass for testing without defining it as inoperable, although during this time period it cannot initiate ESFAS. This allowance is based on the inability to perform the Surveillance in the time permitted by the Required Actions. Eight hours is the average time required to perform the Surveillance. It is not acceptable to routinely remove channels from service for more than 8 hours to perform required Surveillance testing.

BASES

SURVEILLANCE REQUIREMENTS (continued)

A CHANNEL FUNCTIONAL TEST is performed on each required ESFAS channel to ensure the entire channel will perform the intended functions. A successful test of the required contact(s) of a channel relay may be performed by the verification of the change of state of a single contact of the relay. This clarifies what is an acceptable CHANNEL FUNCTIONAL TEST of a relay. This is acceptable because all of the other required contacts of the relay are verified by other Technical Specifications and non-Technical Specifications tests at least once per refueling interval with applicable extensions. Any setpoint adjustment shall be consistent with the assumptions of the current unit specific setpoint analysis.

The Frequency of 31 days is based on unit operating experience, with regard to channel OPERABILITY and drift, which demonstrates that failure of more than one channel of a given function in any 31 day interval is a rare event.

SR 3.3.5 2 for SL-LSSS functions is 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 3.3.5.3

CHANNEL CALIBRATION is a complete check of the instrument channel, including the sensor. The test 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 to ensure that the instrument channel remains operational between successive tests. CHANNEL CALIBRATION shall find that measurement errors and bistable setpoint errors are within the assumptions of the unit specific setpoint analysis. CHANNEL CALIBRATIONS must be performed consistent with the assumptions of the unit specific setpoint analysis.

This Frequency is justified by the assumption of an [18] month calibration interval to determine the magnitude of equipment drift in the setpoint analysis.

SR 3.3.5.3 for SL-LSSS functions is 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

SR 3.3.5.4 ensures that the ESFAS actuation channel response times are less than or equal to the maximum times assumed in the accident analysis. The response time values are the maximum values assumed in the safety analyses. Individual component response times are not modeled in the analyses. Response time testing acceptance criteria for this unit are included in Reference 1. The analyses model the overall or total elapsed time from the point at which the parameter exceeds the

BASES

SURVEILLANCE REQUIREMENTS (continued)

actuation setpoint value at the sensor to the point at which the end device is actuated. Thus, this SR encompasses the automatic actuation logic components covered by LCO 3.3.7 and the operation of the mechanical ESF components.

Response time tests are conducted on an [18] month STAGGERED TEST BASIS. Testing of the final actuation devices, which make up the bulk of the response time, is included in the testing of each channel. Therefore, staggered testing results in response time verification of these devices every [18] months. The 18 month test Frequency is based on unit 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, Chapter [7].

2. 10 CFR 50.49.

3. [Unit Specific Setpoint Methodology.]

4. FSAR, Chapter [14].